



Location Data and Human Mobility: An Evaluation of a Dissonance that Frames Data Protection and Privacy Rights

Jonathan Andrew

Thesis submitted for assessment with a view to obtaining
the degree of Doctor of Laws of the European University Institute

Florence, 09 February 2018

European University Institute
Department of Law

Location Data and Human Mobility: An Evaluation of a Dissonance
that Frames Data Protection and Privacy Rights

Jonathan Andrew

Thesis submitted for assessment with a view to obtaining
the degree of Doctor of Laws of the European University Institute

Examining Board

Professor Deirdre Curtin, European University Institute
Professor Emeritus Marise Cremona, European University Institute
Professor Julia Hörnle, Queen Mary University of London
Professor Claudia Diaz, KU Leuven

© Jonathan Andrew, 2018

No part of this thesis may be copied, reproduced or transmitted without prior
permission of the author

**Researcher declaration to accompany the submission of written work
Department of Law – LL.M. and Ph.D. Programmes**

I, Jonathan Richard Andrew, certify that I am the author of the work 'Location Data and Human Mobility: An Evaluation of a Dissonance that Frames Data Protection and Privacy Rights' I have presented for examination for the Ph.D. at the European University Institute. I also certify that this is solely my own original work, other than where I have clearly indicated, in this declaration and in the thesis, that it is the work of others.

I warrant that I have obtained all the permissions required for using any material from other copyrighted publications.

I certify that this work complies with the Code of Ethics in Academic Research issued by the European University Institute (IUE 332/2/10 (CA 297)).

The copyright of this work rests with its author. Quotation from this thesis is permitted, provided that full acknowledgement is made. This work may not be reproduced without my prior written consent. This authorisation does not, to the best of my knowledge, infringe the rights of any third party.

I declare that this work consists of 121,633 words.

Signature and date:



23/1/2018

Addendum

Research conducted within the scope of this doctoral thesis was completed in the SURVEILLE project, a project co-funded by the European Commission within the Seventh Framework Programme. This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 284725.

**‘Location Data and Human Mobility: An
Evaluation of a Dissonance that Frames Data Protection and
Privacy Rights’**

Jonathan Andrew

Summary

With citizens' movements mediated by many technologies that aid our navigation the potential for omnipresent surveillance may potentially institute fundamental changes to the human condition. Locational privacy is pivotal in developing inter-personal associations and relational ties with others and its function is therefore complex, rather than solely affording a degree of independence from the observations made by others. In this respect, a more nuanced understanding of the utility of location data is required; the current hierarchy that delineates personal data from special categories of personal data does not adequately appreciate the capacity for location data to act as a proxy for other sensitive personal data. Furthermore, the binary distinction that reflects the conceptualisation of the right to privacy as a negative right, with related concepts such as identity and personality formation viewed as positive constructs, is increasingly difficult a notion to preserve. The classification and terminology of technologies can illustrate how terms and legal metaphors are developed and applied so as to bridge gaps in applying existing context and precedent. Though the designation 'location data' once constituted a reasonable accommodation in nomenclature as an intelligible and easily comprehensible term, even while constituting a significant oversimplification of the data it represented, technological advances have rendered the term increasingly problematic. This study asks whether the existing legal framework at the regional level in Europe is apt to provide sufficiently cogent and coherent regulation given recent developments in technologies. The review analyses the risks associated with this predilection in data processing activities that allows for the identification of ever more intimate and nuanced details of a citizen's life, behaviours and convictions through the analysis of their location data; in turn, it shall discern the necessity of considering the resulting impacts on citizens' fundamental rights to privacy and personal data protection.

Table of Contents

Table of Contents	5
Chapter 1: Introduction	11
1. Human mobility and technologies: a short introduction	11
1.1 Framing the role of location in relation to privacy	18
1.2 Location data and the conceptualisation of locational privacy.....	24
1.3 The challenges to locational privacy and data protection of new technologies.....	28
2. Defining the framework of the thesis: research question, purpose of the research	31
3. Structure of the thesis	44
Chapter 2: The Development of a Framework for Personal Data Protection and Privacy as Rights in Europe	49
1. Introduction	49
1.1 The path to personal data protection in Europe	50
1.2 The OECD Guidelines and the international dimension to data processing regulation	53
1.3 COE - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).....	56
2. The EU Data Protection Framework	59
2.1 The Data Protection Directive 95/46/EC	59
2.2 Directive 2002/58/EC	62
2.3 Directive 2009/136/EC	67
2.4 Charter of Fundamental Rights of the European Union (EUCFR).....	68
2.5 The Lisbon Framework and TFEU Article 16: Consolidation of the Right to Data Protection at the EU Level.....	69
2.6 The Comprehensive Reform of EU Data Protection Rules	70
3. The Right to Privacy	72
3.1 The International Covenant on Civil and Political Rights (ICCPR).....	72
3.2 The Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)	75
4. Conclusions	78
Chapter 3: Mobility, Technological Innovation and the Evolving Paradigm of Privacy and Data Protection	81
1. Introduction	81
2. Framing technology and its transformational role vis-à-vis the existing concepts of privacy and data protection	83
2.1 Concept of personal data	83
2.2 Parallels: online and offline locations, and content	87
2.3 Directive 95/46/EC in respect of location data	89
2.4 Distinguishing between traffic and location data	91
2.5 Location data and purpose limitation	96
3. Personal data? The relationship between devices, location data collection and data subjects	99
4. Location data: specifying its sensitivity as personal data	100
4.1 Location data processing in other sectors: security and public safety.....	102
4.2 Law enforcement use of location data	105
4.3 Sensitive personal data in the police and judicial sectors.....	110
5. Location data-based profiling and the risks to third parties	112
5.1 Third parties and location data: further considerations	114
6. Mass surveillance and bulk data retention of location data	116

6.1 Notification and data subjects' access to information	119
6.2 Collection of location data: applying the data minimization principle.....	124
7. Conclusions	127
Chapter 4:	129
A Critique of Developments in Data Analytics: Applying Novel Profiling	
Techniques to Location Data	129
1. Introduction	129
2. Current profiling capabilities.....	129
3. Developing predictive profiling using location data for surveillance purposes –	
social network site analysis as an analogy	133
4. Profiling associations: data-based insights into relationships.....	140
4.1 Mining data for the analysis of inter-personal associations.....	144
4.2 Exploiting link analysis and patterns of association in predictive profiling.....	151
4.3 The specific risks inherent to pattern-based profiling	155
5. Profiling location data: drawing inferences in relation to special categories of data	
.....	160
6. Qualifying and assessing the risks: the implications for location data use in	
profiling.....	161
7. Conclusions	176
Chapter 5:	179
The Internet of Things: A Paradigmatic Shift for the Significance of Location	
Data	179
1. Introduction	179
2. The challenges of IoT to personal data protection principles	181
2.1 A focus on personal devices and the 'quantified self'	185
3. Determining personal from non-personal data: IoT and location data	186
3.1 IoT-specific challenges to the safeguard of the rights to privacy and personal data	
protection	192
3.2 The relationship between personal data, location and time (temporal aspects).....	194
3.3 Purpose specification principle and use limitation	200
4. Contextualizing consent in relation to IoT functionality.....	201
4.1 Consent, control and information asymmetry	205
4.2 Appraising the function of consent in the relationship of IoT devices to the data	
subject	207
5. Purpose limitation versus inferential determination	214
6. Discriminatory effects: ubiquitous location data collection and processing.....	216
7. Conclusions	223
Chapter 6: Establishing and Developing Biometrics using Location Data	227
1. Introduction	227
2. Behaviometric profiles conceptualized.....	229
3. Privacy and personal data protection challenges presented by biometric identifiers	
.....	233
3.1 Applying the principle of purpose specification.....	234
4. The challenge of repurposing location data.....	238
5. Reconciling covert data collection with the principle of informed consent	245
6. The sensitivity of health data, and a data subject's right to self-determination	248
6.1 The application of public interest exemptions to the processing of sensitive data and	
developing movement-based biometrics	255
6.2 In accordance with the law	260
6.3 Necessary in a democratic society	262
7. Location data as a biometric identifier: determining the way forward.....	265
8. Conclusions	270

Chapter 7: Conclusions	275
Appendix I: References	301
A) Books	301
C) Articles in Journals	308
D) Documents	328
E) Cases	341
European Court of Human Rights (ECHR)	341
European Court of Justice (CJEU)	342
Other jurisdictions	343

Acknowledgements

This work is dedicated to the memory of two people in particular who have inspired me during the time researching at the European University Institute: to Peter Andrew, and to Sharon Laws.

I would like to thank Professor Deirdre Curtin for her insight, patience, kindness and enthusiasm in encouraging me to complete my doctoral studies. I am truly grateful for all her endeavours. I also wish to thank the members of the panel: Professor Marise Cremona, Professor Claudia Diaz, and Professor Julia Hörnle, for their guidance and helpful comments while examining my PhD thesis — their efforts are very much appreciated.

I shall forever be immensely thankful for the professionalism of Dr. Celine Agrumi, Dr. Gaëlle Vallencant, Neil McLean-Martin and all the staff at LCDS in Chamonix. Their dedication and care has made such an enormous difference to my life.

During my time at the European University Institute I've had the good fortune to work with many wonderful colleagues. Foremost, I wish to thank Dr. Maria Grazia Porcedda for being a dear friend, for supporting me through the toughest of times, for showing courage and conviction. I feel blessed to have had Maria Grazia's friendship over the years, and have learned so much from her. I also wish to thank Martyn Egan, who has been a constant reminder of all that's best in the Mancunian spirit and has kept my spirits up with his well-timed, witty and astute observations. A special mention must also go to Dr. Karolina Podstawa, who has provided wonderful support and invaluable guidance and advice whenever needed, and has been extremely patient in fielding far too many questions from me! Thank you so, so much, Karolina.

At the European University Institute I was also so very fortunate to have worked with Matthew Langthorne, an especially creative and talented soul, who became a truly great friend. Matt worked tirelessly to help me when we collaborated on project tasks at the EUI, and was there to provide much needed encouragement in the final steps of my thesis writing: thank you for making sure I didn't stop too soon, and that I persevered in those last few weeks and days! Matt also taught me how little I really know about photography...

I am especially grateful too to Annick Bulckaen, who provided me with a huge amount of assistance and advice while we worked together in Villa Schifanoia. I must also thank Machteld Nijsten at the EUI library for her hard work in resourcing materials and for providing me with all the many, many books and journals I requested during my studies. I must also express my gratitude to Andrea, Simona and Antonella at both Villa Schifanoia and Villa Salviati — their professionalism and kindness (and patience with my poor Italian vocabulary!) is much appreciated. I must also thank Paula, Lucia, Antonella and all those working at the villas' facilities on campus for creating a wonderful ambiance in which to work – *grazie mille!*

I am particularly thankful to Professor Rebecca Wallace, who has helped me enormously and provided encouragement during my studies in law. Without Rebecca

I would not have had the opportunity to study in Florence. I am also extremely grateful to both Dr. Karol Nowak and Dr. Christiane Höhn for their moral support and encouragement. I must also express my gratitude to Robert Howie and Dr. Elina Steinerte for their friendship and support while I was in Glasgow at the very start of my studies in the legal field, and for their belief at the very start that human rights law was the career I should work in and dedicate all my efforts to.

I'm very thankful too to Philip and Andrea Blunsum for their unwavering support and friendship during my time studying, and for putting up with my musings and nostalgia for Brighton life when visiting the English coast. I must also thank Kenton and Jazz Cool for being such fantastic friends and really backing me every step, for believing in me, and for keeping my spirits up when times were tough.

There's always a little part of me that's forever in both the US and Russia after my time spent working and studying in these two amazing countries. I feel very fortunate to have had the opportunity to spend time these past five years with Olga, Annemarie and Sergei and to continue learning and reflecting on how my time in California, St. Petersburg and the Caucasus has enriched me. I must also express my gratitude to Dr. Susi Levi-Sanchez and Dr. Azita Ranjbar for their encouraging me to pursue further my academic interests whilst we worked together in Dushanbe, Tajikistan.

While back and forth to Chamonix, France, I've spent a great deal of time on the *autostrada* — and survived! Each time I've made my way back to Florence I've taken time to reflect on just how lucky I've been to have the support of my closest friends in the Alps; Emma Walton, Solange Bertholin Gonzales, Cris Nakano, Yvonne Robertson, Kimberly Van Landingham and Mark Gear. I am very grateful to Professor Alice Henderson, who always seemed intuitively to know when best to drop me a line, to offer great advice, and to motivate me to continue with my academic endeavours. A special mention needs also be made for Neil Brodie, a great friend, who has proved so incredibly generous and supportive over the years. I wish also to thank my dear friends Colin Samuels, Anna Selberg, Violeta Radeckaite, Vanessa Francois and Cristina Marzullo for their support and encouragement during my doctoral studies.

Before my interview in Florence at the EUI for the PhD programme I'd never imagined actually living in Italy. Now, as I complete my studies, I cannot imagine a life without Italy. My time here has taught me so much, and I have met so many inspiring, warm, kind and generous people in Florence and across the country. In particular, I must express my heartfelt thanks to Eva Montanari, Cristina and Omar Mosconi, and to the Gracz family. Eva, Cristina, Omar and the Gracz family were always so welcoming, compassionate and understanding — thank you so much for all you have done for me during my time in Italy.

Finally, a special mention needs be made for Molly, and to my mother, Angela. Both have stuck by me through the all the tough times, and have been incredibly (sometimes perhaps too!) patient with me. I cannot express in words how truly lucky I am to have them in my life. Their love and support means so much to me.

Chapter 1: Introduction

1. Human mobility and technologies: a brief introduction

Our everyday lives are increasingly subject to the influence of technologies that inhere capabilities to track and trace both individual citizens and groups, and to determine interactions and transactions in ever more minute detail.¹ Personal devices such as mobile phones with embedded sensing are becoming ubiquitous², and by incorporating sensing into personal mobile devices a diverse range of potent applications are being created that exploit real-time detection and the monitoring of physical location.³ Moreover, where mobile communications technologies facilitate a multitude of different tasks and functions in society, localisation of the individual is an intrinsic factor in the delivery of information services.⁴ However, whilst many of these services have proven beneficial and highly popular, location data collection and processing may furnish information beyond the immediately discernible trace of an

¹ Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge: Polity. p.12. *See also*: Kitchin, R., 2014. The real-time city? Big data and smart urbanism. *GeoJournal*, 79(1), p.11

² In this context Greenfield makes a particularly salient assertion in affirming that the personal device “is no longer an augmentation but a necessity... the smartphone is becoming a *de facto* necessity, it is at the same time impossible to use the device as intended without, in turn, surrendering data to it and the network beyond.” Greenfield, A. (2017). *A Sociology of the Smartphone*, in ‘Radical Technologies: The Design of Everyday Life’. Verso Books. Available at: <https://longreads.com/2017/06/13/a-sociology-of-the-smartphone/>.

³ Collectively, mobile phones represent a powerful tool with which to study large-scale population dynamics on a global scale, revealing the basic patterns of human movement and mood rhythms. The US National Institute of Health notes: “almost three quarters of adults in developed countries and half of adults in developing economies carry a smartphone.” *See*: NIH, “Smartphone data used in global study of physical activity: Large-scale study reveals targets for obesity prevention, wisdom of walkable communities.” *Science Daily*, 10 July 2017. Available at: www.sciencedaily.com/releases/2017/07/170710113613.htm. *See also*: Tim Althoff, Rok Sosič, Jennifer L. Hicks, Abby C. King, Scott L. Delp, Jure Leskovec. Large-scale physical activity data reveal worldwide activity inequality. *Nature*, 2017; DOI: 10.1038/nature23018; Klasnja, P., Consolvo, S., Choudhury, T., Beckwith, R. and Hightower, J., 2009. Exploring privacy concerns about personal sensing. *Pervasive Computing*, pp.176-183. Available at: http://aiweb.cs.washington.edu/research/projects/aiweb/media/papers/Klasnja_et_al_2009_-_Exploring_privacy_concerns_about_personal_sensing.pdf, p.176

⁴ Danezis et al note that location information is a set of data “describing an individual’s location over a period of time. The time and location resolution vary with the technology used to collect the data.” Danezis, G., Lewis, S. and Anderson, R.J., 2005, June. How much is location privacy worth?. In *WEIS* (Vol. 5), p.2

individual's mobility: aspects of a citizen's behaviour and associations that include their personal interests, relationships and activities may be determined through increasingly complex personal data processing techniques.⁵

Furthermore, the development of the 'Internet of Things' (IoT)⁶ and aligned functionalities intrinsic to ubiquitous computing foresee the extension of ever more pervasive location monitoring capabilities.⁷ Forecasts that IoT heralds an era of omnipresent sensing and surveillance reflect the possibility of a wholesale explosion in the growth of both the spatial scope and temporal coverage of the capability to monitor citizens' movements.⁸ In addition, research on embedded sensors' collection of location data and other personal data in relation to an individual's activity has further driven development of biometrics that infer intimate aspects of a person's physiology related to mobility.⁹ The more widespread sensing of people's movement,

⁵ Strandburg notes in this regard that: "The exploding availability of traffic data is a by-product of modern communication technologies, social practices that increasingly rely on communication carried by intermediaries... The era when most communications and associations were shielded by practical obscurity is over." See: Strandburg, K.J., 2007. Surveillance of emergent associations: Freedom of association in a network society. *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications, Boca Raton, pp.435-459, p.438. Furthermore, Onnela et al note that whilst social communities have been studied for a long time it has only recently become feasible, through the analysis of mobile phone data, to monitor the social interactions and geographic positions of individuals. See: Onnela, J.P., Arbesman, S., González, M.C., Barabási, A.L. and Christakis, N.A., 2011. Geographic constraints on social network groups. *PLoS one*, 6(4), p.e16939. Available at: <http://journals.plos.org/plosone>. See also: Srivatsa, M. and Hicks, M., 2012, October. De-anonymizing mobility traces: Using social network as a side-channel. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 628-637). ACM. Similarly, Pentland and Heibeck assert that "... [with] these new instruments, we have the ability to look past cultural and psychological biases and presuppositions to see ourselves from a new perspective." See: Pentland, A. and Heibeck, T., 2010. *Honest signals: how they shape our world*. MIT press, p.84

⁶ The CASAGRAS Project defined the Internet of Things as: "a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments... These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability." See: EU Commission, Factsheet on privacy, data protection and information security, March 2013, Available at: http://ec.europa.eu/information_society/newsroom, p.1. See also: EDPS, Internet of things: ubiquitous monitoring in space and time, European Privacy and Data Protection Commissioners' Conference Prague, Czech Republic, 29 April 2010, Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Internet_Things_EN.pdf

⁷ See: Peppet, S.R., 2014. Regulating the Internet of things: first steps toward managing discrimination, privacy, security and consent. *Tex. L. Rev.*, 93, p.89

⁸ Langheinrich, M., 2002, October. Privacy invasions in ubiquitous computing. In *Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing. UbiComp*. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.6.6743&rep=rep1&type=pdf>, p.4

⁹ See, for example: Muhammad Shoaib et al., *Towards Physical Activity Recognition Using Smartphone Sensors*, in UIC-ATC 2013: PROCEEDINGS OF 2013 IEEE 10TH INTERNATIONAL CONFERENCE ON UBIQUITOUS INTELLIGENCE & COMPUTING AND 2013 IEEE 10TH

coupled with notable advancements in analytical capabilities rendered by enhanced data processing techniques including data mining of large datasets, presage significant challenges for the information society.¹⁰

Moreover, interest in location data and mobile sensing has been further piqued by the findings of research indicating that insight furnished by data processing evidences immense potential for a diverse range of purposes including the monitoring of urban dynamics, public transportation networks, and the enabling of more nuanced personal and contextual services on the individual level.¹¹ Analysts increasingly predict that information and communication technologies (ICTs) will exert a growing and pervasive influence on the development of infrastructure and the management of aligned economic activities in urban centres.¹² In particular, much of the enticing promise of ‘smart cities’ in terms of socio-economic improvements by way of delivering more secure, livable and functional urban environments for citizens has been premised upon the notion that location awareness will prove intrinsic to developing the next generation of ICTs.¹³ In turn, public authorities, national

INTERNATIONAL CONFERENCE ON AUTONOMIC & TRUSTED COMPUTING 80, 80 (2013) (analyzing how a smartphone’s accelerometer, gyroscope, and magnetometer can be used to collect data about a user’s physical activities). *See also*: Alvina Anjum & Muhammad U. Ilyas, *Activity Recognition Using Smartphone Sensors*, in 2013 IEEE CONSUMER COMMUNICATIONS AND NETWORKING CONFERENCE (CCNC) 914, 918–19 (2013).

¹⁰ See, for example, Cohen’s discussion of the relationship between networked information technologies and their propensity to shape and configure those using such systems: Cohen, J. E. (2012). *Configuring the Networked Self*. New Haven: Yale University Press. *See also*: Ohm, P., (2014). Changing the rules: general principles for data use and analysis. In J. Lane, V. Stodder, S. Bender & H. Nissenbaum (Eds.), *Privacy, Big Data and the Public Good* (pp. 96-75) New York: Cambridge University Press., pp.96-122; Klasnja, P., Consolvo, S., Choudhury, T., Beckwith, R. and Hightower, J., 2009. Exploring privacy concerns about personal sensing. *Pervasive Computing*, pp.176-183. Available at:

http://aiweb.cs.washington.edu/research/projects/aiweb/media/papers/Klasnja_et_al_2009_-_Exploring_privacy_concerns_about_personal_sensing.pdf; Zuboff, S., 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), pp.75-89. Available at: <https://cryptome.org/2015/07/big-other.pdf>.

¹¹ For example, Gonzalez *et al* note that human mobility patterns have been exploited in the development of urban planning and traffic forecasting. *See*: M.Gonzalez, C. Hidalgo, and A.-L. Barabasi. Understanding individual human mobility patterns. *Nature*, 453:779–782, 2008. *See also*: Cheng, X., Fang, L., Hong, X. and Yang, L., 2017. Exploiting mobile big data: Sources, features, and applications. *IEEE Network*, 31(1), pp.72-79. .p.72.

¹² *See, for example*: Kitchin, R., 2014. The real-time city? Big data and smart urbanism. *GeoJournal*, 79(1), pp.1-14. *See also*: Camp, J. and Chien, Y.T., 2000. The Internet as public space: concepts, issues, and implications in public policy. *ACM SIGCAS Computers and Society*, 30(3), pp.13-19.

¹³ Pioneering research by Althoff *et al* has highlighted how data science and modelling may allow the harnessing and analyzing of personalized data from our phones and wearable devices to study human movement, which may in turn influence public authorities’ decision making in respect of security and environmental considerations relating to improving infrastructure and public facilities. *See*: Tim

governments and regional entities such as the European Union have progressively engaged in allocating greater resources to study the possible uses of new technologies enhanced by the collection and processing of location data from communications networks.¹⁴ Strategy studies have also highlighted how future policy interventions and management decisions relating to the operation of vital infrastructure will in part be shaped by contextualisation and analyses derived from the mapping of individuals' mobility patterns across metropolitan spaces.¹⁵

Potentially, the same technological advances rendering these more networked, interconnected communities can also afford greater scope for our understanding of the complexity these developments yield.¹⁶ However, this same complexity also portends the growth of expansive sociotechnical systems that may prove increasingly challenging to comprehend and, in turn, manage and control effectively in consideration of the wider democratic interests of society.¹⁷ Whilst governments, public authorities and other agencies may eagerly anticipate the considerable opportunities to understand with increasing spatial and temporal resolution the utilisation of public facilities and structures by citizens, at the same time important questions surface as to suitability of the existing regulatory and legal frameworks to

Althoff, Rok Sosič, Jennifer L. Hicks, Abby C. King, Scott L. Delp, Jure Leskovec. Large-scale physical activity data reveal worldwide activity inequality. *Nature*, 2017; DOI: 10.1038/nature23018.

¹⁴ See, for example: Kourtit, K., Nijkamp, P., & Arribas-Bel, D. (2012). Smart cities perspective—A comparative European study by means of self-organizing maps. *Innovation*, 25(2), 229–246; Townsend, A. (2013). *Smart cities: Big data, civic hackers, and the quest for a new utopia*. New York: W.W. Norton & Co. See also: Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., et al. (2012). Smart cities of the future. *European Physical Journal Special Topics*, 214(1), 481–518;

¹⁵ Constantiou, I.D. and Kallinikos, J., 2015. New games, new rules: big data and the changing context of strategy. *Journal of Information Technology*, 30(1), pp.44-57.

¹⁶ See: Geoffrey West, Big Data Needs a Big Theory to Go with it, *SCIENTIFIC AMERICAN*, May 1, 2013 (“The digital revolution is driving much of the increasing complexity and pace of life we are now seeing, but this technology also presents an opportunity.”). See also: Felin, T., Devins, C., Kauffman, S. and Koppl, R., 2017. THE LAW AND BIG DATA. *Cornell Journal of Law and Public Policy*. Available at: <http://eureka.sbs.ox.ac.uk/6367/>, p.8

¹⁷ Indeed, Verbeek has asserted that networked information communications technologies “...shape and mediate our relationship with the world around us and, over time, we come to perceive the world through the lenses that our artifacts create.” Verbeek, P.-P. (2006). *Materializing Morality: Design Ethics and Technological Mediation*. *Science Technology & Human Values*, 31, p. 361. See also Marx's discussion of the historical challenges technologies have posed in shaping societies and cultures in: Marx L., *Technology - The Emergence of a Hazardous Concept*, *Technology and Culture*, Volume 51, Number 3, July 2010, pp. 561-577. See further: Martin Heidegger, *The Question Concerning Technology and Other Essays*, trans. William Lovett (New York, 1977); Koonin, S.E. and Holland, M., 2014. The value of big data for urban science. In J. Lane, V. Stodder, S. Bender & H. Nissenbaum (Eds.), *Privacy, Big Data and the Public Good* (pp. 137-158) New York: Cambridge University Press.

oversee the augmentation in surveillance inhered in this nascent exploitation of enhanced monitoring capability. Illustrating this concern, for example, is the call by computer scientists such as Pentland to examine what types of new regulatory instruments are required to deal with the data processing capability coined by the term “reality mining”, whereby the analysis of mobile communications is discerned to render information that shall dramatically improve society where it measures the effectiveness of various government programmes, and improves the transparency and accountability of government.¹⁸

In the courts, legal proceedings increasingly deliberate how information technologies question the cogency of normative precepts framing private life and the social construction of space. The US Supreme Court is to hear the case *Carpenter v. United States*,¹⁹ in which a principal question concerns how far the reach of the Fourth Amendment should extend to safeguarding a person’s electronic devices. The case shall in part review how network cell site data differs from GPS location data, which was prominent in the earlier case *United States v. Jones*.²⁰ In *Jones*, Justice Sotomayor recognised the privacy interests relative to a person’s specific location: “GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”²¹ Moreover, in *Riley v. California*, Chief Justice Roberts Jr. opined that mobile phones are “...now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”²² The prevalence of late of such cases being considered in the highest courts reflects the importance of the issues being considered in relation to the collection and processing of location data, and also the necessity of law keeping track of technological change. Further cases to be heard in US courts, yet also pertinent to the European setting, will shortly rule on mobile device applications that challenge concerns vis-à-vis locational privacy: *Marder v. Niantic Inc.* and *Dodich v. Niantic Inc.* will both in due course examine the issues pertaining to our

¹⁸ Pentland, A. (2009). Reality mining of mobile communications: Toward a new deal on data, in ‘The Global Information Technology Report’, World Economic Forum & INSEAD, p.79

¹⁹ 16-402 *Carpenter v. United States*. Docket file of the pending case available at: <https://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/16-402.htm>

²⁰ *United States v. Jones*, 132 S.Ct. 945 (2012)

²¹ See: JUSTICE SOTOMAYOR, Concurring Opinion, *United States v. Jones*, 132 S.Ct.945 (2012),p.3

²² *Riley v. California*, 134 S.Ct. 2473 (2014)

physical, real-world environment where digital elements are transposed into both notionally public and private locations by way of users' location-aware mobile devices.²³ The above-cited cases highlight the pertinency and timeliness of this research in deliberating the normative and regulatory challenges that arise from an increasing use of, and indeed dependence on, location data in many different aspects of our daily lives.

Anticipation of concerns relating to the possible interferences into the fundamental rights of citizens must also be considered in the light of the topicality of surveillance as a broader issue. Scholarship on technologies has in recent times underscored the propensity of surveillance to subject a greater number of persons and spaces to monitoring.²⁴ Enquiry has also highlighted the growing importance of our examining the relevance of location and mobility to citizens' perception of how privacy relates to formulations of autonomy and personal identity.²⁵ An understanding of human mobility is more central to our wider comprehension of what makes us unique as individuals; and yet, to date, mobility as a subject has remained relatively intangible, elusive and under-theorized an object of study.²⁶

Just as mobility has been spared examination, so too has its inherent connection with the notion of location privacy. Historically, location was a little scrutinized aspect of

²³ *Marder v. Niantic Inc.*, 16-cv-04300, U.S. District Court, Northern District of California (Oakland); *Dodich v. Niantic Inc.*, 16-cv-04556, U.S. District Court, Northern District of California (San Francisco). At question is how augmented reality (AR) objects engage real world concerns including, *inter alia*, the possible extension of property rights to any geo-locative, intellectual property elements that may be placed in it, and interferences into private life stemming from an intrusion by another party. The *Pokémon Go* application is also available in Europe. See: *Pokémon Go - Explore!* 2017, Available at: <http://www.pokemongo.com/>

²⁴ Galič, M., Timan, T. and Koops, B.J., 2016. Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology*, pp.9-37, p.10. See also: Camp, L.J. and Connelly, K., 2008. Beyond consent: privacy in ubiquitous computing (UbiComp). *Digital privacy: Theory, technologies, and practices*, pp.327-343; Kosinski, M., Stillwell, D.J. & Graepel, T. (2013) Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences (PNAS)*, 2013.

²⁵ Rouvory and Pullet, for example, affirm that informational self-determination implies that an individual must be in a position to exercise control over the data that are available about him/her and, in particular, the implications of the use of those data. See: Rouvory, A.; Poulet, Y. (2009), "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy," in: *Reinventing Data Protection*, S. Gutwirth et al. (eds.), p. 51.

²⁶ Indeed, Cresswell asserts in this respect that mobility must be more deeply scrutinized for "...study it we must for mobility is central to what it is to be human. It is a fundamental geographical facet of existence and, as such, provides a rich terrain from which narratives - and, indeed, ideologies - can be, and have been, constructed." Cresswell, T., 2006. *On the move: Mobility in the modern western world*. Taylor & Francis., p.1

privacy, due primarily to the relative scarcity of information relating to our patterns of movement.²⁷ However, the exponential growth in the availability of reliable location sensing technologies has pushed the questions raised by their implementation to the fore.²⁸ As advances in technology and the availability of monitoring have placed the attributes of mobility and location in focus, so too have concerns pertaining to spatial considerations also been subject to greater scrutiny.²⁹ The development of functionality that exploits personal location data allows for the quantification and appraisal of individual characteristics within an explicitly spatial context.³⁰ Heretofore, the role of locality in relation to autonomy, social formation, and organisation between peers and other aspects of associative behaviour has been limited: the study of both individual self-determination and the formation of interpersonal relations has largely been aspatial.³¹ The increasing availability of location data clearly affords scope, therefore, for greater theorization of the role performed by space in the constitution of rights-based concerns such as privacy. Indeed, the inherent complexity of conceptualizing the questions that arise from the consideration of locality in relation to the individual is rendered all the more vexing where spaces themselves may be seen as subtly evolving layers of context and practices that actively influence and shape social relations.³²

²⁷ See: Krumm, J., 2009. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6), pp.391-399.

²⁸ Kosinski et al assert that: "...the widespread availability of extensive records of individual behavior, together with the desire to learn more about customers and citizens, presents serious challenges related to privacy and data ownership." Kosinski, M., Stillwell, D.J. & Graepel, T. (2013), Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences (PNAS)*, 2013., p.1. See also: Ardagna, C.A., Cremonini, M., Damiani, E., di Vimercati, S.D.C. and Samarati, P., 2007. Privacy-enhanced location services information. *Digital Privacy: Theory, Technologies and Practices*, pp.307-326. , p.313.

²⁹ Zhang, for example, has underscored that as "...access to spatial data and spatial analytic approaches advances, so does the need to address sources of bias... the data are assumed to be reliable and free of measurement errors. But in practice, this is often not the case. Measurement errors can affect the data through several mechanisms and many different stages of data collection and analysis...". Zhang, Z., Manjourides, J., Cohen, T., Hu, Y. and Jiang, Q., 2016. Spatial measurement errors in the field of spatial epidemiology. *International Journal of Health Geographics*, 15(1), p.21. Available at: <https://ij-healthgeographics.biomedcentral.com/articles/10.1186/s12942-016-0049-5>, p.21. See also: Rainham D, Krewski D, McDowell I, Sawada M, Liekens B. Development of a wearable global positioning system for place and health research. *Int J Health Geogr*. 2008;7:59.

³⁰ See, for example: Duckham, M. and Kulik, L., Location privacy and location-aware computing. In Drummond, J., Billen, R., and Joao, E., Eds., *Dynamic and Mobile GIS: Investigating Change in Space and Time*, Taylor & Francis, Boca Raton, FL, 2007.

³¹ Kitchin, R. and Dodge, M., 2011. *Code/space: Software and everyday life*. MIT Press. , p.13

³² Refer to, for example, Kitchen and Dodge's discussion of the role played by public and private spaces in relation to their intersection with software and the creation of new spatialities of everyday life and new modes of governance and creativity: Kitchin, R. and Dodge, M., 2011. *Code/space: Software and everyday life*. MIT Press. , pp.12-14

Significant resources have been invested in the field of computer science to further explore and develop information technology based upon location and temporal awareness capabilities.³³ In contrast, however, the discourse amongst lawyers, ethicists and policy makers has lagged. In particular, dialogue concerning the appropriacy and efficacy of the legal framework to appreciate and effectively regulate innovations in the tracking of human mobility has to date been relatively limited. In essence, understanding of the interconnectedness of location with mobility and our apprehension of the value of the spaces we inhabit and move within relative to our conceptualisation of fundamental rights remains decidedly underdeveloped. Furthermore, at issue is how location-aware information technology will influence the interrelationship of the different fundamental rights affected, such as privacy, the right to the protection of personal data, freedom of movement and freedom of assembly and association.

With technologies becoming increasingly context-aware in respect of the intrinsic value of centering sensing and monitoring capabilities of the immediate environment, the need to ascertain whether the established premises that underpin current conceptual approaches to location data collection and processing remain tenable is thus ever more acute. The study of the utilisation of location data is of additional value for the insight it may provide in relation to broader, extant issues pertinent to data protection and privacy rights currently. Particularly as regards data protection, a focus on the transformation of the collection and processing of location data may furnish insight that proves transferable in respect of more extensive concerns relating to our understanding of the evolution of the conceptualisation of metadata.

1.1 Framing the role of location in relation to privacy

Differences in the perceptions of privacy might appear to intimate that the concept remains intrinsically nebulous. Scholars such as Solove have addressed the apparent

³³ Zang and Bolot having noted, for example: "...Cell phones have become a powerful tool to analyze human behavior, in particular as it relates to physical places through the study of mobility patterns, and the research interest in this area has increased dramatically over the past few years." *See*: Zang, H. and Bolot, J., 2011, September. Anonymization of location data does not work: A large-scale measurement study. In Proceedings of the 17th annual international conference on Mobile computing and networking (pp. 145-156). ACM.

perplexity of framing privacy as a notion with the contention that it simply “means different things to different people.”³⁴ It may be observed that efforts to construe privacy adopt quite divergent, even possibly contradictory approaches.³⁵ Conversely, other scholars have asserted that one should avoid framing privacy in too rigid an elucidation by attempting to discern its contours. The pioneering work of Gary Marx has frequently framed privacy as being indeterminate, proposing a relatively indefinite formulation: “a family of concepts encompassing personal information.”³⁶

Locational privacy constitutes a specific facet of privacy and, whilst the concept of locational privacy is not in itself new, its newly acquired significance stems from recent developments in technologies: our mobility is increasingly mediated and

³⁴Solove in effect argues that we should be less concerned with defining privacy; rather, we would do better in analysing “the specific activities that pose privacy problems”. *See*: Solove, Daniel J., *Understanding Privacy*. Daniel J. Solove, *Understanding Privacy*, Harvard University Press, May 2008; GWU Legal Studies Research Paper No. 420; GWU Law School Public Law Research Paper No. 420. Available at: <http://ssrn.com/abstract=1127888>, p.9 (Solove states that: “There is no overarching conception of privacy...”). Similarly, Post declares: “Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all” *See*: Post, Robert C., “Three Concepts of Privacy”, *The Georgetown Law Journal*, Vol. 89, No. 2001, p. 2087. Jutand, in contrast, asserts that: “Privacy is a cultural concept whose definition is connected to social rules establishing what is private or not.” *See*: Jutand F., ‘The Challenges of Privacy’, in *The Futures of Privacy*, Carine Dartiguepeyrou (ed.), February 2014, Available at: <https://cvpip.wp.mines-telecom.fr/>, p.7. On this note we may also consider the concepts explored by Dwork and Roth in their related work on developing the notion of ‘differential privacy’, in which they underscore the vital importance of our considering the different value that individuals in our society may place on their own respective privacy right, noting: “The final, more insidious obstacle, is that an individual’s cost for privacy loss may be highly correlated with his private data itself!” *See*: C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*, *Foundations and Trends in Theoretical Computer Science* Vol. 9, Nos. 3-4 (2014), pp.211-407, Available at: <https://www.cis.upenn.edu/~aaroht/Papers/privacybook.pdf>, p.10. In contrast, privacy scholar Richard Posner adopts an especially insistent and cynical standpoint as regards the notion of privacy, positing that efforts to protect privacy be framed as principally signifying a desire on behalf of the individual to safeguard his secrecy “...in the interest of concealing personal information about oneself.” Interestingly, Posner nonetheless discerns possible motives as to why one may wish to avoid disclosure, and acknowledges a plausible justification for such apprehension: “But I need to distinguish between a person’s pure interest in concealment of personal information and his instrumental interest, which is based on fear that the information will be used against him.” *See*: Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 251 (2008), p.245. Waelbroeck describes privacy simply as the “personal information that identifies the preferences of a person.” *See*: Waelbroeck P. *An Economist’s Thoughts on the Future of Privacy*, in *The Futures of Privacy* (Editor -Carine Dartiguepeyrou), Fondation Télécom, Institut Mines-Télécom, February 2014, p.131

³⁵Parker, for example, asserts that privacy is defined as “[C]ontrol over when and by whom the various parts of us can be sensed by others.” *See*: Richard B. Parker, “A Definition of Privacy,” *Rutgers Law Review* 27 (1974), p.281. *See also*, in contrast, Westin’s discussion of privacy pertaining to the notion of ‘information privacy’, whereby the scholar defines privacy as the claim of an individual to determine what information about himself or herself should be known to others; *See*: Westin A. F., *Privacy and Freedom*, New York: Atheneum, 1967.

³⁶Gary T. Marx & Glenn W. Muschert, *Personal Information, Borders, and the New Surveillance Studies*, *Annual Review of Law and Social Science*, December 2007, p.375

facilitated through them.³⁷ As citizens we are developing more detailed registers of activities linked to our movements through the collection and processing of personal data.³⁸ To date there has been little examination, particularly in Europe, of why locational privacy matters, and as to whether this specific aspect of a broader right to privacy might require distinct protective safeguards.³⁹ Scholarship has focused primarily on whether the monitoring of movements may impede the formation of respective individual identities has been subject to extensive examination.⁴⁰ Locational privacy has also been justified on the basis that it enables citizens to avail themselves of opportunities to circulate and communicate with others in different spaces, which also safeguards vital social processes dependent upon these

³⁷ *See, for example:* Jerome E. Dobson & Peter F. Fisher, 'Geoslavery,' IEEE Tech. and Society Magazine (Spring 2003), pp.48-52. Moreover, Shokri et al affirm the importance of understanding the broader impact of location data collection and processing, whereby "a trace is not only a set of positions on a map. The contextual information attached to a trace tells much about the individuals' habits, interests, activities, and relationships: ... the negative side-effects of insufficient location privacy are becoming more and more threatening." R. Shokri, G. Theodorakopoulos, J. Y. Le Boudec and J. P. Hubaux, "Quantifying Location Privacy," Security and Privacy (SP), 2011 IEEE Symposium on, Berkeley, CA, 2011, p. 247

³⁸ Bridwell's research, for instance, has highlighted how the growth of ubiquitous location sensing prompts serious concerns for individual location privacy. *See:* Bridwell S. A., The dimensions of locational privacy, in *Societies and Cities in the Age of Instant Access*, pp. 209-225. *See also:* Crang, M. and Graham, S. (2007) 'Sentient cities: ambient intelligence and the politics of urban space', *Information, Communication Society*, 10 (6), p.816. Refer also to Schulhofer's discussion of spheres of privacy, in which he notes how, conveniently, in the past physical facts on the ground "typically afforded a refuge, often a better one than the legal rights conferred by statutes and constitutions. Records could be hidden in drawers or under floor boards; walls were opaque." *See:* Schulhofer, Stephen J., "An International Right to Privacy? Be Careful What You Wish For" (2015). New York University Public Law and Legal Theory Working Papers. Paper 508. Available at: http://lsr.nellco.org/nyu_plltwp/508.

³⁹ In contrast, in North America scholarship has focused on the impact of novel forms of surveillance of the monitoring of citizens' movements. *See, for example:* Solove, Daniel J., *Reconstructing Electronic Surveillance Law*. *George Washington Law Review*, Vol. 72, 2004, p.1708 Available at: <http://ssrn.com/abstract=445180>. The work of Uteck too has reviewed in detail the possible impact of location monitoring, and has expressed the consternation that such surveillance could deflect a genuine sea change in the extent to which monitoring of our movements could permeate a society. This pervasiveness surveillance could, it is surmised, provoke unwelcome influences that engender subtle changes in our behavior, in turn proving disruptive to social interaction. *See:* Uteck, Anne, *Ubiquitous Computing And Spatial Privacy* (March, 2009), p.89, *Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society*, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/799

⁴⁰ Wider-ranging concerns expressed by Novotny and Spiekermann have highlighted how developments in personal data processing may present risks to the fundamental rights of citizens: "Personal information is also the core of two facets that constitute humanity: identity and dignity... as more personal information is collected, used, packaged, and leveraged, more conflict arises around how people can retain control of their identities and protect their dignity." *See:* Novotny, Alexander and Spiekermann, Sarah, *Personal Information Markets and Privacy: A New Model to Solve the Controversy* (August 15, 2012). *WI'2013*, Leipzig. Available at: <http://ssrn.com/abstract=2148885> or <http://dx.doi.org/10.2139/ssrn.2148885>, p.1

interactions.⁴¹ The linkage made between privacy, human relationships, intimacy and the development that supports decisional autonomy has constituted an important area of study for the analysis of the specific performative function of location.⁴² Solove's scholarship on surveillance has underscored how observation may promote anxieties connected to personal interactions with other parties, which may be misunderstood whilst associative behaviours could also be misinterpreted.⁴³ Hildebrandt has focused on the extent to which interferences might render changes to the individual's mental state (in respect of the sense of seclusion, for example).⁴⁴ The effects indeed require further examination so that we might determine their relationship, and value, to locational privacy.⁴⁵ Authors such as Cohen, Gutwirth and Patterson have all examined individual autonomy and it being inherently contingent upon a sense of seclusion and selective isolation.⁴⁶ Paradoxically, however, other authors have written

⁴¹ This duality recalls the incisive observation of Brandeis argued in *Whitney*, whereby liberty must be valued "both as an end and as a means". *Whitney v. California* (No. 3), 274 U.S. 357

⁴² In both law and computer science, research has emphasized the extent to which we enact our identity by way of the selective preferences we exercise in the situational and spatial relationships within our respective environments. This elucidation of location privacy conjoins our ability to move freely with the formation of identity, and assimilates both a spatial and informational dimension. *See, for example:* Phillips, David J., *Ubiquitous Computing, Spatiality, And The Construction Of Identity Directions For Policy Response* (March, 2009). *Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society*, New York: Oxford University Press, 2009, pp. 306- 308, Available at: idtrail.org/content/view/full/799. Regarding the relationship of identity formation to privacy, see for example: Rorty, A., *The identities of persons*. Vol. 3. Univ of California Press, 1976; Ricoeur, P., 1992, *Oneself as another*, University of Chicago Press; FIDIS - Future of Identity in the Information Society, "D7.4: Implications of profiling practices on democracy and rule of law", 5 September 2005, Available at: <http://www.fidis.net/resources/fidis-deliverables/profiling>, pp.36-38.

⁴³ *See:* Solove, Daniel J., *Reconstructing Electronic Surveillance Law*. *George Washington Law Review*, Vol. 72, 2004, p.1708 Available at: <http://ssrn.com/abstract=445180> or <http://dx.doi.org/10.2139/ssrn.445180>.

⁴⁴ Hildebrandt et al contend that, more broadly, human rights enable the creation of a "sphere of individual autonomy or self-determination and in doing so, they protect individuals against excessive steering of their lives and doings; they contribute to the creation of the private sphere." *See:* FIDIS - Future of Identity in the Information Society, "D7.4: Implications of profiling practices on democracy and rule of law", 5 September 2005, Available at: <http://www.fidis.net/resources/fidis-deliverables/profiling>, p.13. Refer also to Berlin's extensive articulation of the function of human rights in constituting the notion of 'negative freedom' - as freedom from interference; *See:* Berlin I., *Two Concepts of Liberty* in *Four Essays on Liberty*, Oxford University Press, Oxford, 1969, pp. 118-173. Taylor has asserted that autonomy relates to an individual's integrity and identity, and the ability to exercise agency in defining one's own behaviour and persona; Taylor, Charles. 1976. "Responsibility for Self." pp. 281-301 in *The Identities of Persons*, edited by A. Oksenberg Rorty. Berkeley: University of California Press. For further discussion of the concept of the right to privacy *vis-à-vis* identity, see also: Hildebrandt, M., 2005, "Privacy and Identity" in *Privacy and the Criminal Law*, edited by E. Claes, A. Duff, and S. Gutwirth. Leuven: Intersentia.

⁴⁵ Indeed, Maklem has underscored the universal value of seclusion to our need for self-development, noting: "Isolation is the source of human difference, for it is the exercise of creativity in isolation that makes it possible for people to reach different consolations and thereby develop different ways of life." Macklem T., *Independence of Mind*, Oxford University Press, Oxford (2006), p.56

⁴⁶ *See:* Cohen, Julie E., *Examined Lives: Informational Privacy and the Subject as Object*. Georgetown Public Law Research Paper No. 233597. Available at: <http://ssrn.com/abstract=233597>, p.1423. *See*

that a level of outside scrutiny and interference is also necessary to stimulate and coax introspection and thereby nurture our own identities.⁴⁷ Koops and Leenes have cited privacy as facilitating civility, stability, pluralism, and democracy as central values. In contrast, renouncing an aspect of one's private sphere and disclosing personal data may also favour important societal values.⁴⁸

Also pertinent to the discussion is the nature of physical spaces. In privacy law, physical space has been characterized by an elementary dichotomy whereby space is considered either 'private' or 'public'.⁴⁹ Research in fields such as behavioural

also: Rigaux F., *La protection de la vie privée et des autres biens de la personnalité*, Paris/Bruxelles, Bruylant/LGDJ, 1990, p.849; Gutwirth S., *Privacy and the Information Age*, Lanham, Rowman & Littlefield Publishers, 2002, p.158; *See also:* Patterson D., *Privacy in Ubiquitous Computing*, 2009, Available at: http://www.ics.uci.edu/~djp3/classes/2012_09_INF241/Lectures/Lecture18Slides.pdf. The European Parliament's LIBE Committee noted that: "Having a physical place where one can be left alone as a free human being is a crucial component in democratic societies". Moreover, it noted that a "similar zone of non-interference in the digital world would thereby be legitimate as everyday life becomes increasingly digitized." *See:* IPTS, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)*, July 2003, European Commission Joint Research Centre (DG JRC), Available at: <http://www.jrc.es>, p.80.

⁴⁷ Schwartz indeed notes: "... limitations on the processing of personal information are necessary... Such important acts of individual creative imagination require that citizens be able to both to retreat from and participate in social life." *See:* Schwartz, Paul M. *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 *Iowa L. Rev.*, (1994-95), p.560. *See also:* Phillips, David J., *Ubiquitous Computing, Spatiality, And The Construction Of Identity Directions For Policy Response* (March, 2009). *Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society*, New York: Oxford University Press, 2009. Similarly, Arendt indeed warned of "the danger to human existence from the elimination of the private realm", yet championed individual participation in society: "To live an entirely private life means above all to be deprived of things essential to a truly human life." *See:* Arendt, H., *The Human Condition*, University of Chicago Press, Chicago (1958), pp. 58 & 70.

⁴⁸ *See:* Bert-Jaap Koops & Ronald Leenes, 'Code' and the Slow Erosion of Privacy, 12 *Mich. Telecomm. & Tech. L. Rev.* 115 (2005). Available at: <http://repository.law.umich.edu/mttlr/vol12/iss1/3>, p.136.

⁴⁹ Seidman, for example, speaks of the private sphere constituting the diametric opposite to the public nature of government, and within which citizens can freely develop their own individual, personalised relationships. *See:* Seidman L.M., 'Public Principle and Private Choice', *Yale Law Journal*, Vol. 96, 1987, (pp. 1006-1059), p.1026. Palfrey and Gasser's studies have discussed different perceptions of public and private spaces, and how the meaning of this dichotomy continues to evolve with the deployment of new technologies. *See:* J. PALFREY and U. GASSER, *Born digital. Understanding the first generation of digital natives*, 2008, p.58. In contrast, Tene has contended that the private and public dichotomy has been irreversibly transformed, claiming citizens accept location being tracked and broadcast. *See:* Tene, Omer, *Privacy: The New Generations* (November 17, 2010), *International Data Privacy Law*, 2010, Available at: <http://ssrn.com/abstract=1710688>, p.15. Refer also to Gary Marx's discussion of conceptual borders and the capability of comprehensive monitoring to invade public and private spheres: Marx, G.T. (2001) *Murky conceptual waters: the Public and the Private*, *Ethics and Information Technology*, Vol. 3, No. 3, pp. 157-169. Cohen has argued that the safeguard of individual autonomy requires protected spaces that resist a binary choice of privacy as applied to public or private spheres. Kang, in contrast, delineates three groups of privacy rights: informational, decisional and spatial, and contends that spatial rights in respect of privacy determine the individual's physical sphere of control. *See:* Kang, J., 1998. *Information privacy in cyberspace transactions*. *Stanford Law Review*, pp.1202-05. *See:* Cohen J., 2000. *Examined Lives: Informational Privacy and*

psychology has, in contrast, highlighted the complexity of delineating spaces.⁵⁰ Various authors have noted the function seclusion affords in shaping privacy, reflecting on how this phenomenon influences our identities and sense of selfhood.⁵¹ In contrast, Nissenbaum's study of the relationship of context to personal privacy has described our everyday existence as a continual navigation of dichotomies, such that the individual traverses a plurality of distinct realms.⁵² Conversely, other studies emphasize that in accentuating the indeterminate character of space, humans

the Subject as Object, *Stanford Law Review*, p.1373. Markedly, scholars such as Wood and Graham assert that public spaces that were once arenas for popular debate and protest have already been displaced by surveillance, replaced by the obscure topologies of the technologies, the architecture and the code that drives them. *See*: David Wood and Stephen Graham, *Permeable Boundaries in the Software-sorted Society: Surveillance and the Differentiation of Mobility*, Paper for 'Alternative Mobility Futures' Lancaster University, 9-11 January 2004. Available at: <http://www.academia.edu/1069340/>. Lessig also relates the formulation of privacy as being partially contingent on an architecture of technological capability; technology is diversified across spatial and temporal contexts. *See*: Lessig L., *Code and Other Laws of Cyberspace*. 1999. Basic Books, New York, USA, 1999. Refer also to Lederer et al's discussion of the application of a unified model of everyday privacy in ubiquitous computing environments: Lederer, S., Dey, A.K. and Mankoff, J., 2002. A conceptual model and a metaphor of everyday privacy in ubiquitous computing environments. Available at: <http://www.cs.cmu.edu/~io/publications/old-pubs/privacy-techreport02.pdf>.

⁵⁰ Psychologist Irwin Altman framed privacy as an ever-changing process of controlling boundaries conducted between the self and the environment that surrounds. *See*: Altman, Irwin. "The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding." (1975). *See also*: Westin, A (1970), *Privacy and Freedom*, New York.

⁵¹ *See*, for example: Solove, Daniel J., *Reconstructing Electronic Surveillance Law*. *George Washington Law Review*, Vol. 72, 2004, Available at: <http://ssrn.com/abstract=445180> or <http://dx.doi.org/10.2139/ssrn.445180>, in which Solove asserts that: "Freedom is not just the absence of restraints; it is a mental state, a felt reality in both structure and sentiment." *See also*: Richard Jenkins, *Social Identity*, Second Edition, New York: Routledge, 2004. Jenkins describes identity formation as inexorably linked to visibility, determining that it can be construed as being revealed both internally and externally; essentially identity is thus projected outwardly and at the same time is self-imposed. Goffman describes identity as a reflexive process of self-formation. *See*: Erving Goffman, *The Presentation of Self in Everyday Life*, New York: Doubleday, 1959, p.75. *See also*, for example: Millar, Jason, *Core Privacy - A Problem for Predictive Data Mining* (March, 2009), p.117, *Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society*, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/full/799. Bloustein too has noted the detrimental effect of the deprivation of privacy on personal development: Bloustein, E.J., 'Privacy as an Aspect of Human Dignity', in: Ferdinand David Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology*. New York, Cambridge University Press, 1984, p.188.

⁵² Nissenbaum outlines the scope of different spheres, realms and contexts in her elucidation of the precepts that underpin the basis for the social theory of contextual integrity, outlining the function of established norms (implicit, variable and incomplete) that serve to regulate behaviors within distinct social realms that constitute contrastive contexts, domains or institutions. *See*: Nissenbaum, Helen F., *Privacy as Contextual Integrity*. *Washington Law Review*, Vol. 79, No. 1, 2004, pp.137-138, Available at: <http://ssrn.com/abstract=534622>. Refer also to the April 2013 report of the CEPS Digital Forum for its discussion of the potential applicability of contextual integrity in the reconceptualisation of the EU data protection legislation: CEPS, *Online Personal Data Processing and EU Data Protection Reform - Report of the CEPS Digital Forum*, April 2013, Available at: <http://www.ivir.nl/publicaties/download/1350>, pp.56-57. Also pertinent is Alvaro's argument for the adoption of a contextual approach to data protection in the modern age of data processing; Alvaro, A., *Lifecycle Data Protection Management: A contribution on how to adjust European data protection to the needs of the 21st century*, September 2012, p.12.

constantly reinvent their relationship with their surroundings. Such an approach might also apply to the conceptualisation of locational privacy.⁵³

1.2 Location data and the conceptualisation of locational privacy

Whilst the field of locational privacy in relation to public and private spaces has invited significant research from computer scientists in recent years, studies of the associated impacts on real-life problems that concern the normative considerations pertaining to location privacy have been much more limited.⁵⁴ A 2003 study by De Hert and Gutwirth of ubiquitous computing's enablement of pervasive monitoring however sought to question the efficacy of the existing legal framework of European data protection and privacy law.⁵⁵ Indeed, the authors suggested that its effectiveness had already been eroded by developments outwith the legal domain, notably the advancement of technologies such as satellite-based geolocation and data mining, contending that the advent of these and other ICTs have challenged the principles on which the foundations of the legal framework at the European level was established,

⁵³ Harvey, for example, asserts that space cannot be conceived as absolute, relative or relational in itself; rather it is resolved through human practice with respect to it. *See*: Harvey, D., *Social Justice and the City*, London: Edward Arnold (1973), p.13.

⁵⁴ *See*, for example: F. Giannotti & D. Pedreschi, *Mobility, Data Mining and Privacy: A Vision of Convergence*, in *Mobility, Data Mining and Privacy* (2008) F. Giannotti and D. Pedreschi (eds.), Available at: <http://www.mendeley.com/research/privacy-in-data-mining>, pp.9-10. Giannotti and Pedreschi underscore the pertinence of this theme in noting that the nexus of privacy with mobility and data mining constitutes a nascent, expanding and multi-disciplinary research frontier. Uteck's research, in contrast, has explored the interpretation of the scope and parameters of spatial criteria pertaining to our developing a sense of privacy, arguing that the circumstances of our surroundings — interpreted in accordance with given contextual considerations — establish the conditions by which we anticipate protection from intrusive interference, and notes that this expectation is a nuanced, contextual and fundamentally normative exercise. *See*: Uteck, Anne, *Ubiquitous Computing And Spatial Privacy* (March, 2009), p.89, *Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society*, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/full/799. *See also*: Gewin, V., *Mapping opportunities*, *Nature*, January 2004, Available at: <http://dx.doi.org/10.1038/nj6972-376a>; Sui, D. (2011) *Legal and ethical issues of using geospatial technologies in society*, in T. L. Nyerges, H. Couclelis & R. McMaster, 'The SAGE handbook of GIS and society', London: SAGE Publications Ltd, pp. 504-528.

⁵⁵ *See*: Paul De Hert & S. Gutwirth, *Privacy And Data Protection As Distinct Tools And Concepts*, in 'Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)', July 2003, DG JRC, Available at: <http://www.jrc.es>, p.161; *See also*: European Commission Joint Research Centre, *Future bottlenecks in the information society - Report to the European Parliament, Committee on Industry, External Trade, Research and Energy (ITRE)* (2001), Available at: <http://bookshop.europa.eu/en/future-bottlenecks-in-the-information-society-pbLFNA19917/>, pp. 94-119; *See*: Jan Grijpink & Corien Prins, *Digital Anonymity On The Internet: New rules for anonymous electronic transactions?* *Computer Law & Security Review*, Volume 17, Issue 6, 30 November 2001, pp. 379-389.

on the basis of their formulation in an era when technical capabilities were much less advanced.

However, articulating a cogent rationale for the parameters of locational privacy proves complex, not least because our legal reasoning hinges in part on theoretical precepts relating to physical geography. Paradoxically, spatial considerations in particular appear to add a certain intangibility to the notion of locational privacy, rendering it intrinsically more complex and seemingly, in certain instances, irreducible in terms of simple explanations that the layperson may comprehend.⁵⁶ It might appear that a methodical elucidation of the relationship played by spatial characteristics in framing locational privacy presumes we can conceptualize it absent any indeterminacy. Notably, the approach developed to date in accordance with the interpretation of existing precepts concerning privacy and data protection law has tended to render spaces as either ‘public’ or ‘private’, allowing therefore for a relatively orderly delineation of spatial boundaries relating to the degree of privacy they afford.⁵⁷

Comprehension of the challenges locational privacy faces in the advent of new technologies is further complicated by the necessity of resolving the effect of more extensive personal location data collection and processing in meaningful, measurable terms: the risk of interferences in our fundamental rights can only be determined where intrusions are qualified succinctly, and their impact rendered in unambiguous,

⁵⁶ For instance, see De Souza e Silva and Frith’s framing of spatial and social changes in the context of location-aware mobile technologies and their effect on public spaces and locational privacy. *See*: Adriana de Souza e Silva, Jordan Frith, *Mobile interfaces in public spaces: Locational privacy, control, and urban sociability*, Routledge, 2012, pp.50-77.

⁵⁷ The LIBE Committee noted in its 2003 report on security and privacy that: “socio-cultural norms, habits and legal rules provide the guidelines for people’s assessment of what is a private or a public space. The complex interrelationship between what is regarded as public or as private – affected by ICTs and in the future even more by AmI (ambient intelligence) – is inherently related to issues of privacy and security. In the physical world, personal privacy is typically protected both legally and socially by the notions of “domicile” and “residence”. These are carefully developed and recognized concepts that have evolved.” *See*: IPTS, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)*, July 2003, European Commission Joint Research Centre (DG JRC), Available at: <http://www.jrc.es>, p.74. *See also*, for example: Solove, Daniel J., *Understanding Privacy*. Daniel J. Solove, *Understanding Privacy*, Harvard University Press, May 2008; GWU Legal Studies Research Paper No. 420; GWU Law School Public Law Research Paper No. 420. Available at: <http://ssrn.com/abstract=1127888>; Calo, M. Ryan, *The Boundaries of Privacy Harm* (July 16, 2010). *Indiana Law Journal*, Vol. 86, No. 3, 2011, Available at: <http://ssrn.com/abstract=1641487>.

quantifiable terms. Conventionally, the framing of such interferences has been based upon more traditional notions of visibility, which may more easily be understood by the layperson. In contrast, new methods of tracking individuals' locations underscore the salience of novel, non-visual methods of surveillance based on personal location data collection and processing that may be used to discern data subjects' behaviours and preferences. Moreover, besides being largely hidden, covert and, increasingly, unremitting, the acquisition of personal location data is inherently indiscriminate in terms of the scope of the everyday activities monitored.⁵⁸

As early as 2003, De Hert and Gutwirth expressed concern that the legal framework may prove deficient in confronting the nascent threats to privacy and data protection rights of European citizens from the evolution of ICTs toward an increasingly ubiquitous computing environment enabling pervasive monitoring.⁵⁹ In addition, certain scholars have asserted that the robustness of the legal framework of European data protection and privacy law has been eroded by certain developments outwith the legal domain, notably the advancement of technologies such as satellite-based geolocation, data mining and ambient intelligence. It has been said that the advent of these and other ICTs have challenged the principles on which the foundations of the legal framework at the European level were originally established, having been brought into being in the epoch of mainframe computing.⁶⁰ Cases concerning the right to privacy are replete with elucidations as to *how* society must allow for individuals to move unimpeded, exercise their choice to freely interact and benefit from their mobility, but they rarely elucidate in comprehensive terms precisely *why*

⁵⁸ See: Freiwald, Susan, Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact (April 20, 2011). Maryland Law Review, Vol. 70, p. 732.

⁵⁹ See: Paul De Hert & S. Gutwirth, Privacy And Data Protection As Distinct Tools And Concepts, in 'Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)', July 2003, DG JRC, Available at: <http://www.jrc.es>, p.161; See also: European Commission Joint Research Centre, Future bottlenecks in the information society - Report to the European Parliament, Committee on Industry, External Trade, Research and Energy (ITRE) (2001), Available at: <http://bookshop.europa.eu/en/future-bottlenecks-in-the-information-society-pbLFNA19917/>, pp. 94-119; See: Jan Grijpink & Corien Prins, Digital Anonymity On The Internet: New rules for anonymous electronic transactions? Computer Law & Security Review, Volume 17, Issue 6, 30 November 2001, pp. 379-389.

⁶⁰ See, for example: IPTS, Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, European Commission Joint Research Centre (DG JRC), Available at: <http://www.jrc.es>. See also: Prins, C., 'New Rules for Anonymous Electronic Transactions?', J.I.L.T., 2001, 2, p.20; PRINS, C., 'De juridische status van eena recht op anonimiteit', P&I, 2000, 4, pp.153-157.

this liberty is necessary to a democratic society.⁶¹ In part, therefore, a wider concern relates to how existing assessments of established technologies *vis-à-vis* their degree of intrusiveness into fundamental rights such as privacy and personal data protection are apt to be applied to novel technological innovations relating to location data, or indeed whether the degree of originality these new advancements represent essentially challenges such an appraisal. For example, it has been contended that overly simplistic analogies that compare networked mobile devices to fixed line telephones are unsound, based on the premise that they are just too intrinsically dissimilar and invalidate the application of established models of review.⁶² Early research conducted on behalf of the European Parliament in 2003 highlighted concerns amongst experts that the deployment of location tracking technologies were perceived as presenting privacy risks that continued to undermine their diffusion and adoption by the public. Indeed, the initial findings of the LIBE Committee's review underscored the necessity of researching the impacts of the development of location-based services and location computation technologies.⁶³

Whilst anticipating that the implementation of new methods of personal location data collection and processing will have a major beneficial impact for society by providing insight into the underlying relational mobility dynamics of individuals, groups and communities, interestingly, technologists have nonetheless been amongst the most

⁶¹ Refer also, for example, to the following cases of the ECtHR: *Uzun vs. Germany* (no. 35623/05, 2 September 2010), *Liberty and others vs. United Kingdom* (App. No. 58243/00), *Peck vs. United Kingdom* (2003) 36 E.H.R.R. 41.

⁶² See: Freiwald, Susan, Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact (April 20, 2011). Maryland Law Review, Vol. 70, p. 698, 2011; Univ. of San Francisco Law Research Paper No. 2011-10. Freiwald's assertion is based on the premise that the conjunction of communication with mobility creates an entirely new type of data that does not neatly tie to more traditional technologies. Freiwald affirms that it is too simplistic and thus erroneous to assert that location data derived from cellular phone records is not commensurate with content-related data. Rather, such data may be characterized as content in its own right. For example, a user may convey her location to another user essentially as a communication. See also, for example: David M. Berry, The Computational Turn: Thinking About The Digital Humanities, Culture Machine, Vol 12, 2011, pp.12-14, Available at: www.culturemachine.net. Berry asserts that recent breakthroughs in data processing have fundamentally altered traditional modes of analysis, changing profoundly the nature of the information attainable from the personal data collected. Central to Berry's position is the notion that narrative and patterns are interlinked: that the code that allows for the analysis of databases is itself implicitly a form of narrative, thus inhering an element of subjectivity.

⁶³ IPTS, Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, European Commission Joint Research Centre (DG JRC), Available at: <http://www.jrc.es>, p.54.

vocal advocates for further research into the legal and legal implications.⁶⁴ This requires examining how existing law frames such intrusions, and how interferences in respect of locational privacy may evolve with technologies.⁶⁵

1.3 The challenges to locational privacy and data protection of new technologies

In the past, methods of collecting and processing location data were invariably relatively resource intensive as the technical means of effectively monitoring an individual's mobility patterns were far more limited. In addition, until relatively recently, the monitoring of mobility was a far more complex task limited in its observational capability in terms of efficiency, extensiveness and, particularly important, its unobtrusiveness to the individual concerned. However, technological advancements now allow for pervasive, almost continuous collection and processing of personal location data attributable to an individual's movements.⁶⁶ Similarly, whilst accurate models mapping mobility have been a long-term ambition, until recently efforts have yielded relatively little insight in this domain. The objective was hindered primarily by the unavailability of the innovative wireless technologies recently developed and widely implemented in our society.⁶⁷ Moreover, while human interactions are increasingly dependent upon mobile computing devices connected to

⁶⁴ See: Guzik K., Discrimination by Design: Data Mining in the United States' 'War on Terrorism', Surveillance & Society, Vol 7, No 1 (2009), Available at: <http://www.surveillance-and-society.org>; See also: Goodman, M., 2015. Future Crimes: A journey to the dark side of technology—and how to survive it. Random House, p.130; See also: Nathan Eagle, Alex Pentland, and David Lazer, Inferring friendship network structure by using mobile phone data, 2009, p. 15277, Available at: <http://www.pnas.org>.

⁶⁵ Parker indeed emphasizes the significance of sensory oversight over a party's activity in defining privacy, interpreting privacy as constituting "control over who can sense us." See: Richard B. Parker, A Definition of Privacy, 27 RUTGERS L. REV. (1974), p.281. See also, for example: Uteck, Anne, Ubiquitous Computing And Spatial Privacy (March, 2009), p.88-90, Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/799

⁶⁶ See, for example: Jerome E. Dobson & Peter F. Fisher, "Geoslavery," IEEE Tech. and Society Magazine (Spring 2003), pp.48-52; also, for example: R. Shokri, G. Theodorakopoulos, J. Y. Le Boudec and J. P. Hubaux, "Quantifying Location Privacy," Security and Privacy (SP), 2011 IEEE Symposium on, Berkeley, CA, 2011, p. 247

⁶⁷ Elwood et al. note that rapid technological advancements, coupled with evolving demands for geographic data, have radically altered the environment within which location data is now collected and processed. See: Sarah Elwood, Michael F. Goodchild, and Daniel Z. Sui, Researching Volunteered Geographic Information: Spatial Data, Geographic Research, and New Social Practice Article in Annals of the Association of American Geographers, May 2012, Available at: https://www.researchgate.net/publication/233475586_Researching_Volunteered_Geographic_Information_Spatial_Data_Geographic_Research_and_New_Social_Practice, pp.1-4

communications networks, these devices are in addition becoming progressively more proficient in providing location data relating to the behavior of an individual through improved sensing capabilities.⁶⁸ Recent scholarship has also highlighted the consequence of certain heuristic processes by which individuals develop a capacity to distinguish between different types of personal location data collection and processing, and whether the safeguards provided for in existing legislation are apt to adequately protect locational privacy. Tene and Polonetsky's work has indeed questioned whether individuals are suitably qualified to make decisions pertaining to their personal location data given well-documented cognitive biases and the increasing complexity of the information ecosystem."⁶⁹

Studies relating to the analysis and interpretation of personal location data continue to highlight how fundamental gaps in our understanding still persist. Indeed, essential questions relating to the collation and transformation of the raw location data into knowledge into, as Giannotti and Pedreschi suggest, "useful models and patterns that discriminate with the requisite precision between individual and collective behaviours", remain as yet unanswered.⁷⁰ Furthermore, scholars have highlighted deficiencies in the analytical capabilities of geographic information systems (GIS) that use location data, and have challenged the notion whether the current formulations that they render are entirely dependable and accurate. This lacuna thus has wider implications for our cognizance of the interference the monitoring of citizens' patterns of mobility may impart.⁷¹

⁶⁸ Indeed, in this respect telecommunications operators have asserted that the wider use of such networks to collect and process personal location data from citizens is an inevitability. *See*: RSA (Royal Society for the encouragement of Arts, Manufactures and Commerce), *The Future of Mobile*: RSA Keynote, 27 October 2010, Available at: <http://www.thersa.org/events/audio-and-past-events/2010/the-future-of-mobile>.

⁶⁹ Omer Tene & Jules Polonetsky, *Privacy In The Age Of Big Data: A Time For Big Decisions*, 64 *Stanford Law Review Online* 63, February 2, 2012, p.67

⁷⁰ *See*: F. Giannotti & D. Pedreschi, *Mobility, Data Mining and Privacy: A Vision of Convergence*, in *Mobility, Data Mining and Privacy* (2008) F. Giannotti and D. Pedreschi (eds.), pp.1-2

⁷¹ Concerns have been raised, for example, with respect to the use of cell phone location data and overstating its accuracy in law enforcement investigations *See*: *The Economist*, *The Two Towers*, 6 September 2014, Available at: <http://www.economist.com/news/united-states/21615622-junk-science-putting-innocent-people-jail-two-towers>. *See also*: Tech Dirt, which has asserted: "Turns out cell phone location data is not even close to accurate, but everyone falls for it." *Tech Dirt*, Sept. 2014, Available at: www.techdirt.com/articles/20140908/04435128452; Paul A. Zandbergen, *Accuracy of iPhone locations: A comparison of assisted GPS, WiFi and cellular positioning*, *Transactions in GIS* 13, June 2009, Available at: www.onlinelibrary.wiley.com. *See, also*: Huffman, Nikolas H. "You can't get here from there: reconstructing the relevancy of design in postmodernism in *Cartographic Design: Theoretical and Practical Perspectives*", (ed.) CH Wood and CP Keller. (1996): pp. 35-53; Miller, H.J.,

The specific concerns outlined above therefore underscore the importance of further enquiry to better understand the effects continued innovation heralds. The importance of greater scrutiny is supported by survey research⁷² that indicates the necessity of addressing underlying anxieties amongst the general public: a recent poll also revealing that a majority of citizens profess to be concerned with a perceived loss of control over their personal data.⁷³ Evidently, therefore, the attempts to date to elucidate and conceptualize the contours of the privacy of location and to delineate boundaries between different types of spaces, safeguard knowledge of patterns of our own movement, have proven contentious.⁷⁴ Furthermore, advancements in

2000. Geographic representation in spatial analysis. *Journal of Geographical Systems*, 2(1), pp.55-60. Sui and Goodchild suggest, for example, that rather than regard GIS “as ‘a distant mirror’ faithfully reflecting reality” it is “perhaps more appropriate to treat GIS as ‘a close dialogue’ among different players in society.” *See*: Sui, D.Z. and Goodchild, M.F., 2003. A tetradic analysis of GIS and society using McLuhan’s law of the media. *The Canadian Geographer/Le Géographe canadien*, 47(1), p.12. Schneier asserts that our inability to comprehend how new technologies function is especially salient in considering surveillance, noting that we have evolved highly attuned and delicately social psychological systems to navigate complex privacy decisions, however, technology may inhibit our social abilities and undermine our intuition. *See*: Schneier B., *Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W.W. Norton & Company, 2015, p.203. *See also*: Couclelis, H., 1996. Geographic illusion systems: towards a (very partial) research agenda for GIS in the information age. *GIS and Society: The Social Implications of How People, Space, and Environment Are Represented in GIS* (ed.) T. Harris and D. Weiner, Technical Report, pp.96-7.

⁷² *See*, for example: EU Commission, Full report on the public consultation on the ePrivacy Directive, December 2016, Available at: <https://ec.europa.eu/digital-single-market/news-redirect/37204>.

⁷³ *See*, for example: Boston Consulting Group, *The Value of Our Digital Identity*, Liberty Global Policy Series, November 2012, Available at: <http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity>, pp.13; *See also*: Berendt, B., O. Günther & S. Spiekermann (2005), ‘Privacy in e-Commerce: Stated Preferences vs. Actual Behavior’, *Communications of the ACM*, Volume 48, No. 4, pp.101-106; Compañó, R. & W. Lusoli, ‘The Policy Maker’s Anguish: regulating personal data behaviour between paradoxes and dilemmas’, in T. Moore, C. Ioannidis & D. Pym (eds.), *Economics of Information Security and Privacy*, 2010, New York: Springer.

⁷⁴ For an analysis of evolving perspectives vis-à-vis the role of technology in shaping privacy rights, *see*: Flaherty D.H., ‘Visions of Privacy: Past, Present and Future’ in C.J. Bennett & R. Grant (eds.), *Visions of Privacy: Policy Choices for a Digital Age*, 1999, Toronto: Univ. of Toronto Press, pp.19-38. Kluitenberg, in contrast, has argued that the proliferation of wireless networks redefines space geographically, and that this superimposition of monitoring intersects with a person’s privacy by creating a new type of shared space cannot be properly understood without a very precise analysis of the meanings conveyed by the physical places it manipulates. *See*: Kluitenberg, E., *The Network of Waves: Living and Acting in a Hybrid Space*, in *Open 11: Hybrid Space. How wireless media are mobilizing public space*, NAI Publishers, 2006, p.7. Kranzberg also notes that technology’s interactions with the social ecology have human consequences that go far beyond the immediate purposes of the technical devices and practices themselves. *See*: Kranzberg, M. (1986) ‘Technology and History: Kranzberg’s Laws’, *Technology and Culture* vol. 27, no. 3, p.545. Goldman has commented that arguments as to the viability of privacy constituting a fundamental right routinely devolve into an irresolute binary polemic, asserting: “It is, of course, impossible to refute the argument that privacy is a fundamental right. Social scientists cannot empirically prove or disprove the claim, and no single objective source authoritatively classifies what constitutes a fundamental right.” *See*: Goldman, Eric, *Data Mining and Attention Consumption. Eric Goldman, Privacy And Technologies Of Identity: A Cross-Disciplinary Conversation*, Springer, 2005, Available at: <http://ssrn.com/abstract=685241>, p.4. In contrast, Calo offers a seemingly straightforward definition in affirming: “Privacy harm is

technologies render the delineation of the parameters that govern levels of privacy to certain spaces ever more complex. Questions pertaining to the intrinsic value of location data and knowledge generated by monitoring mobility prove increasingly contentious. That these issues remain unresolved despite their growing importance for society supports the assertion that further, more detailed assessment of their impact is required.

2. Defining the framework of the thesis: research question, purpose of the research

This study therefore aims to address the extant gap in respect of our understanding the specific utility of location data relative to other metadata; it aims to evaluate whether the location data collection and processing that continues to proliferate in emergent technologies is synchronously shaping citizens' perception and appreciation of their fundamental rights to privacy and data protection. In addition, this analysis appraises whether the legal term 'location data' is in itself an apt designation, and questions whether the term inappropriately frames an intrinsically more complex conception. More specifically, of pertinence in this context is our considering the nature of the actual data itself that the term relates to, notably, both the spatial and temporal aspects of the relevant metadata in question.⁷⁵ Historically, much of the generation of location data originated from the necessity of communications networks to function effectively.⁷⁶ That there exists a term to describe location data, to reference and distinguish it from other types of personal data, is significant: the distinction recognizes that the data in question has specific attributes. From both a semantic and legal perspective, classification is a necessity of formulating such distinctions, so that we might frame and conceptualise different notions and abstractions that emerge from

conceptualized, if at all, as the negative consequence of a privacy violation." *See*: Calo, M. Ryan, The Boundaries of Privacy Harm (July 16, 2010). *Indiana Law Journal*, Vol. 86, No. 3, 2011, Available at : <http://ssrn.com/abstract=1641487>, p.2.

⁷⁵ For a more detailed explanation see, for example: Silberschatz, Korth & Sudarshan, *Temporal and Spatial Data - Database System Concepts*, 6 March 2007, Available at: <http://www.wis.win.tue.nl/~tcalders/teaching/dbmodels/pdf/>

⁷⁶ *See further*: Pei Zheng, Lionel Ni, *Smart Phone and Next Generation Mobile Computing*, 2010, Morgan Kaufmann/Elsevier, San Francisco, p.417. *See also*: E. Trevisani & A. Vitaletti, Cell-ID location technique, limits and benefits: an experimental study, *Proceedings of the Sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2004)*, 2004, Available at: <http://ieeexplore.ieee.org>, p.1; WP29, Opinion 13/2011 on Geolocation services on smart mobile devices, 16 May 2011, WP 185, Available at: <http://ec.europa.eu/justice/policies/privacy/>

our examination of the utility of the data in question. The overarching objective of this research is to evaluate the appropriacy of the continued use of the term ‘location data’ as applied in the legal and regulatory frameworks at the European level. The utilisation of the designation ‘location data’ in respect of evolving capacities in data collection and processing thus engenders particular challenges, and places in question the congruity of this term vis-à-vis other definitions pertaining to personal data on a normative level.

The principal research question of this study is therefore: “Does the term ‘location data’ represent a cogent designation that aptly frames the intrinsic qualities of the metadata it concerns, permitting a coherent application of the legal framework pertaining to the safeguard of privacy and data protection at the regional European level?”

From a technical perspective, viewed through the lens of computer science, such a distinction is not a moot point. Recognition of the intrinsic spatio-temporal duality of location data is fundamental feature of the metadata in question.⁷⁷ The salience of this issue, and the pertinence of dedicating further investigation, stems from the realisation that both from a theoretical and practical perspective our understanding of the utility of metadata remains underdeveloped.

This research study also considers the following related issues that inform the analysis:

— In privacy law a distinction has traditionally be drawn between ‘public’ and

⁷⁷ See, for example, the RAND report discussing the foundations of spatiotemporal analysis and heuristic methods used to analyze spatiotemporal features: RAND, *Predictive Policing - The Role of Crime Forecasting in Law Enforcement Operations*, 2013, Available at: www.rand.org, p.44. See further: Betsy George, James M. Kang, Shashi Shekhar, “Spatio-Temporal Sensor Graphs (STSG): A data model for the discovery of spatio-temporal patterns,” *Intell. Data Anal.* 13(3): 457-475 (2009); NCHRP, *Quality and Accuracy of Positional Data in Transportation*, 2003, Available at: http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_506.pdf; Shen Bin, Liu Yuan, Wang Xiaoyi, *Research on Data Mining Models for the Internet of Things*, 2010 International Conference on Image Analysis and Signal Processing, Available at: <https://www.ceid.upatras.gr/webpages/faculty/vasilis/Courses/>, p.5; Groff, Elizabeth, David Weisburd, and Nancy Morris, ‘Where the action is at places: examining spatio-temporal patterns of juvenile crime at places using trajectory analysis and GIS’, in *Putting Crime in Its Place: Units of Analysis in Spatial Crime Research*, 2009, eds. David Weisburd, Gerben Bruinsma, and Wim Bernasco. New York: Springer Verlag.

‘private’ spaces. It is reasonable to assert that we maintain this seemingly binary separation, the public and private spheres, especially given that the determination of a private zone of seclusion is proving ever more an elaborate and convoluted process?

— To what extent are definitions such as ‘location data’ apt to distinguish between different metadata; can distinctions be drawn in a cogent manner, with the requisite foreseeability and certainty?

— Given the challenges of developing profiling based on the collection and processing of location data, what specifically are the newly emergent considerations relevant to maintaining appropriate regulatory oversight?⁷⁸

— What challenges does the implementation of the Internet of Things (IoT) present in terms of location data collection and processing? The rapid expansion of IoT suggests a major augmentation of monitoring capabilities. The collection of location data relating to human mobility raises pertinent questions as to qualifying whether such data identifies specific individuals and constitutes personal data.

— To what extent are current provisions pertaining to the use of location data in the legal framework apt to ensure the safeguard of citizens’ rights where personal data is collected and processed to develop biometric and behavioristic⁷⁹ information? Discrete and embedded devices present challenges to our applying existing conceptualisations and precedents as regards the relationship between data subjects,

⁷⁸ See: CEPS, Online Personal Data Processing and EU Data Protection Reform - Report of the CEPS Digital Forum, April 2013, Available at: <http://www.ivir.nl/publicaties/download/1350>, p.72; Korff, D., ‘Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments. Working Paper Number 2, in Kantor (2010), Comparative Study of the Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments, study commissioned by the European Commission, Directorate-General Justice, Freedom and Security. Available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf; De Hert, P. & V. Papakonstantinou (2012), “The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals”, Computer Law & Security Review, Vol. 28, No. 2, p.138

⁷⁹ Behavioristics utilise algorithms and models to measure and quantify unique human behavioural patterns in place of human bio-attributes (note: commonly referred to as ‘biometrics’). Behavioristic algorithms process multiple data from various sensors as inputs and fuse them to build behavioural models capable of producing application specific quantitative analysis on the unique individuals who were the originators of the personal data. See further: Zhu, Jiang. “Mobile Behavioristics: Behavior Modeling from Heterogeneous Sensor Time-Series.” (2014). Available at: <http://repository.cmu.edu/dissertations/388/>

data processors and controllers. Additional concerns also demand further examination in respect of data quality; namely, with regard to collection limitation, purpose specification and use limitation. What issues are raised by the collection of location data to capture the physical context of the user and her/his surrounding conditions?⁸⁰

In answering the research question the scope of the enquiry conducted will be limited to a review of the legal framework in place at the regional level, focusing upon the jurisprudence of the ECHR and the CJEU. This restriction on the ambit of the review is necessary so as to allow, given the resources available to the author, the opportunity to explore the subject in sufficient depth. As regards the relevant working framework at the EU level for the consideration of matters pertaining to location data, the principal legal instrument at the current point in time is the Data Protection Directive (95/46/EC).⁸¹ The Directive applies where personal data are being processed as a result of the processing of location data. The e-Privacy Directive (2002/58/EC), as revised by 2009/136/EC, only applies to the processing of base station data by public electronic communication services and networks (telecommunications operators).⁸² It should be noted in this context that the scope of the definition of “location data” as articulated by Article 2(c) of Directive 2002/58/EC was widened by Directive

⁸⁰ Goodman observes of the tendency that smartphones are progressively turning people into human sensors, with precision location data relating to the individual capable of generating vast sums of highly granular information pertaining to our respective idiosyncrasies. *See*: Goodman, M., 2015. *Future Crimes: A journey to the dark side of technology—and how to survive it*. Random House, p.128. *See also*: W. Scheirer and T. Boult. Biometrics: Practical issues in privacy and security. Technical report, Securics, Inc. and the University of Colorado. Colorado Springs, 2011. Tutorial at International Joint Conference on Biometrics.

⁸¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

⁸² *See*: WP29, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN WP 185, 16 May 2011, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, p.7. Note: The Data Protection Directive (95/46/EC) does not provide a definition for the term ‘location data’: rather, one needs consider the relevant references within the e-Privacy Directive (2002/58/EC),

“Recital 14:

Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

Article 2:

Definitions:

(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;”.

2009/136/EC; in addition to data processed in an electronic communications network, data processed by an electronic communications service is also covered by the term.⁸³ As has been clearly articulated in the WP29 Opinion on Geolocation services on smart mobile devices, a major risk with the use of location data is function creep, the reality that “based on the availability of a new type of data, new purposes are being developed that were not anticipated at the time of the original collection of the data.”⁸⁴

The study of the nomenclature in respect of location data also allows for a broader review of the implications for the coherency of the structuring of the applicable legal framework vis-à-vis considerations pertaining to metadata as a whole. Indeed, it has been observed how in this regard spatial metaphors are useful due to the power they inhere heuristically, particularly in the developing domain of pervasive computing, where discourse has integrated issues of social, natural and temporal spaces.⁸⁵ Furthermore, certain terminology may function to unnecessarily obscure and obfuscate the ability of the data subject concerned to rationally deliberate and take informed decisions. As mobility becomes a crucial factor to data processing activities, so to will the criticality of resolving whether ‘location data’ is sufficiently precise a term.⁸⁶ Investigation of these issues may also reveal broader concerns in respect of

⁸³ Directive 2009/136/EC, Article 2:

Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications)

Directive 2002/58/EC (Directive on privacy and electronic communications) is hereby amended as follows:

2) Article 2 shall be amended as follows:

(a) point (c) shall be replaced by the following:

‘(c) “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;’

⁸⁴ See: WP29, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN WP 185, 16 May 2011, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, p.7

⁸⁵ See: Camp, J. and Chien, Y.T., 2000. The internet as public space: concepts, issues, and implications in public policy. *ACM SIGCAS Computers and Society*, 30(3), pp.13-19. See also: Langheinrich, M., 2002, October. Privacy invasions in ubiquitous computing. In *Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing. UbiComp*.

⁸⁶ An individual’s position history may consist of a series of four dimensional space-time positions with the associated attributes of speed, direction of travel and positional accuracy. Mountain and Raper affirm that: “In contrast to purely spatial data, the representation, storage and analysis of spatio-temporal data has received relatively little attention.” See: Mountain, D. & Raper, J., 2001. Spatio-temporal representations of individual human movement for personalising Location-Based Services. In *Proceedings for GISRUK 2001*, p. 57

oversights in the distinctions drawn between other types of metadata. Of interest is whether the current legal discourse demonstrates inconsistencies in the theoretical framing of distinctions made in the collection and processing of metadata more generally. The increasing ubiquity and pervasiveness of computing in our environment render such concerns ever more immediate and pertinent.

A further objective of this review is to illustrate the critical importance of location data and its interconnection with to the right to locational privacy, thereby illustrating the particular value that locational privacy serves — both to the individual citizen and society as a whole. Examining interrelated rights such as association, data protection and freedom of movement through the lens of locational privacy, this distinct perspective affords scope to discern its importance relative to the other dimensions of privacy that are more routinely examined. This review shall prove constructive for its generation of new knowledge pertaining to the specific value of locational privacy, and contribute toward our comprehension of the strengths and limitations of the existing legal framework as applied, where advancements in technology may portend future challenges.

Furthermore, customary distinctions drawn between physical and abstract spaces are increasingly problematic in privacy terms. Questions arise as to how we seek to delineate events that are either categorised as ‘online’ or ‘offline’, and how such determinations relate in a spatial context.⁸⁷ The challenges society faces in this respect are intrinsically multi-disciplinary, and require solutions — and hence research — that cross the boundaries of traditional disciplines. Crucially, a key aspect of this

⁸⁷ European citizens will find themselves increasingly surrounded by pervasive, always-on wireless networks; these systems will further bridge physical spaces and the virtual world. As such, therefore, ensuring individuals’ privacy in conjunction with preserving public security will only grow in importance. *See*: IPTS, Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, European Commission Joint Research Centre (DG JRC), Available at: <http://www.jrc.es>, p.58. Inazu speaks of a “collapsing distinction” between online and offline contexts that blurs not only our relationships, but also our identities. *See*: Inazu, J.D., 2012. Virtual Assembly. *Cornell L. Rev.*, 98, pp.1093. US Supreme Court Justice Anthony Kennedy remarked in this regard: “Minds are not changed in streets and parks as they once were. To an increasing degree, the more significant interchanges of ideas and shaping of public consciousness occur in mass and electronic media.” Thus, increasingly relevant to our framing expressive association between individuals are the distinctions made between traditionally defined geographic, spatial environments and nascent conceptions of the metaphysical. *See*: *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, 518 US 727, pp. 802–03, (1996) (Opinion of Justice J. Kennedy, concurring in part and dissenting in part).

method must be the diligent appraisal and apprehension of the characteristics of the technologies themselves.

The growth in the generation and uses of location data has not been paralleled by a similar intensification of research into the implications in the legal domain. As technological advance continues unabated, the level of enquiry as to its effects has been deficient: inducing a disquieting lacuna in our cognizance and appreciation of the consequences for society. Of necessity, therefore, is an analysis and evaluation as to the adequacy of the existing framework of regulation and protection of citizens' fundamental rights where these intersect with the exploitation of location data in the operation of technologies. As highlighted heretofore, the study of location data perforce requires an examination of the relationship of location to human mobility; to the conceptualisation of space; and to the framing of associated fundamental rights, including privacy and data protection. The ambit of this review thus needs be of sufficient scope so as to appositely encompass the complexity of the conceptualisation of location vis-à-vis human mobility, undertaking an analysis of sufficient rigour to comprehensively address the current deficiencies in our understanding.

The wider purpose of this research is the consequence of whether definitions that relate to metadata adequately describe the actual attributes of the data implicated. Should there indeed exist inconsistencies, we need appreciate the resultant effects that stem from such dissonance. By endeavouring to discern the adequacy of the definition, we may also further illuminate the issue of the application of the term contextually in relation to human mobility, and ascertain how the conceptualisation of location data influences the normative framework and textual interpretation pertinent to the right to privacy and the right to data protection. Of interest, therefore, is whether any inexactitude vis-à-vis the legal term relative to its accepted technical composition generates discrepancies with substantive repercussions. Any such outcome would in turn influence substantively the framing of a potential interference to an individual's rights where the activity concerned encompasses location data collection and/or location data processing. Answering this question constitutes the objective of this research, and institutes a conversation that the author hopes shall engage and prove of interest to academics, information technologists, policymakers and the general public.

Scope and context of the research study

Chapter 2, which furnishes a detailed discussion of the development of the privacy and data protection legal framework at the European regional level, outlines the current status of legislative reforms at the time of writing. Regarding the adoption of this new legislation, it is important to note that the Commission explained its intention that the new general legal framework for the protection of personal data in the EU would cover data processing operations in all sectors and policies of the EU. The proposal intended that a “comprehensive new legal framework will ensure an integrated approach as well as seamless, consistent and effective protection.”⁸⁸ One needs note too the Commission’s assertion that the principles enshrined in the Data Protection Directive remain and, whilst, the legislation required revision and modernisation “to respond to new challenges and situations” it nonetheless affirmed that “...until new rules are adopted and enter into force, the current rules remain entirely valid and still have to be correctly implemented by Member States and applied by all those concerned.”⁸⁹

The aforementioned point is particularly important as the affirmation validates the approach of the author’s intent to retain a primary focus on the application of the existing legal framework at the EU level, rather than attempt to develop a review based upon the shifting, changeable considerations that characterise the evolving law-making process to enact new legislation on data protection. Having taken this decision at the commencement of this analysis, the reasonableness of this initial decision would appear to have been borne out in considering the subsequent political deliberations and parliamentary proceedings that ensued.⁹⁰

⁸⁸ EU Commission, Data protection reform – frequently asked questions - PRESS RELEASE: MEMO/10/542, 4 November 2010, Available at: http://europa.eu/rapid/press-release_MEMO-10-542_en.htm?locale=fr.

⁸⁹ EU Commission, Data protection reform – frequently asked questions - PRESS RELEASE: MEMO/10/542, 4 November 2010, Available at: http://europa.eu/rapid/press-release_MEMO-10-542_en.htm?locale=fr. On 24 May 2016 the General Data Protection Regulation entered into force. It will apply from 25 May 2018. See: EU Commission - Home Affairs, Data protection reform- The general data protection regulation, 27 September 2016, Available at: <http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-regulation/>. For the final full text of the GDPR, adopted 27 April 2016, which enters into force 20 days from its publication in the Official Journal on 4 May 2016, thus on 24 May 2016, visit: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

⁹⁰ For a summary timeline including the principal milestones in the history of the EU’s adoption of the General Data Protection Regulation (GDPR), see: EDPS, The History of the General Data Protection

This approach is not inapposite. The initial decision to retain a focus on the legislation in force was based primarily on two counts. Firstly, as has already been indicated, during the course of this research the deliberations and machinations relating to the adoption of the GDPR took many turns. As such, without there being any guarantee as to the scope of the substantive provisions finally adopted in the legislation and, furthermore, taking into consideration the obvious absence of any provision that a regulation would definitely be enacted (the proposal being subject to the collective democratic will of the European Parliament, the Council and the Commission), it was considered by the author prudent to follow the approach originally selected. To elect to attempt a review of pending legislative provisions would have otherwise meant dedicating an inordinate amount of analysis and resources to a process without guarantee of any specific, defined outcome.

Purpose, relevance and objectives of the research study

This study adopts a forward-looking perspective and aims to discern how the evolution of information and communications technologies in relation to the collection and processing of location data shall in the future influence our understanding of the normative basis for the existing legal framework established at the European level. The approach of a positivistic legal study also embraces the discussion of the philosophical foundations of the justification for the basis to the fundamental rights of privacy and data protection as they pertain to the developments specific to the conceptualisation of individual mobility and locational privacy. This approach to the appraisal of the wider ramifications of the development of pervasive computing and their resulting impact on society also analyses how they might further influence and transform existing theoretical perspectives as regards the nature of our civil liberties in European constitutional democracies.

The focus of this research necessarily centres on the legal domain. Where relevant this study also however evaluates the scholarship of computer science, behavioural

Regulation, 2017, Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

psychology, sociology and philosophy. This interdisciplinary approach affords scope to take advantage of the insight offered through alternate and complimentary perspectives developed.

This research is also important in terms of understanding the potential impact the institutional entrenchment of the technologies and methods of location tracking may inhere once they have become integrated within public institutions, such as law enforcement agencies and civic authorities.⁹¹ Crucially, as regards European citizens' level of comprehension as to how data protection and privacy rights have come into being, surveys show that an understanding of the legal framework at both the national and regional levels is extremely limited.⁹² The lack of examination given to the subject of locational privacy does not in any way reflect it being inconsequential, or indeed of simply lesser importance than other aspects integral to the wider framing of privacy as a fundamental right. Rather, we may reconcile the comparative inattention given this topic of research in part to the need to consider that, historically, practical constraints limited the availability of the means to determine an individual's location at any particular time. In the past, methods of collecting and processing location data were invariably relatively resource intensive as the technological means of effectively monitoring an individual's mobility patterns were far more limited; primarily it was this burden that had historically limited more widespread general application of the monitoring of people's movements. However, technological advancements now allow for the pervasive and unrelenting collection and processing of personal location data attributable to an individual's movements.⁹³ Thus, while locational privacy is an established notion, it has thus far remained underdeveloped conceptually and, as a result, has been under appreciated in respect of its inherent value in furnishing citizens capacity to enjoy wider fundamental freedoms. Today, continuous, pervasive and unrelenting monitoring of citizen's movements is increasingly realizable. Of

⁹¹ See further: Michael Levi & David Wall, 'Crime and Security in the Aftermath of September 11: Security, Privacy and Law Enforcement issues relating to emerging information communication technologies' in 'Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)', July 2003, DG JRC, Available at: <http://www.jrc.es>, pp.171-172

⁹² See further: Hallinan, Dara, Michael Friedewald, and Paul McCarthy, "Citizens' Perceptions of Data Protection and Privacy", *Computer Law and Security Review*, Vol. 28, No. 3, 2012, p. 267

⁹³ See: Peter Swire & Kenesa Ahmad, 'Going Dark' Versus a 'Golden Age for Surveillance', *Security & Surveillance*, November 28, 2011, Available at: <https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/>, p.4

importance, therefore, is the need to develop an extensive, coherent conceptualisation of the relationship of location data to both locational privacy and data protection as rights.

The purpose of the research conducted in the latter part of this study in respect of current profiling capabilities and in conjunction with a forward-looking analysis on the Internet of Things (IoT) and behaviometrics is to attempt to discern how these innovations will shape the collection and processing of location data. Purported patterns pertaining to the attributes of location data are increasingly forming the basis for forward-sighted predictions of citizens' behaviour.⁹⁴ It has been suggested that efforts to collate and analyze different individuals' personal location data for the purposes of discerning the composition of relationships between parties may pose further additional risks: sensitive nascent relationships and interactions that would

⁹⁴ Millar, Jason, Core Privacy - A Problem for Predictive Data Mining (March, 2009), p.106, Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society, New York: Oxford University Press, 2009; Available at: www.idtrail.org/content/view/799. Similarly, Phillips underscores the primacy of behavioural monitoring as an objective of ubiquitous location tracking, identifying the abnormal from a background of normalcy. *See also*: Phillips, David J., Ubiquitous Computing, Spatiality, And The Construction Of Identity - Directions For Policy Response (March, 2009). Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society, New York: Oxford University Press, 2009, p.310. This issue remains contentious, however. Eagle and Pentland demonstrated in limited studies of personal location data collected over longer periods the distinctive temporal and spatial patterns in physical proximity between peers based on cellphone calling records. *See*: Nathan Eagle, Alex (Sandy) Pentland, and David Lazer, Inferring friendship network structure by using mobile phone data, 2009, p.15274, Available at: <http://www.pnas.org/>. In a similar vein, Gonzalez et al argue in their research that, in contrast with the random trajectories predicted of humans, our movements follow simple reproducible patterns and, as such, knowledge of the intrinsic similarity of our travel patterns could prove transformative the monitoring and predictive modeling of human mobility. *See*: Gonzalez M.C., Hidalgo C.A., Barabasi A.L., Understanding individual human mobility patterns, Nature, 2008, pp.779–782 Available at: <http://www.nature.com/nature/journal/v453/>. Freiwald also asserts that cellular networks afford sufficient resolution in allowing for detailed inferences to be drawn relating to individual patterns of movement, noting that the short-term irregularity and imprecision of specific data points is adequately compensated for by the larger datasets of location data furnished over time. *See*: Freiwald S., Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact (April 20, 2011). Maryland Law Review, Vol. 70, pp.731-732. *See*, for further examples: Cohen, Julie E., Privacy, Visibility, Transparency, and Exposure. University of Chicago Law Review, Vol. 75, No. 1, 2008; Georgetown Public Law Research Paper No. 1012068, p.186, Available at: <http://ssrn.com/abstract=1012068>. *See also*: Boyd, Danah and Crawford, Kate, Six Provocations for Big Data (September 21, 2011). A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011, pp.4-5. *See*: Bollier, D. (2010) 'The Promise and Peril of Big Data', Available at: <http://www.aspeninstitute.org/publications/promise-peril-big-data>, accessed 12 January 2012, p.13. *See also*: Boyd and Crawford's account of the issues of apophenia (erroneous pattern recognition) advocates particular caution in relation to the processing of large datasets of personal data: Boyd, Danah and Crawford, Kate, Six Provocations for Big Data (September 21, 2011). A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011, p.5, Available at: <http://ssrn.com/abstract=1926431>

otherwise remain undetected could be exposed.⁹⁵ The review examines current practices in profiling more generally, and then investigates how the exploitation of location data might furnish even greater insight into highly personal aspects of people's lives. This insight is then developed with respect to emergent location data collection and processing techniques and then, in turn, applied in the latter stages of this study to the review of two particularly important spheres of innovation with regard to location data: namely IoT and biometrics.

With IoT questions arise in relation to distinctions made in law as to the determination of whether location data collected by devices constitutes personal data. Increasingly of concern in respect of the proliferation of sensing devices is whether location data implicitly contains information pertaining to a user or identifiable individual. This distinction as to what constitutes personal location data will become even more pressing where such devices may potentially capture information that relates to different data subjects. The existing EU legislative framework specifies that data must be collected for specified, explicit and legitimate purposes and not subject to further processing in a manner incompatible with the specified purposes. With IoT it may not immediately clear *ex ante* as to the grounds for processing. Furthermore, with IoT it may be unclear as to the nature of the data collected and whether it indeed constitutes 'personal data'.

The corollary of advances in sensing capabilities may also bring forth further enquiry into the corresponding impact of biometrics based on location data. Increasingly a wide range of human characteristics will find themselves captured and rendered as personal data, including location data. Embedded sensors have made possible the capture of the physical context of an individual within their environment, based upon

⁹⁵ Rachels highlights the importance of this concern with regards to the risk an interference might pose to the privacy of the individual and parties with whom they associate, stating that the requisite measure for privacy protection should assure individuals "...the important power to share information discriminately, which in turn enables them to determine not only how close they are to others, but the nature of their relationships." Rachels, J., Why Privacy Is Important, in *Philosophical Dimensions of Privacy: An Anthology*, Ferdinand D. Schoeman, ed., Cambridge: Cambridge University Press, (1984), p.294. *See also*: Thrift N., *Non-Representational Theory: Space, Politics, Affect*; Routledge, March 2008, p.87; C. Dwork & A. Roth, *The Algorithmic Foundations of Differential Privacy*, *Foundations and Trends in Theoretical Computer Science* Vol. 9, Nos. 3-4 (2014), 211-407, Available at: <https://www.cis.upenn.edu/~aaroht/Papers/privacybook.pdf>, p.10

the collection and processing of personal data relating to movement.⁹⁶ This modelling permits the generation of ‘behaviometrics’⁹⁷ utilizing location data. The Joint Research Centre of the European Commission has highlighted the need to further study the consequence of an increasing weight of electronic expression of such characteristics leading to new indicators of privacy. To date only limited research has addressed the concerns raised regarding rights of data subjects, focusing upon the implications of location-aware technologies associated with sensor-body interfaces and the means by which their implementation might implicate how individuals conceive of their respective identities.⁹⁸ Each of these chapters covering profiling, IoT and location data-based biometrics thus constitutes a case study through which to directly apply the theoretical and conceptual postulations developed in the critique of the normative challenges posed by the developing uses of location data.

The objective of this study is, therefore, to illustrate exactly the critical importance of location data and interconnection with to the right to locational privacy and, furthermore, elucidate the particular value that locational privacy serves - both to the individual citizen and society as a whole. Examining interrelated rights such as those pertaining to association, data protection and freedom of movement through the lens of locational privacy, this distinct perspective affords scope to discern the importance of location data relative to the other dimensions of privacy that are more routinely examined. This research shall expand our understanding of the specific value of location data as it relates to locational privacy, and contributes toward our

⁹⁶ See: Zhu, J., Hu, H., Hu, S., Wu, P. and Zhang, J.Y., 2013, August. Mobile behaviometrics: Models and applications, in 2013 IEEE/CIC International Conference on Communications in China (ICCC) (pp. 117-123). IEEE.

⁹⁷ The concept constitutes a linkage of the terms ‘behavioural’ and ‘biometrics’. *Behavioural* refers to the way a human person behaves and *biometrics*, in an information security context, refers to technologies and methods that measure and analyzes biological characteristics (bio-attributes) of the human body for authentication purposes. See: BehavioSec, White Paper BehavioMetrics - A Paradigm Shift in Computer Security, February 2016, Available at: <https://www.behaviosec.com>, p.4. See also: Zhu, Jiang, “Mobile Behaviometrics: Behavior Modeling from Heterogeneous Sensor Time-Series” (2014). Dissertations. Paper 388. Available at: <http://repository.cmu.edu/dissertations/388>, p.i

⁹⁸ See, for example: Lyon, D. (2001) *Surveillance Society*, Buckingham: Open University Press; Haggerty, K. and Ericson, R., ‘The Surveillant Assemblage’, *British Journal of Sociology*, Volume 51, No. 4, (2000), pp. 605-622; Poster, M., *What’s the Matter with the Internet?* (2001), Minneapolis: University of Minnesota Press. See also: Michael Levi & David Wall, ‘Crime and Security in the Aftermath of September 11: Security, Privacy and Law Enforcement issues relating to emerging information communication technologies’ in ‘Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)’, July 2003, DG JRC, Available at: <http://www.jrc.es>, p.174

comprehension of the strengths and limitations of the existing legal framework as applied where technology developments portend possible lacunae in the coverage of safeguards to our fundamental rights.

3. Structure of the thesis

This study is divided into two main parts. The first section discusses the general context concerning approaches to the conceptualisation of privacy and personal data protection as rights with regard to our physical environment. The discussion begins with an examination of the historical development of data protection and privacy protections and then appraises how the legal framework is applied where notions of locational privacy intersect with broader formulations that delineate public and private spaces. The analysis frames the debate in accordance with the necessary evaluation as to the basis for location data collection and processing in the evolving paradigm of more ubiquitous computing. The review also discusses the intrinsic social processes that privacy and personal data protection rights facilitate and examines the between privacy, human relationships, intimacy and the development that supports autonomy in an individual's decision making.

Further enquiry then focuses on articulating the discoveries of prior scholarship in respect of the possible interferences into fundamental rights that monitoring of movement may effect, and asks whether new technologies may require a reassessment of the existing conceptual and legal frameworks in which location data is situated. The evaluation then appraises how historically the regulatory framework at the European level has framed privacy and personal data protection in relation to location data, and then appraises the suitability of more general provisions when applied to specific spatial and temporal concerns unique to the notion of safeguarding knowledge of an individual's whereabouts from other parties. The review provides a basis for more detailed reflection as to how stipulations relating to the collection and processing of location data have developed, and questions whether the existing nomenclature pertaining to location data proves cogent in terms of its application to the novel legal challenges presented by technological innovations.

It should be noted at this juncture that the study examines the existing legal instruments and court rulings adopted and in force to date at the regional level in Europe. The scope of the analysis extends to a review of the particular concerns pertaining to the collection and processing of location data, rather than adopt a broader assessment incorporating the specific issues that relate to data retention. The findings of the research do not extend to the implementation of reforms being made to personal data protection legislation at the regional level in the European Union by way of the new legislative package that shall shortly come into force, principally the General Data Protection Regulation (GDPR) and the Directive on data protection in law enforcement.⁹⁹ The basis for this limiting of scope is the necessity of utilizing established parameters, rather than contend with attempting to speculate how future legislative provisions will be applied. At the time that the author's research was being conducted discussions regarding the provisions to be enacted within the reform package at the EU level were still subject to review.

The second part of the thesis seeks to identify and appraise how the development of capabilities to collect and process location data may challenge existing precedents established in the existing jurisprudence in relation to the safeguard of fundamental rights. Firstly, the analysis assesses recent developments in respect of profiling citizens' behaviours, and examines whether parallels may be drawn with regard to creating profiles based on the processing of location data in an analogy to social network analysis. The two approaches to profiling share similar obstacles in certain respects, not least in terms of how we may conceive of, and conceptualise, any interference. Both methods portend challenges as regards the complexity of discerning the scope of any harm to welfare that data collection and processing activities may imply. The use of location data in relation to the analysis of mobility patterns for the purpose of predicting future behaviours of individuals and groups is discussed. The study then considers how profiling capabilities in relation to analysis patterns of citizens' movements in both public and private spheres will evolve with the roll out of the Internet of Things (IoT) into everyday life. Of particular interest to this review are concerns regarding the application of existing personal data protection laws that ideally provide the individual with the necessary certainty and foreseeability

⁹⁹ *See further:* European Council — Council of the European Union, Data protection reform, September 2016. Available at: <http://www.consilium.europa.eu/en/policies/data-protection-reform/>

as regards the collection and processing of their personal data. Immediate identifiable concerns include, *inter alia*, the pertinence of issues relating to informed consent of the data subject, data quality and purpose specification in data collection and processing. Having explored the privacy and data protection dimensions of IoT, the study then continues by examining the scope and content of the development of applying location data in the course of developing biometric identifiers. The review then contemplates how the expansion and advancement of processing capabilities in relation to more precise measurements of temporal and spatial attributes relating to an individual's location will potentially present acute challenges to the coherence of existing nomenclature in relation to the term 'location data'.

According to the structure outlined above, chapter two proceeds with a review of the development of the legal framework at the regional level in Europe in terms of personal data protection and privacy law. This analysis provides the context in chapter three for a more detailed examination of the scope of the regulations contained within existing legislation, constituting the structure by which the review then considers the development of the principal theories that have shaped the reasoning behind locational privacy as formulated in the legislative provisions. The discussion then elucidates how the paradigm of locational privacy is evolving, being shaped by advancements in technology, and contemplates how the discourse of prior scholarship has framed the reassessment of established conceptual approaches relating to the role of location privacy in human development, particularly as regards individual autonomy and identity formation.

Chapter four then continues the analysis by examining the adaptation of profiling techniques to incorporate the unique potential intrinsic to location data collected from individuals' respective patterns of mobility. With this sphere constituting a nascent field of technological development, the review adopts a somewhat novel approach to most studies on this subject, whereby it draws on comparable research conducted in respect of social network analysis; the two techniques inhering analytical methodologies that correspond in terms of the challenges they present by way of possible interferences into the fundamental rights of privacy and personal data protection. Chapter five of the study then applies the findings of the preceding chapter relating to profiling to the contextualisation of the changing nature of location data

collection and processing in the pervasive computing environment that the Internet of Things (IoT) has already begun to constitute. The review contemplates the very real challenges ubiquitous monitoring portends for both the individual and society at large.

Chapter six then continues by examining the use of the pervasive monitoring techniques enabled by IoT in the creation and application of behaviometrics. In the past research in biometrics focused on well-established physical biometrics such as, for example, iris scans. However, the increased sensitivity of embedded sensors, in conjunction with their greater ubiquity, has made integration of biometric technologies that collect location data a rapidly evolving sphere for innovation and development. The new systems being developed exploit physiological traits to allow for categorisation and identification of individuals and the remote collection of personal location data upon which behavioural attributes may be modelled. Chapter six concludes with a discussion of the implications of the wider use of location data in advancing biometric profiling methods, and reviews the concerns highlighted by the repurposing of data and the sensitivity of the use of biometric identifiers in revealing an individual's physical characteristics, which may in turn act as a proxy for other attributes. The final chapter, chapter seven, offers concluding remarks to this study, and elucidates an approach to resolving the challenges presented in articulating an appropriate application of the existing legal framework to the use of location data for the purposes of developing identifiers, metrics and profiles.

Chapter 2: The Development of a Framework for Personal Data Protection and Privacy as Rights in Europe

1. Introduction

Advances in data analysis have been such that more data, including location data, than ever before can be related to an individual and thus fall within the scope of safeguards outlined within data protection regulation. In addition, the growing ubiquity of interconnected, networked devices heralds an era of increasingly complex interactions between different technologies; this phenomenon potentially portends further challenges for the safeguard of the citizen's right to privacy.¹⁰⁰ This chapter examines the development of the legal framework of privacy and data protection law at the regional level in Europe. It reviews the inception of data protection as a concept, and then considers the appropriation of privacy as an established norm through which it could be safeguarded. It then considers the interpretation of a nexus between the two rights through which protection data functioned under the auspices of a broadly conceptualized right to privacy. It then further details the maturation of the principle whereby data protection constitutes a standalone right, distinct from that of its forebear in human rights law. The purpose of this appraisal is to highlight the historical foundations that underpin the foundational premises that structure the rights to privacy and the protection of personal data. The aim is to advance a more comprehensive understanding by which to appraise new developments and to consider, should issues arise, how the relevant principles to be applied have evolved and from whence may stem any deficiencies in their appropriateness to consider novel scenarios.

¹⁰⁰ Of note, then, is that the OECD indeed asserted in its recent review of its 1980 Guidelines that the "traditional concept of data controller (and data processor) may not be able to encompass all of the actors that may have a role to play in data protection." *See*: OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", OECD Digital Economy Papers, No. 176, OECD Publishing, p.4

1.1 The path to personal data protection in Europe

The move toward developing principles to guide the protection of individuals' personal data began to emerge in the late 1960s with the emergence of the first generation of mainframe computers. The advances in computerised processing in this period reflected wider developments in the era of the postindustrial information revolution and the greater use of personal data by public authorities.¹⁰¹ Early on it was acknowledged that, whilst gains in computing capabilities would allow for significant gains in efficiency in the processing of data, advancements might also risk the erosion of fundamental rights of data subjects if their personal data were to be misused.¹⁰²

Aware that growing government use of personal data might herald possible challenges to the safeguard of their citizens' rights, states began to respond by implementing investigatory panels and enquiries to determine possible policy and regulatory responses. West Germany took an early lead in initiatives to bring about safeguards, with consultations on the issues arising from data processing beginning in Germany in the Federal State of Hesse in 1969. The German region adopted a legal instrument instituting for the first time in law the German term *Datenschutz*, which would later be translated as 'data protection'.¹⁰³

Following the progress made by the states on instituting data protection law, in 1971 Germany's federal government commissioned additional research on a possible

¹⁰¹ See: Bennett, C.J., 1992. *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press; Bennett, C. J. 2001. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" pp. 99-125, in *Technology and Privacy: The New Landscape*, edited by P. E. Agre and G. Bramhall. Cambridge, Massachusetts: MIT.

¹⁰² See: OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", OECD Digital Economy Papers, No. 176, OECD Publishing, p.7

¹⁰³ The law was approved in October 1970 as the *Hessischer Datenschutzgesetz*, or 'Data Protection Act of Hesse'. See: *Hessischer Datenschutzgesetz vom. 7 October 1970* GVBl. II 300-10. The Act regulated the use of data retained in the regional government's filing system. See, further: Fuster, Gloria González. *The Emergence of Personal data Protection as a Fundamental Right of the EU*. Vol. 16. Springer Science & Business, 2014, p.56. See also: Bygrave, L.A., 2010. Privacy and data protection in an international perspective. *Scandinavian studies in law*, 56, p. 168; Bygrave, L.A., 2002. *Data protection law: approaching its rationale, logic and limits*. Kluwer Law Intl. For a detailed discussion of the *Hessischer Datenschutzgesetz* and its wider impact on the development of German data protection law, see: Burkert H. (1999) 'Privacy / Data Protection: A German/European Perspective' Proc. 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Mass., June 1999. Available at: <http://www.coll.mpg.de/sites/www/files/text/burkert.pdf>, pp.44-45

framework for federal data protection law. Interestingly, the review conducted by scholars at the University of Regensburg drew heavily from the theoretical research on privacy and data protection developed by Westin and Miller.¹⁰⁴ Across differing party lines a political agreement was reached in Germany's parliament in November 1976 with the Federal Data Protection Law, covering both public and private sectors, and enacted in January 1977: the *Gesetz zum Schutz vor Mißbrauch personenbezogener Date bei der Dateverarbeitung, Federal Data Protection Act* (BDSG), *Bundesgesetzblatt* (BGBl) 1, S 201.

In the United Kingdom the Younger Committee on Privacy published its report containing the evidence and conclusions of its enquiry into issues arising from data collection and processing in July 1972.¹⁰⁵ Concurrently, the Nordic Council also began discussion of data protection issues beginning in 1971, while at the national level in Sweden a Parliamentary Commission review panel had begun its work in 1969, publishing its report in 1972 entitled *Computers and Privacy*.¹⁰⁶ Further work at the domestic level in Sweden saw the first national law regulating data processing to be passed in Europe, entering into force in July 1973 - the *Datalag* (Data Act).¹⁰⁷ In the Netherlands, a review of data protection issues began in 1972 with the instigation of the State Commission Protection of Private Life in relation to Personal Data Registrations, which later reported its findings in 1976. Similarly, in 1972 a working group on *Informatique et vie privée* was established at the Ministry of Justice, to study

¹⁰⁴ The research group in particular was influenced by Miller's two works on computing and privacy, and Westin's seminal publication on privacy and liberty: Miller, Arthur R., *The Assault on Privacy: Computers, Data Banks and Dossiers*. Ann Arbor 1971; Miller, Arthur R., *Computer and Privacy*. In: *Michigan Law Review* 67 (1969), pp.1162- 1246; Westin, Alan F., *Privacy and Freedom*, 6th ed., New York 1970. *See also*: Burkert H. (1999) 'Privacy / Data Protection: A German/European Perspective' Proc. 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Mass., June 1999. Available at: <http://www.coll.mpg.de/sites/www/files/text/burkert.pdf>, p.49.

¹⁰⁵ *See*: UK Home Office, *Younger Committee's Report on privacy*, July 1972, Cmnd. 5012, Note: the report is not available online. However, Appendix B of the 1973 HEW Report from the United States contains a brief review of the UK's Younger Committee report.

<http://epic.org/privacy/hew1973report/appenb.htm>. *See also*: Dworkin, Gerald. "The Younger Committee Report on Privacy." *The Modern Law Review*, vol. 36, no. 4, 1973, pp. 399-406. <http://www.jstor.org/stable/1093890>.

¹⁰⁶ *See*: Gloria González, *The Emergence of Personal data Protection as a Fundamental Right of the EU*. Vol. 16. Springer Science & Business, 2014, p.47

¹⁰⁷ For further discussion of the Swedish *Datalag* and its influence on other European jurisdictions' development of data protection law, *see*: Burkert H. (1999) 'Privacy / Data Protection: A German/European Perspective' Proc. 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Mass., June 1999, pp.47-48.

possible issues arising from the increasing use of computers in public administration operating under existing French legislation. The study indeed inferred that additional new legislation was necessary.¹⁰⁸

Subsequently, a further committee established at the French Ministry of Justice in 1974, named the *Commission informatique et libertés*, was tasked with recommending the scope of measures to be taken in terms of instituting further regulatory provisions regarding data processing. Of note, in respect of the work then conducted by the Paris-based committee, was its close review of the efforts of such international bodies as UNESCO, the OECD and the Council of Europe with regards to their work on aligned data processing-related concerns.¹⁰⁹ The findings of this commission and other enquiry later influenced the Law on Informatics and Freedom in 1978¹¹⁰, and the creation of the French data protection agency *La Commission nationale de l'informatique et des libertés* (CNIL).¹¹¹

At the same time, in the United States the Secretary of the Department of Health, Education and Welfare (HEW) Elliot Richardson established the 'Committee on Automated Personal Data Systems' in response to the expanding use of automated systems processing the personal data of individuals in both public and private sector organizations. The 1973 report, entitled '*Records, Computers and the Rights of Citizens*' was especially notable for its initial proposition of the Fair Information Practices (FIPs), created as a set of principles for protecting the privacy of personal data in record-keeping systems.¹¹² That there were two committees reviewing data processing in the UK and the United States (the Younger Committee in the UK, and the US HEW's Committee on Automated Personal Data Systems) is especially interesting in respect of the policy discussion on privacy and data processing at the

¹⁰⁸ See: González G., *The Emergence of Personal data Protection as a Fundamental Right of the EU*. Vol. 16. Springer Science & Business, 2014, p.62

¹⁰⁹ See: OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", OECD Digital Economy Papers, No. 176, OECD Publishing, p.7

¹¹⁰ *Loi Informatique Et Des Libertés*, Act N°78-17, 6 January 1978, On Information Technology, Data Files And Civil Liberties. Available at: <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf>

¹¹¹ France was especially sensitive to data protection concerns following revelations regarding a proposal to use personal identifiers to cross-reference a number of databases and public registers holding personal data on citizens, which had led to the Tricot Commission being established in 1974.

¹¹² US Dept of Health, Education, and Welfare - United States of America. "Records Computers And The Rights Of Citizens." (1973). Available at: <http://epic.org/privacy/hew1973report/default.html>

time; the deliberations of the committees on both sides of the Atlantic appear to have influenced each other. The UK's Younger Committee recommended specific safeguards for automated personal data systems that bare a resemblance indeed to many of the protections articulated in the Fair Information Practices (FIPs) report published by the Committee created by the US Secretary of the Department of Health, Education and Welfare.¹¹³ The 1973 report of the Committee on Automated Personal Data Systems strongly influenced the drafting of the United States Privacy Act in 1974.¹¹⁴ The Privacy Act of 1974, 5 U.S.C. § 552A establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.¹¹⁵

1.2 The OECD Guidelines and the international dimension to data processing regulation

With different nations enacting their own privacy laws instituting provisions to regulate data processing, various institutions began to examine the broader international implications of such regulation. Indeed, by 1980 more than one third of the member countries of the OECD had adopted national legislation, including the European nations of Germany, Norway, Denmark, Austria and Luxembourg.¹¹⁶ At the same time, it should be noted that whilst each jurisdiction in question had enacted its own specific regulations, scholars have nonetheless noted that by the mid-1970s a striking level of agreement had been developed across different advanced economies as to establishing principles relating to the functioning of data systems; in turn influencing the legislative processes and bringing about a relatively large degree of consistency in the respective laws passed.¹¹⁷

¹¹³ See: Bennett, C.J., 1992. *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press, p. 99. See also: Gellman, R., 2015. Fair information practices: A basic history. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020, p.4

¹¹⁴ See: Gellman, R., 2015. Fair information practices: A basic history. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020, pp.4-5;

¹¹⁵ See: US DOJ, Privacy Act of 1974, 5 U.S.C. § 552a, Available at: <https://www.justice.gov/opcl/privacy-act-1974>

¹¹⁶ See: OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", OECD Digital Economy Papers, No. 176, OECD Publishing, p.8

¹¹⁷ See: McAdam, D., Stearns L. & Uglow D., *The politics of privacy: Planning for personal data systems as powerful technologies*. (New York: Elsevier, 1980), p. 111.

As early as 1969 the OECD had undertaken the study of the implications for privacy of transborder data flows and the importance of information and communications technologies in facilitating such transfers. Following a major symposium in 1977 on ‘Transborder Data Flows and the Protection of Privacy’, an Expert Group was established to begin working on developing international guidelines to address the increasing use of personal data and the growing reliance being placed upon computerised processing. Discussions reflected a more general understanding that efforts to develop greater coherency and uniformity across jurisdictions would prove beneficial for the states parties.¹¹⁸

The adoption by the OECD of the Privacy Guidelines constituted a significant landmark in terms of its promotion of a broad consensus on key principles and constituting the first attempt to deal with transborder data flows from a global perspective. The Guidelines articulate a set of non-binding principles that aim to encourage acceptance of specific minimum standards of personal data protection and privacy while at the same time pursuing the objective of eliminating the conditions that might otherwise prompt nations to restrict transborder data flows.¹¹⁹ The 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* represented the OECD member countries’ consensus on the handling and protection of personal data. The development of the Guidelines reflected a growing appreciation amongst the member states of the OECD that, in developing regulations, inconsistencies between different jurisdictions’ competing domestic national data protection legislation could create problems for the protection of privacy and individuals’ liberties.¹²⁰

It should be noted, however, that even at this early juncture of negotiation of international instruments on data protection and privacy and, even while its provisions are non-binding on member countries, reaching agreement on the principles was not a

¹¹⁸ See: OECD (2011), “The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines”, OECD Digital Economy Papers, No. 176, OECD Publishing, pp.9-10

¹¹⁹ See: Kuner, C. (2011), “Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future”, OECD Digital Economy Papers, No. 187, OECD Publishing. Available at: <http://dx.doi.org/10.1787/5kg0s2fk315f-en>, p.14

¹²⁰ See: OECD (2011), “The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines”, OECD Digital Economy Papers, No. 176, OECD Publishing, p.7

simple task. According to the chairperson of the Expert Group of the OECD, the Honourable Justice Michael Kirby, the Guidelines reflect carefully crafted compromises, whilst the text also proves illustrative of the differing views of the members of the Expert Group on potentially contentious issues.¹²¹ Indeed, this observation is clearly evidenced in the Council Recommendation that notes the divergence of national law and policies, and recognises the challenge of: “...reconciling fundamental but competing values such as privacy and the free flow of information”.¹²²

Although the Guidelines’ eight basic principles do not refer to sensitive data or to automated processing, the Scope section suggests that “different protective measures” can be applied based on the context or the sensitivity of the personal data, and recognises that some member countries may choose to limit the application of the Guidelines to the automatic processing of personal data. It should be noted that within the eight basic principles of the Guidelines no reference is made either to sensitive data or to automated processing. However the section of the Guidelines that elaborates their scope notes that “different protective measures” may be applied based on either context or sensitivity of personal data concerned, while also acknowledging that member countries may wish to limit their application of the Guidelines to automatic processing of personal data.¹²³

¹²¹ See: Honourable Justice Michael Kirby, “Privacy Protection – A New Beginning”, presentation to the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September, 1999. Available at: www.austlii.edu.au/au/journals/PLPR/1999/41.html. Of note too is that the chair of the Expert Group, Justice Kirby, has suggested that their work drew in part on parallel discussions at both the Council of Europe, and the Nordic Council. See also: OECD (2011), “The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines”, OECD Digital Economy Papers, No. 176, OECD Publishing, p.10

¹²² See: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Council Recommendation, RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (23 September 1980); OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - The Explanatory Memorandum, 23 September 1980, Available at: <https://www.oecd.org>

¹²³ One should note how the Explanatory Memorandum of the Guidelines resolves to frame ‘the problems’ they instrument attempts to address; the level of detail at which such problems are addressed; and the means by which its guidance should be applied. Inter alia, of particular note are the following provisions:

I. GENERAL BACKGROUND

The problems

(3). As far as the legal problems of automatic data processing (ADP) are concerned, the protection of privacy and individual liberties constitutes perhaps the most widely debated aspect. Among the reasons for such widespread concern are the ubiquitous use of computers

Marking the 30th anniversary of the Guidelines, an Expert Group convened by the OECD and chaired by Privacy Commissioner of Canada Jennifer Stoddart embarked on their review. The OECD Expert Group ultimately recommended the Guidelines be updated in specific key areas. However, of particular note is that the Expert Group recommended that the core eight basic principles at the heart of the Guidelines be retained without amendment. Thus in July 2013 the OECD Council adopted a revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, following the recommendations given by the Expert Group.¹²⁴

1.3 COE - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

While Convention 108 differs from the OECD Guidelines in a number of significant respects (for example: its binding character, and its treatment of sensitive data and application to automated processing) nonetheless the foundational principles of the

for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data...

Level of detail

27. The level of detail of the Guidelines varies depending upon two main factors, viz. (a) the extent of consensus reached concerning the solutions put forward, and (b) available knowledge and experience pointing to solutions to be adopted at this stage. For instance, the Individual Participation Principle (Paragraph 13) deals specifically with various aspects of protecting an individual's interest, whereas the provision on problems of choice of law and related matters (Paragraph 22) merely states a starting-point for a gradual development of detailed common approaches and international agreements. On the whole, the Guidelines constitute a general framework for concerted actions by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation.

Paragraph 3: Different degrees of sensitivity

45. The Guidelines should not be applied in a mechanistic way irrespective of the kind of data and processing activities involved.

OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - The Explanatory Memorandum, 23 September 1980, Available at: <https://www.oecd.org/>.

¹²⁴ OECD, OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, as amended on 11 July 2013, Available at: www.oecd.org/. See also: Cate, Fred H., Peter Cullen, and Viktor Mayer-Schönberger. "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines." Available at:

www.oii.ox.ac.uk/.../Data_Protection_Principles_for_the_21st_Century.pdf (2014).

two instruments exhibit a great deal of consistency.¹²⁵ Convention 108 asserts as its objective: “The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (‘data protection’).”¹²⁶ Those drafting the Convention 108 selected language of a broad scope; in particular, the definition of “personal data” being “any information relating to an identified or identifiable individual”,¹²⁷ while “automatic processing” is framed as the automation in whole or in part of “storage of data, carrying out of logical and/or arithmetical operations on those data, [or] their alteration, erasure, retrieval or dissemination.”¹²⁸

The Convention constituted the first international treaty on data protection of a legally binding nature. *Inter alia*, Convention 108 is notable for its articulating binding principles addressing data quality (Article 5), data security (Article 7) and special categories of data (Article 6). Furthermore, the treaty is also progressive in its articulation of additional safeguards for the data subject in respect of subject access rights (Article 8). Article 8 of the Convention is particularly noteworthy in the extent to which it articulates the right of the data subject to establish the existence and main purposes of an automated personal data file, confirm whether personal data relating to the data subject are stored in the file; to review the data and, where appropriate, to rectify or erase the data, in conjunction with establishing the right of the data subject to a remedy where there is a failure in compliance with other rights granted by the instrument.¹²⁹

¹²⁵ The eight principles set out by the OECD are: 1) collection limitation; 2) data quality; 3) purpose specification; 4) use limitation; 5) security safeguards principle; 6) openness principle; 7) individual participation; and 8) accountability, *See*: OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, Available at: <https://www.oecd.org>

¹²⁶ Council of Europe - ETS no. 108 - Convention for the Protection of Individuals with regard to automatic Processing of Personal Data, 28 January 1981, Article 1. Note: The Convention entered into force on 1 October 1985.

¹²⁷ Council of Europe - ETS no. 108 - Convention for the Protection of Individuals with regard to automatic Processing of Personal Data, 28 January 1981, Article 1. Note: The Convention entered into force on 1 October 1985, Article 2(a).

¹²⁸ Council of Europe - ETS no. 108 - Convention for the Protection of Individuals with regard to automatic Processing of Personal Data, 28 January 1981, Article 1. Note: The Convention entered into force on 1 October 1985, Article 2(c).

¹²⁹ Gellman maintains that we need recognise the importance of the earlier work in the United States developing the fundamental concepts outlined within the FIPs, stating that both the Council of Europe Convention and the OECD Guidelines “relied on FIPs as core principles, although neither document used the term. Both organizations revised and extended the original U.S. statement of FIPs”. *See*:

Convention 108's Chapter II, which outlines the basic principles for data protection, is especially notable for its articulation of requirements relating to data quality, automatic data processing and sensitive data in Article 5 and Article 6. According to Article 5, data subject to automatic processing shall be:

- a. "obtained and processed fairly and lawfully;
- b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored;
- d. accurate and, where necessary, kept up to date;
- e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.¹³⁰

In a further innovation, Article 6 introduced the concept of "special categories of data" to the regulatory framework at the European level. According to the provisions of Article 6, sensitive data must not be processed unless the relevant domestic legislation provides sufficient safeguards.¹³¹

In 2001, Convention 108 was further supplemented with the addition of a protocol that directed parties to create within their jurisdiction a data protection authority. The Additional Protocol also added new limitations on data transfers. It should be noted that the amendments brought about by the Additional Protocol reflected changes occurring in the regulatory framework of the EU on data protection that strengthened

Gellman, R., 2015. Fair information practices: A basic history, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020, p.8. The Privacy Act of 1974 mandates the application of the FIPs to the work of federal agencies in the United States: Privacy Act of 1974, 5 U.S.C. § 552a Gellman notes that the findings and the purposes of the original Act provisions of the Act – Public Law 93-579 – reflect the influence of the HEW Advisory Committee, with Congress basing substantive provisions for the most part on the report published by the Committee. *See:*

Gellman, R., 2015. Fair information practices: A basic history. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020, p.10

¹³⁰ Council of Europe - ETS no. 108 - Convention for the Protection of Individuals with regard to automatic Processing of Personal Data, 28 January 1981, Article 5.

¹³¹ Council of Europe - ETS no. 108 - Convention for the Protection of Individuals with regard to automatic Processing of Personal Data, 28 January 1981, Article 6: "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."

the authority of agencies across the Member States charged with oversight of data protection and addressed the increasing volume and challenges associated with data exportation.¹³²

2. The EU Data Protection Framework

With the Maastricht Treaty establishing the European Union the Commission's focus expanded, allowing for a greater emphasis to be played in its role protecting the fundamental rights of European citizens.¹³³ Owing to the great variation in domestic laws and the uneven application of the provisions relating to data protection outlined in the OECD Guidelines and Convention 108, the then Commission of the European Community published its draft Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data.¹³⁴ It should also be mentioned in this context that the varying degrees of protection afforded personal data across the Member States also proved a motivation for the drafting of the Directive as a response.¹³⁵

2.1 The Data Protection Directive 95/46/EC

In 1995 the EU Data Protection Directive (Directive 95/46/EC) therefore introduced data protection principles within EU law and established the foundation for the main benchmarks safeguarding the protection of personal data within the EU.¹³⁶ Directive

¹³² Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Nov. 8, 2001, C.E.T.S. No. 181, available at <http://conventions.coe.int/treaty/en/treaties/html/181.htm>.

¹³³ Consolidated Version of the Treaty of European Union, Feb. 7, 1992, 2008 O.J. (C 115) 13 [hereinafter Treaty on European Union], Available at: <http://eur-lex.europa.eu/>

¹³⁴ See: Cate, F.H., 1994. EU Data Protection Directive, Information Privacy, and the Public Interest, *The Iowa L. Rev.*, 80, p.432. Note: refer also to: Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal data and on the Free Movement of Such data, COM (92) 422 final at 30 (note: the amended version was submitted by the Commission on October 16th 1992).

¹³⁵ For example, one may cite the concerns raised by France data protection authority CNIL with regard to cross border transfers between subsidiaries of multinational companies and, in particular, with respect to concerns raised in 1989 by FIAT's activities between France and Italy. *Commission Nationale de l'informatique et des libertés* (CNIL), 10eme rapport d'activité, Paris, (1989), p. 32

¹³⁶ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

95/46/EC addressed the then evident need to establish a regional legal framework where, up until that point, regulatory provisions on data protection had been left open to the enterprise, and interpretation, of national legislative initiatives. The approach of Directive 95/46/EC is to carefully resolve the inherent tensions between the establishing of norms relating to personal data protection, workable exceptions to such norms where appropriate, and the need to secure the free movement of data — addressing the EU’s economic priorities in relation to promotion of trade within the single market. Particularly important in respect of the broader framework of the rights of data subjects provided for by Directive 95/46/EC are its references to Article 8 of the ECHR and the privacy safeguards articulated in COE Convention 108.¹³⁷ Moreover, Article 1 reaffirms this emphasis stating, as a principal object of the Directive: “(1). In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”¹³⁸

A critical consideration when reviewing the scope of the provisions articulated within Directive 95/46/EC is that the regulations reflect the directive being instituted when the European Community’s pillar structure was in place. During this era the divisions between the respective pillars: Community law (first pillar), foreign and common security (second pillar), and justice and internal affairs (third pillar) were distinct and, as such, with Directive 95/46/EC having its foundation under the first pillar, Directive 95/46/EC to an extent thus prioritises data processing and the free movement of data, as opposed to making the protection of individuals with regard to the processing of personal data its primary objective.¹³⁹ Notwithstanding the limitations inherent to Directive 95/46/EC, it nevertheless is still regarded as a major advancement in

¹³⁷ Directive 95/46/EC

Preamble, Recital 10: “Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law...”

Preamble, Recital 11: “Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;...”

¹³⁸ Directive 95/46/EC, Article 1 (1).

¹³⁹ See: Galetta, A. and De Hert, P., 2015. The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-Oriented Remedial System?. *Review of European Administrative Law*, 8(1), pp.125-126

developing the scope of data protection as a fundamental right at the EU level.¹⁴⁰

Article 7 of EC/95/46/EC is significant for its inclusion of the provision outlining the need for the data subject to provide their consent to ensure that data processing shall be legitimate.¹⁴¹ Of note with regard to the inclusion under Article 7 of the Data Protection Directive is the observation that the regulation does not provide any elucidation as to the conditions under which consent may be required absent any ambiguity i.e. that that the data subject has given her consent “unambiguously”. However, various parties have provided guidance as to how this clause may be interpreted. For example, the European Data Protection Supervisor (EDPS) has asserted that: “Before a data subject can be considered to freely have given consent to a specific processing operation, he or she must receive sufficient information to be able to understand the scope and consequences of consent...”. Furthermore, the EDPS also noted that: “Apart from having to be given freely, consent must be specific and there may be no doubts as to whether it was given or not. Moreover, consent is strictly linked to the processing that the data subject was informed of.”¹⁴²

¹⁴⁰ See: Gloria González Fuster & Raphaël Gellert, The fundamental right of data protection in the European Union: in search of an uncharted right, *International Review Of Law, Computers and Technology* Volume 26, Issue 1, 2012, pp. 73-82.

¹⁴¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 7:

Member States shall provide that personal data may be processed only if:

- (a) the data subject has unambiguously given his consent; or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

¹⁴² EDPS, Legitimate Reasons For Processing Of Personal Data, Available at:

<https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA6>. Interestingly, the WP29 notes in its Opinion on the definition of consent that there has indeed existed some uncertainty as to how consent may be expressed, noting *inter alia* that: “The legislative history of Directive 95/46/EC shows relative consensus on the conditions of valid consent, namely: freely given, specific and informed. However, it also shows some uncertainty over the ways in which consent may be expressed - whether it has to be explicit, written, etc.”

See: WP29, Opinion 15/2011 on the definition of consent, 13 July 2011, 01197/11/EN WP187, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf, p.5. Refer also the discussion of the Council’s as to the basis of their position in relation to consent, articulated in the Common Position of the Council on the proposal for a Parliament and Council Directive on the

2.2 Directive 2002/58/EC

Directive 2002/58/EC on Privacy and Electronic Communications has as its objective the safeguard of citizens' privacy and the regulation of the processing of personal data in the electronic communications sector. Directive 2002/58/EC is a complement to Data Protection Directive 95/46/EC whilst at the same time constituting a part of the Regulatory Framework for Electronic Communications. Directive 2002/58/EC provides, *inter alia*, specific guidance as to how the principles of Directive 95/46/EC are to be applied to the electronic communications sector.¹⁴³

Within the scope of Directive 2002/58/EC are services consisting wholly or mainly in the conveyance of signals as opposed to, for example, the provision of content. Critics such as Kosta and Dumortier, however, have noted that the definition of the scope of application of Directive 2002/58/EC are ambiguous, noting that the notion of "electronic communications service" is limited in scope by the definition provided in Directive 2002/21/EC Article 2(c), severely curtailing the extent to which the Directive's provisions made be applied.¹⁴⁴

Mirroring the approach adopted by Directive 95/46/EC, the preamble to the 2002 ePrivacy Directive also referenced the directive's observance of the principles and safeguards encompassed within both the EuCFR and the ECHR.¹⁴⁵

protection of individuals with regard to the processing of personal data and the free movement of such data, (00/287) COD, adopted on 15/03/95. While the position paper indeed provides a degree of guidance in respect of the articulation as to the need for "explicit consent" in relation to the legitimate processing of sensitive data (Article 7), its more general observations vis-à-vis the scope for providing valid consent is somewhat lacking. Page 4 states, somewhat obliquely that: "... a number of amendments have ... been made to ... introduce a measure of flexibility which guarantees equivalent protection ... but does not lead to any lowering in the level of protection; they allow the general principles to be applied in an efficient and non-bureaucratic way in keeping with the wide variety of ways in which ... data are processed."

¹⁴³ See: Directive 2002/58/EC - Article 1 (2), stating: "The provisions of this Directive particularise and complement Directive 95/46/EC...". Also of relevance in this context is Recital 10 of Directive 2002/58/EC, which affirms the respective scopes and application of the two directives: "In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services."

¹⁴⁴ See: Kosta, E. and Dumortier, J., 2015. ePrivacy Directive: Assessment of transposition, effectiveness and compatibility with the proposed Data Protections Regulation, p.8

¹⁴⁵ Directive 2002/58/EC, Preamble, Recitals (2) and (3).

(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this

Unlike the Data Protection Directive (95/46/EC) which does not articulate a definition for ‘location data’ (on the basis that the legislation relates to data processing and personal data protection in its widest context, rather than it constitute a framework for privacy in the electronics communications sector), importantly Directive 2002/58/EC requires that a definition of ‘location data’ be provided. Recital 14 of 2002/58/EC provides the original elucidation of the technical parameters of the term in the following description:

“Location data may refer to the latitude, longitude and altitude of the user’s terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.”¹⁴⁶

In Recital 35 of Directive 2002/58/EC the text provides an outline of the context in which location data is processed in respect of electronic communications networks:

“In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers.”

The above note is important insofar as Directive 2002/58/EC constitutes a revision to Directive 97/66/EC, which originally sought to translate the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector. Indeed, the

Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.
(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

¹⁴⁶ Directive 2002/58/EC, Preamble - Recital 1

basis on which this requirement for a revision of the regulations was instituted is framed in respect of technological advancements in the use of public communications networks (see Recital 5 of Directive 2002/58/EC, which notes, *inter alia*: “New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services.”

Importantly, Directive 2002/58/EC provides additional definitions to complement those already outlined in Directive 95/46/EC and in Directive 2002/21/EC. *Inter alia*, Article 2 states:

2(b) “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) “location data” means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;¹⁴⁷

With respect to data processing by providers of electronic communications networks and services, of specific concern in relation to traffic data and location data are Articles 6 and 9 of Directive 2002/58/EC. These articles articulate the requirements to be applied to these specific two types of personal data.¹⁴⁸

¹⁴⁷ Directive 2002/58/EC, Article 2

¹⁴⁸ Article 6

Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).
2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.
3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

Articles 6 and 9 of the ePrivacy Directive are particularly significant where we consider the application of the provisions of the Directive as a whole, for they provide a justification for distinguishing between different technologies such that, from a functional perspective, the application of legal protection to a data subject's traffic or location is dependent upon the context of the service and the data processing taking place. This differentiation in applicability of these provisions has been the subject of discussion vis-à-vis its coherency, particularly as regards its application in the light of the development of new technologies and services.¹⁴⁹ Scholars Kosta and Dumortier, for example, have highlighted in their scholarship their conviction that Article 6 of Directive 2002/58/EC, relating to the processing of traffic data, and Article 9, regarding location data other than traffic data, both provide too limited a scope in

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 9

Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple he network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

¹⁴⁹ See: Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. C 128 of 6 June 2009, p. 36.

their interpretative accounts of the two terms, which lead to instances where traffic data or location data may receive divergent standards of legal protection when subject to processing in very similar services from both a contextual and functional perspective.¹⁵⁰

Also of note is that Directive 2002/58/EC maintained the technology-neutral approach to regulation of earlier legislation, including that which it replaces (Directive 97/66/EC). Directive 2002/58/EC, Recital 4 states:

“Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used.”

The aforementioned point is especially salient in the context of our considering Recital 10, which affirms that Directive 95/46/EC shall be applied “in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.”¹⁵¹ The latter point is a critical detail insofar as it underscores the crucial distinction drawn between the scope of the legislative provisions vis-à-vis their applicability to public communications services and, conversely, to non-public communications services.” The pertinence of this observation lies in its illuminating a fundamental contention; namely that the provenance of the term ‘location data’ originates from regulation concerning electronic communications services. In particular, much of the impetus behind the implementation of Directive 2002/58/EC was the growth in new digital technologies introduced in public communications services accessed through digital mobile networks (see Directive 2002/58/EC Recitals 4-7 inclusive).

¹⁵⁰ See: Kosta, E. and Dumortier, J., 2015. ePrivacy Directive: Assessment of transposition, effectiveness and compatibility with the proposed Data Protections Regulation, p.9

¹⁵¹ Directive 2002/58/EC, Recital 10

That the initial articulation of location data in Directive 2002/58/EC was however deficient is evidenced in the selectivity of the legislation's articulation of the utility of the data concerned. Recital 35, for example, refers only the spatial criterion of location data (the "geographic position") relating to the terminal equipment of the mobile user, rather than the temporal aspect that relates to timing. Having recognised the scope of the different attributes of location data in Recital 14, this oversight is somewhat surprising. The omission reflects a problematic tendency toward simplifying the interpretation of both the term and the underlying concepts that 'location data' inheres and defines. This reductive process renders the simplified form, and our understanding, as far too unexact for the purposes of our examining the processes location data is subject to. In essence, our analysis must apprehend the vital importance of appreciating the duality of purpose of the data concerned i.e. that intrinsically this data inheres both temporal and spatial criteria.

2.3 Directive 2009/136/EC

The replacement of Directive 2002/58/EC by Directive 2009/136/EC was made on account of the need to update the legislative framework, implementing a series of amendments to the existing laws regarding electronic communications and data privacy. Article 3 outlines the wider nature of the scope of the new Directive, stating that the provisions of the e-Privacy Directive are applicable to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices."¹⁵² In keeping with the notion articulated by Recital 13 of Directive 2009/136/EC, definitions also "need to be adjusted so as to conform to the principle of technology neutrality and to keep pace with technological development." It should be noted in this context that the scope of the definition of "location data" as articulated by Article 2(c) of Directive 2002/58/EC was widened by Directive 2009/136/EC; in addition to data processed in an electronic communications network, data processed by an electronic communications service is also covered by the

¹⁵² Directive 2009/136/EC, Article 3

term.¹⁵³

2.4 Charter of Fundamental Rights of the European Union (EUCFR)

In June 1999 the EU Heads of State or Government attending the Cologne European Council agreed to the establishment of a Charter of the Fundamental Rights of the Union.¹⁵⁴ Later that year the Working Party 29 recommended that the European Commission, the European Parliament and the Council of the European Union include a right to data protection in the then recently-proposed EU charter on fundamental rights. WP29 highlighted its view that, with the growth of the information society, the right was of increasing importance to citizens in Europe.¹⁵⁵ This decision followed a long debate within Europe as to the structure by which recognition of fundamental rights within the European Union should be formalised. The Charter, promulgated at the Nice Council in December 2000, would include a provision by which Article 8 duly recognised and delineated data protection of its own accord, expressly distinguishing the fundamental right from that of privacy, covered by Article 7 of the Charter.¹⁵⁶

The European Charter of Fundamental Rights, Article 8 stipulates:

“Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid

¹⁵³ Directive 2009/136/EC, Article 2:

Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications)
Directive 2002/58/EC (Directive on privacy and electronic communications) is hereby amended as follows:

2) Article 2 shall be amended as follows:

(a) point (c) shall be replaced by the following:

‘(c) “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;’

¹⁵⁴ Conclusions of the European Council in Cologne, 3 and 4 June 1999, Annex IV.

¹⁵⁵ WP29, ‘Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights’, 5143 /99/EN WP 26, 7 September 1999, available at: <http://ec.europa.eu/justice/data-protection/article-29/>, p. 2.

¹⁵⁶ Charter of Fundamental Rights of the European Union. Published in the Official Journal of the European Communities, 18 December 2000 (2000/C 364/01). The Charter became legally binding when the Treaty of Lisbon entered into force on 1 Dec. 2009.

down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.”¹⁵⁷

The Charter thus not only explicitly articulates a right to data protection in Article 8(1), but additionally outlines key data protection principles in Article 8(2). Lastly, Article 8(3) of the provision within the EUCFR also ensures the requirement that an independent authority control the implementation of these principles.

2.5 The Lisbon Framework and TFEU Article 16: Consolidation of the Right to Data Protection at the EU Level

The signing of the Treaty of Lisbon in 2007, which entered into force in December 2009, substantially overhauled the pillar structure of the EU and established a new legal foundation, heralding therefore fundamental changes in the Union’s system of data protection. Article 16 TFEU of the treaty replaced the treaty provision regarding data protection in the First Pillar (Article 286 EC) such that data protection is now applicable in all EU sectors.

Article 16 TFEU states:

“1. Everyone has the right to the protection of personal data concerning him or her.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on the European Union.”¹⁵⁸

¹⁵⁷ Charter of Fundamental Rights of the European Union, Article 8

¹⁵⁸ Treaty Of Lisbon Amending The Treaty On European Union And The Treaty Establishing The

Article 16 TFEU is important in that it provides the basis upon which the existing deficiencies in the current regulation of data protection may be addressed through the establishment of a new, overarching legislative framework across all sectors. The provision is also significant in that it further signifies the differentiation of data protection as an explicit right distinct from that of the right to privacy. The right to data protection is further reinforced by the revised Article 6 TEU, which asserts that the EUCFR “shall have the same legal value” as the TEU and the TFEU.¹⁵⁹ The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties.

Article 16 of the TFEU provides that Parliament and the Council lay down rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law. The pillar structure disappeared with the Lisbon Treaty, while also stipulating new powers for the European Parliament, which has become co-legislator. The Commission has stated that this revision “provides a stronger basis for the development of a clearer and more effective data protection system.”¹⁶⁰

2.6 The Comprehensive Reform of EU Data Protection Rules

In January 2012 the European put Commission proposed a “comprehensive reform of data protection rules”.¹⁶¹ Noteworthy in the Commission’s announcement is that its intention to institute the inaction of “comprehensive reform of the EU’s 1995 data protection rules to strengthen online privacy rights”, further stating that:

European Community, (2007/C 306/01), Article 16 TFEU

¹⁵⁹ Treaty Of Lisbon Amending The Treaty On European Union And The Treaty Establishing The European Community, (2007/C 306/01), Article 6(1) TFEU

¹⁶⁰ See: European Parliament, Personal Data Protection: Fact Sheets on the European Union - 2016, February 2016, Available at: www.europarl.europa.eu

¹⁶¹ EU Commission, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses - PRESS RELEASE, 25 January 2012, Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

“Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used.”¹⁶² It should be noted that the announcement followed on from previous initiatives of the Commission to set in motion a process of reform, including its November 2010 strategy to strengthen EU data protection rules.¹⁶³

At this juncture it is necessary to note, however, that while this initiative is of course significant, it should be mentioned that the reform effort would also in time include further proposals vis-à-vis complementary legal instruments to include the e-Privacy Directive¹⁶⁴ for the communications sector and the specific rules for the protection of personal data in police and judicial cooperation in criminal matters (Framework Decision 2008/977/JHA).¹⁶⁵ Following the proposal for a Regulation for a general framework of data protection in the EU (the future GDPR), the Commission set out a second proposal for a Directive on protecting personal data processed for law enforcement purposes to replace Framework Decision 2008/977/JHA. It was envisaged from the outset that the scope of the proposed Directive would be broader in scope than that of the existing Framework Decision, as it was intended to cover domestic processing operations in addition to “cross-border” data transfers (with only

¹⁶² EU Commission, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses - PRESS RELEASE, 25 January 2012, Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

¹⁶³ See: EU Commission, European Commission sets out strategy to strengthen EU data protection rules - PRESS RELEASE: IP/10/1462, 4 November 2010, Available at: http://europa.eu/rapid/press-release_IP-10-1462_en.htm?locale=en; See also: EU Commission, Data protection reform – frequently asked questions - PRESS RELEASE: MEMO/10/542, 4 November 2010, Available at: http://europa.eu/rapid/press-release_MEMO-10-542_en.htm?locale=fr. The Commission noting that: “The goals were to protect individuals' data in all policy areas, including law enforcement, while reducing red tape for business and guaranteeing the free circulation of data within the EU. The Commission invited reactions to its ideas and also carried out a separate public consultation to revise the EU's 1995 Data Protection Directive (95/46/EC).” See: EU Commission, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses - PRESS RELEASE, 25 January 2012, Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

¹⁶⁴ The proposal for a Regulation on Privacy and Electronic Communications was published by the Commission on January 10th 2017. For the draft text, see further: EU Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 10 July 2017, Available at: <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications>

¹⁶⁵ See: EU Commission, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses - PRESS RELEASE, 25 January 2012, Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

the latter having been covered to date).¹⁶⁶

3. The Right to Privacy

The United Nations (UN) Universal Declaration of Human Rights (UDHR) of 1948 was the first international legal instrument in which the individual's right to the safeguard of their private sphere against intrusion was first articulated. Article 12 of the Declaration states:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”¹⁶⁷

3.1 The International Covenant on Civil and Political Rights (ICCPR)

The International Covenant on Civil and Political Rights, which was adopted by the UN General Assembly in 1966 and has to date been ratified by 168 States, provides in article 17 of the Convention that: “no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation”. It further states: “everyone has the right to the protection of the law against such interference or attacks.”¹⁶⁸ The report

¹⁶⁶ See: ECLAN, EU 2016/680 Directive, 27 April 2016, Available at: <http://eur-lex.europa.eu/legal-content>. Following trilogue negotiations between the European Parliament, the Commission and the Council lasting a period of three years, agreement was reached as to the final text of the Police and Criminal Justice Authorities Directive in relation to data protection in the police and justice sectors. Member States of the EU have a two-year period to implement the Directive 2016/680 into domestic law. Member States are required to adopt any relevant legislative acts for compliance with the Directive by 6th May 2018. The Commission released a communication to confirm its support for this agreement on 11 April 2016. As no amendment was adopted by the Council, its position at first reading was approved by the European Parliament. The final text of the Directive was released on 27 April 2016, with Directive 2016/680 being published in the official journal on 4 May 2016 (OJ L 119). See: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 27 April 2016, Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG.

¹⁶⁷ United Nations (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948.

¹⁶⁸ UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, Available at: <http://www.refworld.org/docid/3ae6b3aa0.html>.

General Comment No. 16 of the UN Human Rights Committee on Article 17 (Right to Privacy) of the ICCPR noted that, in the view of the Committee, “the expression “arbitrary interference” can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.”¹⁶⁹ A further point raised by the Human Rights Committee in General Comment No. 16 of relevance to the consideration of the safeguard of privacy in the broader context of personal data collection and processing vis-à-vis the requisite functions public authorities may perform, whereby the HRC stated: “As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual’s private life the knowledge of which is essential in the interests of society as understood under the Covenant.”¹⁷⁰ General Comment No. 16 of the UN Human Rights Committee also provides further guidance as to the scope of the right to privacy enshrined in Article 17 of the ICCPR with regard to the obligations of data controllers where public authorities are engaged in data collection and processing activities, stating:

“The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person’s private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should

¹⁶⁹ UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988. Available at: <http://www.refworld.org/docid/453883f922a>, p.1, para. 4

¹⁷⁰ UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988. Available at: <http://www.refworld.org/docid/453883f922a>, p.2, para. 7

also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.”¹⁷¹

Moreover, in its assessment as to the necessity of a measure, the Human Rights Committee, in its General Comment No. 27, on Article 12 of the International Covenant on Civil and Political Rights, reaffirmed that: “the restrictions must not impair the essence of the right [...]; the relation between right and restriction, between norm and exception, must not be reversed.” The Committee further explained that “it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them.” Furthermore, such measures must be proportionate: “the least intrusive instrument amongst those which might achieve the desired result”.¹⁷² The UN General Assembly Resolution on ‘The Right to Privacy in the Digital Age’ further articulates the scope whereby the limitation of the right to privacy is permitted, stating:

“To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other

¹⁷¹ UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988. Available at: <http://www.refworld.org/docid/453883f922a>, pp.2-3, para. 10

¹⁷² CCPR/C/21/Rev.1/Add.9, paras. 11 – 16

human rights, including the prohibition of discrimination.”¹⁷³

Furthermore, the UN General Assembly Resolution on ‘The Right to Privacy in the Digital Age’ also underscores the importance of the requirement to consider ICCPR Article 17 on the Right to Privacy in respect of the principle of non-discrimination (Article 26 of the International Covenant on Civil and Political Rights), which provides that “all persons are equal before the law and are entitled without any discrimination to the equal protection of the law” and, further, that “in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.” These provisions are to be read together with Article 17, which provides that: “no one shall be subjected to arbitrary interference with his privacy” and: “everyone has the right to the protection of the law against such interference or attacks”, as well as with Article 2, paragraph 1.”¹⁷⁴

3.2 The Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)

The idea of creating a European assembly arose first at the Congress of Europe, held by the International Committee of the Movements for European Unity in The Hague in May 1948. In the aftermath of the Second World War, pro-European movements had actively encouraged the establishing of an organisation that would work to defend fundamental freedoms, promote peace and the develop the spread of democratic principles in the region. The formation of the Council of Europe (COE) in 1949 was followed by the adoption of the European Convention on Human Rights (ECHR) in Rome in 1950, which entered into force in 1953.¹⁷⁵ Article 8 of the ECHR guarantees the right to respect for private and family life, home and correspondence. The

¹⁷³ UN, UN General Assembly Resolution, The Right to Privacy in the Digital Age - Report of the Office of the United Nations High Commissioner for Human Rights, A/RES/68/1670 of January 21, 2014, Available at: http://www.un.org/en/ga/search/view_doc.asp, p.8, para. 23

¹⁷⁴ UN, UN General Assembly Resolution, The Right to Privacy in the Digital Age - Report of the Office of the United Nations High Commissioner for Human Rights, A/RES/68/1670 of January 21, 2014, Available at: http://www.un.org/en/ga/search/view_doc.asp, p.12, para. 36

¹⁷⁵ Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No.005, 1950.

safeguards from interference in the right to privacy are qualified, with the conditions under which restrictions of this right are permitted being stipulated in Article, 8(2)). The right to respect for private and family life is articulated thus:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”¹⁷⁶

The Contracting Parties to the ECHR established the European Court of Human Rights (ECtHR) in Strasbourg with the purpose of providing greater oversight in ensuring the obligations required of the States by the Convention were respected. The ECtHR may hear complaints brought by individuals, groups of individuals or legal persons alleging violations of the Convention. An applicant to the Court need not be a citizen of a member state to the Convention. The Court has jurisdiction to decide complaints (“applications”) submitted by individuals and States concerning violations of the Convention, which principally concerns civil and political rights. It cannot take up a case on its own initiative. Complaints submitted to the Court must concern violations of the Convention allegedly committed by a State Party to the Convention and that directly and significantly affected the applicant.

While establishing civil and political rights and freedoms, the Convention in addition set up a mechanism for the enforcement of the obligations entered into by Contracting States. Three institutions were thus created to ensure the appropriate implementation and functioning of the treaty: the European Commission of Human Rights (established 1954), the European Court of Human Rights (1959) and the Committee of Ministers of the Council of Europe (the latter being composed of the Ministers of

¹⁷⁶ Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No.005, 1950, Article 8

Foreign Affairs of the member States or their representatives).¹⁷⁷ Over time the ECtHR has elaborated on the scope of the right to privacy in its judgments, the evolution of its jurisprudence in part reflecting the notion first articulated by the Court in the *Tyrrer* case that the document constituted a “living instrument” subject to evolutive interpretation.¹⁷⁸

From the 1980s onwards, the growth in cases brought before the institutions of the Convention was such that it became increasingly challenging to keep proceedings to within acceptable timeframes. In 1998 the Convention system was overhauled such that the original institutions established, the Commission of Human Rights and the European Court, were replaced by one full-time court. Protocol No. 11, which came into force on 1 November 1998, replaced the existing, part-time Court and Commission by a single, full-time Court.¹⁷⁹

Increasingly acknowledging the human rights dimension of its policies, the EU recognised the need to further recognise this element of its relationship to citizens. The EU thus proclaimed the Charter of Fundamental Rights of the European Union, dividing the range of civil, political, economic and social rights it affirms into six chapters, with Article 7 of the document articulating Respect for private and family life, stating: “Everyone has the right to respect for his or her private and family life, home and communications.”¹⁸⁰ While the Charter originally reflected a policymaking initiative, it would eventually become EU primary law in accordance with Article 6(1) of the TEU, with it coming into force with the Lisbon Treaty on December 1st 2009.¹⁸¹ Also relevant with respect to broader interpretative approaches to the right to

¹⁷⁷ COE, European Court of Human Rights - Historical Background, 2016, Available at: <http://www.coe.int/en/web/tirana/european-court-of-human-rights>

¹⁷⁸ *Tyrrer v United Kingdom* (1978) 2 EHRR 1, para. 31

¹⁷⁹ Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, restructuring the control machinery established thereby, ETS No.155, 1994. Entry into Force: 01/11/1998 - Ratification by Parties to Treaty ETS 005.) See also: European Court Of Human Rights, Historical Background, Available at: <http://www.echr.coe.int/ECHR/EN/Header/The+Court/The+Court/History+of+the+Court/> (last visited Jan. 20, 2007).

¹⁸⁰ European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02. Published in the Official Journal of the European Communities, 18 December 2000 (2000/C 364/01). The Charter became legally binding when the Treaty of Lisbon entered into force on 1 Dec. 2009, as the Treaty confers on the Charter the same legal value as the Treaties.

¹⁸¹ See the consolidated versions of European Communities (2012), Treaty on European Union, OJ 2012 C 326; and of European Communities (2012), TFEU, OJ 2012 C 326.

privacy are the Charter's provisions articulated in both Article 1 and Article 3, which concern 'Human dignity' and 'Right to the integrity of the person'. Article 1 states: "Human dignity is inviolable. It must be respected and protected." Whilst Article 3(1) "Everyone has the right to respect for his or her physical and mental integrity."¹⁸²

It should be noted that Article 52(1) of the Charter thus accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as any limitation on the exercise of the rights and freedoms recognised by the Charter "must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."¹⁸³

Article 52(1) further qualifies the interpretation of the Charter's safeguard of rights corresponding to those guaranteed by the ECHR, stating:

"In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."¹⁸⁴

4. Conclusions

The purpose of this chapter has been to provide a contextualization of the historical development of the regional framework at the European level in respect of the protection of personal data and the right to privacy. With regard to data protection law in particular, the review has illustrated how the legislative framework has been subject to revision and development on the part of lawmakers to ensure its regulatory competences keep abreast of innovations in information technologies. Knowledge of

¹⁸² *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, Articles 1 & 3(1)

¹⁸³ EUCFR, Article 52(1)

¹⁸⁴ EUCFR, Article 52(3)

the evolution of the bodies of law that provide a framework for the safeguard of the fundamental rights to privacy and data protection shall prove of particular value when we subsequently further examine normative developments in the light of both change in data processing activities, and with respect to perceptible shifts toward delineating the scope of privacy protection. One needs apprehend, therefore, how such challenges may add to the complexity of ensuring the continuance of the application of coherent and consistent legal principles. Technology, by its nature, gives rise to novel situations that require continuous adaptation of interpretive approaches to the law in place. In applying the respective provisions of the current legal instruments that constitute the framework to the deliberation of novel predicaments borne of advances in technologies, we need consider how, should lacunae appear in the protective scope of existing safeguards, these may have originated. The appraisal heretofore thus provides a foundation upon which to examine in greater depth the articulation of the respective normative concepts that contribute to the framing of the rights in question. The next chapter will discuss further and examine in greater detail the core doctrinal relationships that shape the principles that order the framework of regulation in respect of personal data protection and locational privacy.

Chapter 3: Mobility, Technological Innovation and the Evolving Paradigm of Privacy and Data Protection

1. Introduction

The objective of this chapter is to provide a broad structured critique of the fundamental changes in progress as a result of the implementation of new technologies that collect and process location data, and to furnish a preliminary review as to the initial difficulties and concerns that arise from the application of the existing legal framework. This enquiry sets the stage for the following chapters to explore in more depth the specific issues that arise from the use of location data in profiling activities and, thereafter, to explore the development of profiling beyond existing capabilities toward those anticipated by location data collection based on ambient monitoring (principally, Internet of Things (IoT) devices) and, subsequently, biometric sensing. As such, this section further provides a contextualization of the discussion that shall be developed in greater depth in subsequent chapters of this study in examining the core relationship between location data, locational privacy and data protection and the determination of the intrinsic value of location data in shaping these paradigms.

The analysis works from the premise that whilst the notion that individual's each exhibit a pattern of mobility that is inherently personal, to date the means by which to measure this phenomenon have not been limited. Thus, whilst innovation brings about more extensive capabilities to capture the dynamics of human mobility, we need appraise the broader transformative effect this may render in shaping norms. In the light of the ongoing evolution apparent in the utilisation of location data, one needs examine how innovation is continuing to shape perceptions of the spatial and temporal aspects of locality in respect of privacy and data protection concerns. The review considers the development of the principal theories that have shaped the reasoning behind locational privacy as formulated in the legislative provisions that have emerged. The discussion then describes how the evolving paradigm of locational

privacy has been influenced by advancements in technology to date, and how the discourse of research and scholarship have defined the analysis and reassessment of established conceptual approaches. The chapter then examines how developments in the discourse have influenced the development of the legal framework at the European level.

The technological advancements that characterize the ever-expanding utility and ubiquity of the different devices capable of collecting and processing location data are such that we need consider whether the provisions within the framework of existing legislation provide adequate safeguards to citizens' fundamental rights. In this appraisal one needs review how location data is framed conceptually; the relationship of location data to traffic data and other forms of metadata; and, furthermore, its compatibility with respect to the current specifications that determine special categories of data. That location data might potentially be categorized as sensitive data, and thus subject to a higher level of protection under data protection law, is part of the continuing discussion on the modernization of the legal framework for the protection of personal data in Europe.¹⁸⁵

Significant to this analysis is the role served by mobile devices that both generate location data and exploit location-based functionality. The complexity of the technical means by which location data is automatically collected is such that citizens may struggle to appreciate the extent to which their movements may be detected and tracked. An immediate concern thus arises where individuals and, more broadly, groups and communities, may not understand how the use of these evolving technologies may impact their fundamental rights. In particular, consideration needs to be given as to how existing legal precedents established in respect of simpler, less conceptually impenetrable technologies are applied to newer technologies that may encroach much deeper into the private lives of citizens.¹⁸⁶

¹⁸⁵ See: Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions - A Comprehensive Approach On Personal Data Protection In The European Union, 4 November 2010, COM(2010) 609 final, Available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

¹⁸⁶ A concern in this respect is also whether the basic assumptions upon which rules are interpreted in the light of evolving technologies can institute robust precedents; the principles they embody need remain constant and resist shifting unpredictably in the light of technological advancements. See: Kerr, Orin S., *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for*

2. Framing technology and its transformational role vis-à-vis the existing concepts of privacy and data protection

2.1 Concept of personal data

The concept of ‘personal data’ is central to existing EU data protection law and is fundamental to the application of obligations placed upon parties that are either data controllers or processors. Central to Directive 95/46/EC is the stipulation that ‘personal data’ is defined so as to articulate a concept that is broad and encompassing in scope. In particular, it must be noted that it covers all information that relates to both identified persons and those whom may later be rendered identifiable where account must be given to “all means likely reasonably to be used either by the controller or by any other person to identify the said person.”¹⁸⁷

That this provision articulates a relatively expansive, forward-looking approach in determining the bounds of personal data allows for the necessary flexibility and adaptability of existing legislation to nascent challenges to fundamental rights. Whilst the provision “all means likely reasonably to be used either by the controller or by any other person to identify the said person” provides the requisite adaptability needed to respond to evolving data collection and processing capabilities, nonetheless the open-textured nature of such a provision raises the question as to how the particular terms ‘likely’ and ‘reasonably’ are to be interpreted appropriately. This point is especially pertinent where we consider location data that may be subject to analysis using technologies that draw upon a variety of disparate sources of personal data. In this respect, the Article 29 Working Party has further stated in relation to the use of new technologies that allow for the monitoring of an individual’s movements: “data relates to an individual if it refers to the identity, characteristics or behaviour of an individual

Caution. Michigan Law Review, Forthcoming. Available at: <http://ssrn.com/abstract=421560>, pp.157-158

¹⁸⁷ See: Recital 26 of the Preamble to Directive 95/46/EC. It should be noted that the broad scope of the application of this principle has long been recognised; the 1987 Explanatory Memorandum to Recommendation Rec(87)15 indeed asserted that it was: “...worth repeating that whether or not an individual is to be regarded as “identifiable” is to be determined objectively, bearing in mind the sophistication of methods of identification at the disposal of the police, for example fingerprint techniques, voice recognition systems, data base surveillance, etc.” See: Committee of Ministers, Preamble - Recital 24 to the Explanatory Memorandum to Recommendation Rec (87)15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, 17 September 1987, Available at: <https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM>,

or such information is used to determine or influence the way in which that person is treated or evaluated.”¹⁸⁸

Data subjects require meaningful exercise of effective control over their own personal data. Furthermore, individuals require the opportunity to examine whether sufficient safeguards are being provided with respect to the protection of their personal data. Of importance in this regard is the necessity of providing the individual with information that is both clear and easily understood, ensuring that those without a technical understanding of the technologies that underpin mobile devices may be sufficiently well briefed so as to be empowered to make decisions on an informed basis. Such a requirement is increasingly necessary where the proliferation of mobile devices and increasing ubiquity of cellular communications, coupled with the technical complexity of telecommunications services, make it difficult for an individual to know whether personal data are being collected, by whom, and for what purpose.

Further, the protection of data subjects’ rights also requires that additional preconditions be met. Importantly, if individuals are to be accorded the requisite level of data protection, the limitation of the data controllers’ processing in relation to its purposes (based upon the principle of data minimization) must be duly recognised and respected. In conjunction with this requirement, a further prerequisite is that data subjects retain a meaningful and effective level of control over their own personal data.¹⁸⁹ In the commercial sector these principles relating to data quality need also be considered in conjunction with a data subject’s right of access to data: Directive 95/46/EC Article 12 requires that errors or discrepancies in personal data be corrected, obliging the data controller: “as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.”¹⁹⁰

¹⁸⁸ Working Party 29, Working document on data protection issues related to RFID technology, 10107/05/EN WP 105, November 2005, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf, p.8

¹⁸⁹ See: Article 6(c, d) of Directive 95/46/EC pertaining to data quality, whereby personal data must be: (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.”

¹⁹⁰ Directive 95/46/EC, Article 12(b)

However, a precursor for effective observance to the aforementioned provisions is the adherence of the data controller to fair information practice principles contained within the preceding clauses of Directive 95/46/EC whereby, *inter alia*, a data subject has the right to: “confirmation as to whether or not data relating to him are being processed; communication to him in an intelligible form of the data undergoing processing; and knowledge of the logic involved in any automatic processing of data concerning him.”¹⁹¹ Data subjects may struggle to exercise these rights where for the layperson finds it difficult to comprehend the complex technical environment of the communications services they utilize. Data may be retained without the individual having been informed or having given his consent. Location data represents a particular test for these principles in that providing a clear, lucid articulation as to how the data are collected and processed is a formidable challenge.

An immediately identifiable problem for both the data subject and the service provider, then, is how queries relating to an individual’s personal location data might be handled; how might an effective process function allowing a person to successfully request and retrieve personal data in accordance with the exercise of their rights to access, rectification and deletion of personal data be achieved? A distinct problem is therefore how to provide a meaningful implementation of these protective safeguards whilst taking into account the peculiarities of a data subject’s location data.

In the commercial sector, location data presents particular challenges where data subjects should be empowered to give free and informed consent where to data collection and data processing. Article 2(h) of the Data Protection Directive specifies that individual’s consent be such that: “‘the data subject’s consent’ shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.”¹⁹² This should equally apply in the context of location data. Currently, though, it must be acknowledged that these conditions are generally interpreted liberally; the requirements are construed in broadly different terms, such that in certain instances consent may be requested in written form, while in other respects consent is deemed

¹⁹¹ Directive 95/46/EC, Article 12(a)

¹⁹² Directive 95/46/EC, Article 2(h)

as having been implicitly given.¹⁹³ The divergence in practice thus provides a relatively weak foundation upon which to develop greater engagement of data subjects in allowing for their consent to the use of their location data.

Regarding consent, the data subject needs meaningfully grant acceptance of the terms under which their data is used.¹⁹⁴ Location data adds complexities to our framing of consent where it is difficult for individuals to understand the specific context of their data protection rights vis-à-vis location data — a prerequisite in terms of their being able to meaningfully convey their consent.

The processing of location data presents instances where it is not entirely clear how an individual may reasonably give specific and informed consent, based on the necessity of providing sufficient information as to how such data would be utilized. A user's inability to see a technology can make it difficult for them to comprehend how it might affect their privacy. However, the technology's unobtrusiveness remains a vital goal for developers; such systems in fact require that they minimize the impositions placed on users.¹⁹⁵ Further clarification is therefore essential to determine under what conditions consent may be considered valid, such that there exists an intelligible, coherent framework for articulating the necessary preconditions to guarantee a data subject's informed consent.

It should be noted that WP29's 2005 opinion on the use of location data asserts that the processing of location data is a particularly sensitive matter insofar as it involves "the key issue of the freedom to come and go anonymously." Interestingly, in this

¹⁹³ See: EU Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4 November 2010, Available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf p.8

¹⁹⁴ Note: In this context we need also consider the wider margin given by the EUCFR. Article 8(2) of the Charter Of Fundamental Rights Of The European Union provides significantly wider scope for the fair processing of personal data, where a lawful basis (other than the consent of the person concerned) may also be "some other legitimate basis laid down by law." Charter Of Fundamental Rights Of The European Union (2000/C 364/01), Article 8: Protection of personal data: 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis established by law.

¹⁹⁵ G. Myles, A. Friday, and N. Davies, "Preserving Privacy in Environments with Location-Based Applications," IEEE Pervasive Computing, vol. 1, no. 1, Jan.–Mar. 2003, pp. 56–64.

communication articulating the applicability of the relevant provisions pertaining to location data processing in Directive 95/46/EC and Directive 2002/58/EC it affirms its belief that the two pieces of legislation constitute a “satisfactory framework.”¹⁹⁶ Moreover, this statement of adequacy also takes into account the WP29 group’s acknowledgement of the broad exemptions and restrictions contained within Article 13 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC that allow for location data to be processed by way of exception to the principles laid down by the two Directives as a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and for the prevention, investigation, detection and prosecution of criminal offences.

2.2 Parallels: online and offline locations, and content

The potential of personal location data to impart further information relating to an individual is an important factor for consideration. In gauging the scope of its ramifications we may find useful analogies made in relation to Internet user activity on the web. In particular, one observation that is especially relevant pertains to the potential for navigation data to disclose further personal information relating to an individual (and indeed, in certain circumstances, with respect to other parties — such as an association between a person and those members of a group with which she is identified or linked). Working Party 29 highlighted this concern in its discussion of the scope of application of the term ‘traffic data’:

“The definition includes location data generated during the transmission of a communication. It also includes ‘navigation data’ (such as URLs/Unique Resource Locator) which might reveal an individual’s personal interests (e.g. web sites visited that give indications about an individual’s religious beliefs, political opinions, health or sex life). Because they show precisely which

¹⁹⁶ See: WP29, Working Party 29 Opinion on the use of location data with a view to providing value-added services, 2130/05/EN WP 115, November 2005, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf, p.3

pages on a web site have been visited they effectively reveal the actual content that the individual has accessed.”¹⁹⁷

Indeed, this point relating to navigation data's propensity to reveal content (raising the question as to whether classical distinctions made between ‘content’ and ‘metadata’ are legitimate) has been explored in more detail by scholars such as Solove and Klamberg, where they discuss its significance for the deliberation of the level of seriousness into fundamental rights that metadata collection and processing alone may constitute.¹⁹⁸

However, not mentioned by WP29 (or indeed discussed in the recent comparative analyses that critique the distinctions made between content and metadata) are the timing-related aspects of the aforementioned traffic and location data. This aspect is however very much relevant in the context of the present discussion; due deliberation must be given the observation that, as regards Internet navigation data, it will also provide further detail directly relating to the associated temporal attributes, such that inferences may in turn be drawn from the personal data allowing the analyst to resolve, for example, relative levels of interest in different topics (based on the time period spent reviewing the material identified by a particular URL). Similarly, a parallel capability exists in respect of location data, whereby the processing of spatio-temporal data can provide further information as to an individual's disposition toward visiting certain localities, associating with other individuals or groups. The integral temporal attributes found within the location data may yield valuable detail as to the significance of places and persons the individual interacts with, based upon their propensity to spend different proportions of their time at the various locales.

¹⁹⁷ WP29, Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385, 5042/00/EN/F INAL WP36, 2 November 2000, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf, p.3

¹⁹⁸ See: Solove, Daniel J (2003-2004). *Reconstructing Electronic Surveillance Law*. Geo. Wash. L. Rev., vol 72, pp. 1264- 1305, p. 1287; see also Kerr, 2009, p. 23; See also: Fura, Elisabet and Klamberg, Mark, *The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA* (October 23, 2012). Josep Casadevall, Egbert Myjer, Michael O’Boyle (editors), “Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights”, Wolf Legal Publishers, Oisterwijk, 2012, p.467

2.3 Directive 95/46/EC in respect of location data

According to Article 2(a) of the Directive: ‘personal data’ shall mean any information relating to an identifiable natural person (data subject).¹⁹⁹ Location data collected by telecommunication service providers would in most instances be covered by this definition: a link between the data and a specific person such that a person is identified or identifiable is in the majority of cases clear. Whether or not location data meet with this definition of personal data is in each instance critical (insofar as it acts as a trigger in terms of whether the protections afforded by the Directive apply), though achieving this objective with certainty may however prove difficult.

In this regard it should be noted that the Directive does not specifically define the term ‘identified.’ this deficiency proves germane where one considers different data that may or may not allow for identification of a particular natural person. Indeed, in some easily foreseeable scenarios it may be far less certain whether location data clearly constitutes personal data e.g. where a single mobile device is widely shared between different persons absent any detailed record that accounts for its use by a particular individual. However, location data may in these instances be reconciled with an individual where it is possible to ascertain from other personal data reliable inferences that point to a particular person’s identity. Indeed, here the data points that characterize the location data itself may be of value when matched with supplemental data. This use of location data indicates the underlying utility, and potential sensitivity, of location data.

According to Article 8(1) of Directive 95/46/EC special categories of personal data require a higher level of protection based on the sensitivity of the information regarding a natural person to whom the data pertains. Location data may potentially comprise information that allows for a nuanced depiction of a person’s movements and activities reflecting a wide range of personal characteristics. For example, location data which evidences a habitual sequence of attendance at a locality associated with religious congregation, corresponding in turn to a pattern of religious worship ascribed to a particular faith, would not immediately be regarded as data

¹⁹⁹ Article 2(a), Directive 95/46/EC

directly concerning ‘religious or philosophical beliefs’ as outlined within Article 8(1) of Directive 95/46/EC. Nonetheless, the aforementioned example evidences immediate problems with an oversimplified approach to understanding the particularities of the contextual nature of location data.

Article 6 of Directive 95/46/EC stipulates that personal data must only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with these purposes, except with the consent of the data subject (the finality principle). Personal data collection should be limited to that which is strictly necessary; it must be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed (the principle of proportionality in personal data protection). Location data presents various risks in terms of possible re-use and misuse for various purposes, either by a data controller, data processor or potentially by third parties. As highlighted earlier, location data can constitute a proxy in depicting sensitive aspects of private life, including one’s associations and relationships with others. Considering the complexity and potential sensitivity of the information that location data may potentially convey, its impact requires serious examination. In assessing this we need also to consider the prospective impact any additional, secondary processing might constitute. In this regard, Article 6 of Directive 95/46/EC clearly prohibits further processing where it is incompatible with the purpose for which the data was collected.

Considering the growing interest in the use of aggregated location data in diverse fields of research, further comprehensive review is required of the eventualities and impacts on fundamental rights that this development represents. Whilst Article 6(e) of Directive 95/46/EC specifies the measures incumbent on data controllers and processors to implement the necessary practical safeguards to ensure data quality, it is imperative that due consideration be given the impediments to de-identification that location data frequently encompasses.²⁰⁰

²⁰⁰ See: Xin Lu, Erik Wetter, Nita Bharti, Andrew J. Tatem & Linus Bengtsson, Approaching the Limit of Predictability in Human Mobility, *Scientific Reports* 3, Article number: 2923, Available at: <http://www.nature.com/srep/2013/131011/srep02923/full/srep02923.html>

2.4 Distinguishing between traffic and location data

The variability in terms of how the terms ‘traffic data’ and ‘location data’ are used interchangeably is problematic. The transposition of the terms from older texts into newer instruments presents impediments to articulating precisely the scope of certain provisions. That this should arise stems from the fact that, at least initially, location data was generally perceived as nothing more than purely technical data generated in the course of making or receiving a call from a cellular phone, and was therefore principally of interest only to electronic communication service providers. Perhaps too the confusion also originates in part from the ambiguity of guidance given on this issue by parties such as the WP29 group, which has on occasion conflated the two terms ‘traffic data’ and ‘location data’, thus creating further ambiguity.²⁰¹

More explicit, practicable definitions have been articulated by the data protection authorities based on the definition given in the e-Privacy Directive 2002/58/EC.²⁰² On this basis the UK’s Information Commissioner’s Office provides the following definition:

“Location data means any data processed in an electronic communications network or by an electronic communications service that indicates the geographical position of the terminal equipment of a user, including information relating to: the latitude, longitude or altitude of the terminal equipment; the direction of travel of the user; or the time the location information was recorded.”²⁰³

²⁰¹ In its 2005 opinion on the use of location data with a view to providing value-added services the WP29 group use “traffic data” and “location data” interchangeably, and add to the uncertainty surrounding the applicability of the terms where, in describing the particular relevance and context of location data it then asserts that the broader designation “traffic data” be applied to describe precisely the same data. Where, commenting on data that relates to a handset’s position at the time of a call it states: “The term “traffic data” is used in this connection. Such data merely result from the use of a given technology and are no different from other “traces” created every day. *See*: WP29, Working Party 29 Opinion on the use of location data with a view to providing value-added services, 2130/05/EN WP 115, November 2005, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf, p.2

²⁰² *See*: Recital 14 to the Preamble, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

²⁰³ ICO, The Guide, 2014, Available at: <http://ico.org.uk>

In contrast, the broader scope of the term ‘traffic data’ is aptly encapsulated in the following definition: “Traffic data means any data which is processed to convey a communication on an electronic communications network. It includes data relating to the routing, duration or time of a communication.”²⁰⁴

It should also be noted, however, that difficulties have arisen in respect of the terminology that applies as a result of the requirement that the relevant legal instruments be structured in a technology neutral way, adopting language that allows broad application of the respective provisions of the applicable Directives. As such, it should be taken into consideration that in doing so there arise inevitable challenges where, for example, instruments such as the e-Privacy Directive 2002/58/EC must articulate data protection principles across a broad spectrum of different technology platforms. This is certainly the case where Directive 2002/58/EC regulates processing of personal data and the protection of privacy in the electronic communications sector, which necessarily encompasses a broad range of different digital networks: in doing so, terms need be adopted that afford sufficient flexibility in their interpretation. In this context, the term ‘traffic data’ is an example worthy of further detailed scrutiny.

Article 2 of Directive 2002/58/EC states: “‘traffic data’ means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof”.²⁰⁵ As such, this provides a relatively broad elucidation of the term. Where we compare the scope of the personal data included in respect of the application of the provisions that relate to traffic data, we can see how differences arise as regards interpreting what the term covers.

The Working Party 29 statement in its 2000 opinion concerning the drafting of

²⁰⁴ ICO, *The Guide*, 2014, Available at: <http://ico.org.uk>

²⁰⁵ Article 2 of Directive 2002/58/EC

Directive 2002/58/EC and, in particular, its Article 2 definitions, that:

“‘Traffic data’ includes location data generated during the transmission of a communication. It also includes ‘navigation data’ (such as URLs/Unique Resource Locator) which might reveal an individual’s personal interests.”²⁰⁶

Of note, then, is the requirement that ample distinction be given the respective sub-categories of traffic data (to include location data and navigation data). It is quite evident that, depending on the particular context, confusion might arise should the terms ‘traffic’, ‘location’ and ‘navigation’ be considered comparable: they are not. Furthermore, the inclusive scope, in terms of the personal data processed within each sub-category of traffic data (location data, for example), will vary depending upon the type of electronic communications network being considered: this necessarily reflects the differences inherent in the respective digital networks subject to the provisions of the legal framework.

In this respect it should be noted that the wide definition given the term ‘traffic data’ in drafting Directive 2002/58/EC was indeed a source of early concern. In this regard, WP29 expressed its disquiet at an early juncture (though, however, to little apparent effect). The group highlighted its reservation that treating all items of traffic data in the same manner was unacceptable. Instead, WP29 affirmed that it would be far preferable for the proposed e-Privacy Directive to explicitly articulate to what extent particular types of traffic data (in the sense of a new wider definition) may be generated, collected and stored, and for what purposes they might be further used.²⁰⁷

In examining Directive 2002/58/EC we find that the concerns expressed as regards the necessity to distinguish between different types of traffic data produced what are

²⁰⁶ WP29, Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385, 5042/00/EN/F INAL WP36, 2 November 2000, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf, p.3

²⁰⁷ WP29, Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385, 5042/00/EN/F INAL WP36, 2 November 2000, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf, p.6

in effect quite unintelligible distinctions. Early comments on the draft of Directive 2002/58/EC focused on the need to distinguish within the instrument's provisions between the location data generated in electronic communications networks in relation to establishing a connection for the purposes of communication and other (as yet unspecified) location data. The primary concern of the experts of WP29 appears to have been their requirement that the user/subscriber must have full control over processing of location data in relation to 'value added services' (a widely used term in this context that preceded the more apposite term 'location-based services').²⁰⁸ Even here, however, in calling attention to the existing deficiencies in the draft legislation vis-à-vis the use of language employed, the group compounds the problem where it ineffectively articulates how legal provisions should direct the processing of location data. A clear example of this lack of congruence being their assertion that, where value-added services are concerned: "Given the sensitivity of location data with respect to freedom of movement and the fact that the location data covered here are not necessary to establish the communication, the user/subscriber must have full control over their processing."²⁰⁹

The aforementioned citation, then, is problematic where it refers only to location data emanating from the establishment of a communication; it does not provide any further elucidation as to how further location data relating to such a communication (such as that which pertains to the maintenance of a network connection for the duration of the communication i.e. not just the initial establishment of the connection) are to be treated. Indeed, a clearer and more accurate a conceptualization of this notion might better be articulated thus: "All location data generated in setting up a connection and during the transmission of a communication are to be treated as traffic data."

²⁰⁸ WP29, Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385, 5042/00/EN/F INAL WP36, 2 November 2000, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf, p.7

²⁰⁹ WP29, Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385, 5042/00/EN/F INAL WP36, 2 November 2000, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf, p.7

These apparent difficulties in selecting the appropriate terminology to adequately differentiate between the different location data appear to have influenced the eventual phrasing of the instrument in question, Directive 2002/58/EC. Article 9 of the e-Privacy Directive is particularly cumbersome where it resorts to the concept of “Location data other than traffic data.” The basis of “Location data other than traffic data” is premised on the distinctions drawn in Recital 35 to the preamble to Directive 2002/58/EC, which *inter alia* state:

“In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the *capacity to process location data which are more precise than is necessary for the transmission of communications* and which are used for the provision of value added services such as services providing individualized traffic information and guidance to drivers.”²¹⁰

However, the specific distinctions here that draw upon the different degrees of precision that at the time distinguished the use of location data by the network operator and the provider of value-added services is no longer valid. Thus the rationale that at first existed for conceiving of “location data other than traffic data” (which characterizes the provisions made within Article 9 of the Directive) no longer remains a relevant basis for making such a distinction. Essentially, then, in this respect the rationale behind Recital 35 in establishing the foundation for a division of location data into “Location data other than traffic data” (subject to Article 9) and “location data” as traffic data (covered by Article 6 of this Directive) has been rendered obsolete: in effect invalidated by technical developments. This particular observation therefore provides a fitting example as to the particular problems that arise where the drafting of an instrument relies to heavily on technical distinctions to effectively establish categorizations. This is especially the case where provisions struggle to differentiate between personal data that is closely interrelated. Such complications may instead justify adopting a more ‘technology neutral’ approach.

²¹⁰ Recital 35 to the Preamble of Directive 2002/58/EC

2.5 Location data and purpose limitation

An intrinsic limitation in applying fair information practice principles to location data concerns the way in which the data is itself generated. A difficulty arises from the reality that certain types of personal data are relatively easy to conceptualize and apprehend, whilst others are significantly more difficult for data subjects to grasp and understand. Content data, such as the text of an email message, likely falls into the first category; location data, in contrast, more plausibly fits the second category. It is important that we bear in mind this observation when we examine the efficacy of data protection law in respect of different types of personal data.

Understanding citizens' expectations and experience is extremely valuable in our assessing the quality and cogency of a specification aimed at safeguarding the rights to privacy and data protection and, furthermore, the actual effectiveness of these provisions. This proposition is in part founded on the reasonable premise that an apposite legal framework appropriately addresses the requirement that citizens be able to anticipate and predict the impact of their decision making — the principle of foreseeability. The notion is in turn partly contingent on the presumption that those affected are able to suitably inform themselves prior to expressing their chosen preference.

Thought therefore needs be given how these observations affect decision-making as regards data subjects and their location data. In short, it is not implausible to suggest that many data subjects are ill equipped to make informed decisions relating to their use of location data. That the means to collect location data *en masse* is a relatively new phenomenon, and still under-researched in terms of our developing an understanding of its impact on society, would suggest that forming an opinion as to whether citizens' perceptions' of the processing of location data match with the technical realities is premature.²¹¹ Scholars such as Cameron have asserted that it is the vulnerability and the diffuse nature of threats to democratic societies that has led to data being collected on anything that is, or can become, a danger.

²¹¹ See: Dara Hallinan, Michael Friedewald, and Paul McCarthy. "Citizens' Perceptions of Data Protection and Privacy in Europe" *Computer Law and Security Review* 28.3 (2012): 263-272. Available at: http://works.bepress.com/michael_friedewald/59

Cameron asserts there exists a natural tendency in all security and intelligence agencies to over-collect information. This propensity may damage the vital values of these societies unless external limits are imposed, and continually re-imposed to mitigate the risk.²¹² Purpose specification is an indispensable requirement in allowing for the appropriate processing of a data subject's personal data: absent this prerequisite the necessary conditions for application of other data quality provisions do not ordinarily arise. Purpose specification carries significance as a precondition for data processing as it acknowledges the fundamental value of transparency, legal certainty and predictability; these contribute toward the data subject's ability to make informed decisions regarding the use of their personal data. The principle establishes the necessity of placing limitations on data controllers such that the fairness of processing may be maintained such that controllers are prevented from utilizing individuals' personal data in a manner or purpose that runs counter to the expectations of the data subject. Balancing this limitation is the notion of compatible use, which provides data controllers with some latitude where data may be used with a degree of flexibility.²¹³

Purpose limitation provides that processing must be in conformance with the stipulations set down in the relevant provisions that articulate the scope of the compatibility assessment. In this regard the scope of application of the principle of purpose limitation may be restricted only where specific cases meet the requirements defined in Directive 95/46/EC's Article 13 or, where applicable, in Directive 2002/58/EC's Article 15. The exemptions and restrictions outlined in Article 13 of Directive 95/46/EC affirm:

²¹² Risk assessments should be subject to a meaningful 'second opinion' by way of relevant accountability mechanisms otherwise, Cameron, affirms, the necessary safeguards to the fundamental rights of privacy and data protection will be lacking, foreseeability substituted in their stead by 'ideological smokescreens'.

See: Iain Cameron, Venice Commission, Speaking Notes - European Parliament Hearing on Mass Surveillance, 7 November 2013, Available at: <http://www.europarl.europa.eu/document/activities/cont/201311/20131114ATT74429/20131114ATT74429EN.pdf>, p.2

²¹³ See further: WP29, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy/>, p.11

“Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Article 6 (1) ... when such a restriction constitutes a necessary measure to safeguard ... national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; an important economic or financial interest of the Member State or the European Union ... ; a monitoring, inspection or regulatory function ... and the protection of the data subject or of the rights and freedoms of others”²¹⁴

The exceptions cited in Article 13 that restrict the scope of the obligations and rights of data subjects are relatively narrow. Moreover, it should not be considered appropriate to legitimize incompatible processing of personal data simply by relying on one of the grounds listed in Article 7. Indeed, in this respect WP29 have provided specific guidance on this issue, on the basis that further clarification was required to elucidate the implicit limits that should be interpreted from the phrasing of the Directive so that of domestic legislatures would not fall foul of the provisions, noting:

“...The legislative measures adopted under Article 13 of the Directive must be interpreted restrictively as they are introduced by way of exception to the general principles of Article 6. Therefore, a legislative measure providing for a legal obligation under Article 7 would not necessarily be sufficient to make processing compatible.”²¹⁵

The measure must be aimed at safeguarding specific and important public interests as opposed to articulating a general requirement; this need is borne of the necessity that the exception meets a legitimate aim. Moreover, in this regard the opinion of Working Party 29 on the purpose limitation principle should also be taken into consideration where it emphasizes that domestic legislation providing for exceptions under Article 13 must include a provision that articulates the necessary test to verify that the measure concerned is in conformity with the criteria established by the ECtHR that determine the conditions which must be met for the derogation from a fundamental

²¹⁴ Article 13, Directive 95/46/EC

²¹⁵ WP29, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy/>, p.37

right.²¹⁶ As such, the required test should be founded on the requirements that the measure be clearly and precisely articulated so as for its effects to be suitably foreseeable, and that the measure itself is necessary in a democratic society and proportionate.

3. Personal data? The relationship between devices, location data collection and data subjects

Those providing counsel on the interpretation of the legal instruments relating to the processing of personal data are not impervious to self-contradiction. An example being the generalizations made in respect to qualifying the status of location data in relation to the use of mobile cellular devices: the guidance given by WP29 is confusing where, when qualifying how information can be considered to relate to an individual, it states that in certain situations the information conveyed by the data concerns objects in the first instance, and not individuals, noting:

“Those objects *usually belong to someone*, or may be subject to particular influence by or upon individuals or may maintain some sort of physical or geographical vicinity with individuals or with other objects. It is then only indirectly that it can be considered that the information relates to those individuals or those objects.”²¹⁷

The above distinction, drawn so as to distinguish how information relates either directly or indirectly toward an individual (an appropriate observation in respect of the general use of mobile devices, then) contradicts an earlier statement specifically regarding location data processed in an electronic communications network in particular context of mobile telephony, whereby it affirmed:

²¹⁶ Of further relevance in this context is the commentary of the Working Party 29, where it qualified the conditions such measures would need to specifically address, noting that they should: “describe the objectives of the relevant data processing, the categories of personal data to be processed, the specific purposes and means of processing, the categories of persons authorised to process the data, the procedure to be followed for the processing, and the safeguards against any arbitrary interference by public authorities.” See: WP29, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy/>, p.37

²¹⁷ WP29, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, 20 June 2007, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf, p.9

“Since location data always relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in Directive 95/46/EC of 24 October 1995.”²¹⁸

The conflict here is therefore quite apparent: the contradiction in the two statements reflects the fallacy that location data always corresponds to an identifiable natural person; it therefore entirely fails to appreciate the entirely reasonable eventuality that that location data might in certain instances identify only a device and its particular geographic coordinates (such that this information does not, either directly or indirectly, identify a natural person).

Furthermore, whilst identification through name remains the most common practice, a person’s name may not be necessary in all cases to identify an individual. Other identifiers may allow for identification and profiling may still occur even absent the name and address of an individual. A person may thus be categorized using criteria determined by either the preferences expressed or behaviours exhibited that express attributes that denote psychological or philosophical indicators pertaining to a person’s character. In this way, identification no longer necessarily requires the disclosure of identity in the limited sense i.e. the notion of identifying an individual does not necessarily mean that one needs ascertain their name.²¹⁹ In this respect it should be taken into consideration that the definition of personal data does not require that identification by name need be established, rather only that they be distinguished as an “identified” natural person (which may be attributed to pieces of information other than the name).

4. Location data: specifying its sensitivity as personal data

With limited exceptions the processing of sensitive data is prohibited under Directive 95/46/EC. Whilst the restriction extends to data revealing racial or ethnic origin,

²¹⁸ WP29, Working Party 29 Opinion on the use of location data with a view to providing value-added services, 2130/05/EN WP 115, November 2005, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf, p.3

²¹⁹ COE, Report on the application of data protection principles to the worldwide telecommunication networks, by Mr. Yves POULLET and his team, for the Council of Europe's T-PD Committee, point 2.3.1, T-PD (2004) 04 final, 13th December 2004, Available at: <https://rm.coe.int/168068416a>

political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life, in the light of changes in data collection and processing capabilities we might consider whether this provision be widened. Location data might potentially be framed such that it constitutes an additional special category. Evidence indeed suggests that citizens at times wish to restrict disclosure of their whereabouts; a recent study having revealed that twenty per cent of a cellular communication network's users admitted to regularly lying to others about their location while using their mobile devices.²²⁰ Whatever the basis for this deception, it nonetheless seems reasonable, therefore, to assert that a significant number of citizens value keeping their location private.

With respect to locations that reveal sensitive aspects of an individual's private life, it can reasonably be assumed that a person might be particularly inclined to exercise a right to restrict disclosure of this information. Classifying a broader selection of data types as constituting sensitive data to include location data would not constitute an entirely unprecedented venture. Indeed, in the light of both technological and societal developments discussion and the reconsideration of existing provisions with respect to special categories of data are already underway in Europe.²²¹

²²⁰ A.M. Townsend, "Life in the Real-Time City: Mobile Telephones and Urban Metabolism," *J. Urban Technology*, vol. 7, no. 2, 2000, pp. 85–104.

²²¹ For example, the provisions under Article 8 Directive 95/46/EC pertaining to special categories of data currently exclude a specific reference to genetic data, which has prompted concerns amongst experts. Interestingly, the review of WP29's consideration of the processing of genetic data provides a useful parallel in terms of providing a foundation for analyzing questions that arise from the science of location data analysis and, critically, its capacity to offer uniquely individualized insight into the private life of an individual. WP29 noted in its Working Document on Genetic Data that: "the technical progress which science has made over recent years in the field of genetic research has given rise to new data protection questions and concerns in relation to the significance and impact of genetic tests and the processing of genetic data." Thus, we might indeed further reflect as to the extent whether, for comparative purposes, identification based on location data is unique in nature and may therefore also require specific legal protective measures regulate its use. With regard to genetic data, and perhaps mirroring certain assertions that might credibly be made of location data, genetic data: "reveal the uniqueness of the data subject." *See*: WP29, Working Document on Genetic Data, 12178/03/EN WP91, 17 March 2004, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp91_en.pdf, p.4

4.1 Location data processing in other sectors: security and public safety

With much of the location data being generated by the use of mobile personal devices and other pursuits associated with everyday civilian activities, we need consider how the rationale behind the application of existing legal instruments at the EU level with respect to data processing in the police and judicial sectors may begin to shape and influence wider practices. The increasing ubiquity of devices capable of collecting location data relating to a determinable individual is a dynamic that may in time alter the broader paradigm of surveillance in society. An analysis of Recommendation No. R (87)15 and successive instruments, such as Framework Decision 2008/977/JHA, reveals the impact of the broad advancements in information technology on data use and the implications for the data subject's right to privacy and right to personal data protection. Indeed, the appreciable changes in practices are evidenced in the evolution of the language articulating the necessary distinctions that need be drawn between types of personal data collected and processed in this sector.

The progression is most noticeable in respect of the acknowledgement of the growing importance of the role of automation integral to the use of the increasingly sophisticated file storage and retrieval methods of advanced information systems. The challenges that the technical developments present are most clearly evidenced where we compare the terminology of respective legal instruments and how they formulate elementary concepts such as file types and automation. For example, for the purposes of control and notification, Recommendation No. R (87)15 distinguishes between 'permanent automated files' and 'ad hoc files'; how these two file types are exactly distinguished from one another being somewhat unclear from the text of the recommendation itself.²²² It is particularly important however in considering the evolutive process that has shaped the drafting of the various instruments that form the basis for regulating European data protection that the language employed is in each

²²² *Note:* The Explanatory Memorandum to Recommendation Rec (87)15 provides only limited and incomplete guidance on the distinctions; it outlines that data protection activities in the police sector requires a differentiation be made between "automated police files" and "manual police files", where the former relies upon computer-based automatic data-processing methods and the latter on traditional physical routines not contingent upon information technology resources. *See:* Paragraphs 24, 25 & 26, Committee of Ministers, Explanatory Memorandum to Recommendation Rec (87)15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, 17 September 1987, Available at: <https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM>

case partly a necessary reflection of the technical capabilities in existence at the time of drafting.

As an example, the notion of ‘automated processing methods’, which was initially articulated as a concept in Convention 108, now appears somewhat anachronistic nomenclature today when digital technologies are so pervasive: it is questionable whether as a society we any longer draw a distinction based on such a binary distinction as ‘automated’ or ‘non-automated’ processing when we contemplate the use of modern information technology. Rather, as regards intelligence capabilities in particular, emphasis has over time progressively been placed on the value of algorithms and problem-solving operations critical to modern information technology. This aspect of information technology was indeed appreciated at an early juncture, and was therefore integral to the distinctions drawn up in the founding instruments on data protection.²²³

In this context it should also be appreciated that certain earlier distinctions drawn between types of police files retaining personal data identifying an individual are in the present day rather dated, where such categorizations may no longer prove pertinent given technological advancements in information technology that permit wider use of data processing.

The example of the initial differentiation made in Recommendation No. R (87)15 between ‘permanent automated files’ and ‘ad hoc files’ is of relevance in this context. The Explanatory Memorandum to Recommendation No. R (87)15 subsequently clarified matters in choosing to elucidate a more general explication such that police files “cover all structured/organised personal data which are managed by the police services to meet their requirements in regard to the prevention or suppression of criminal offences or the maintenance of public order”.²²⁴ Furthermore, paragraphs

²²³ Convention 108 Article 2(c) defines the scope of ‘automatic processing’ thus: “[it] includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of *logical and/or arithmetical operations on those data*, their alteration, erasure, retrieval or dissemination.” Note: *emphasis added*. See: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981.

²²⁴ Committee of Ministers, Explanatory Memorandum to Recommendation Rec (87)15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, 17 September 1987, Available at: <https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM>, para. 36

26 and 27 of the Explanatory Memorandum to Recommendation No. R (87)15 also outline the necessary contextualization required here, noting, *inter alia*, that even police computerisation is highly advanced the data stored on computers may only be intelligible if reference is made to manual files. It noted at the time, however, that this situation would evolve such that increasingly data held in manual form will be automated; thence the principles contained in the instrument will in turn be extended to cover them.²²⁵ This therefore provides a more coherent, pragmatic articulation that obviates subjective distinctions based on degrees of permanence (which prove problematic where newer technologies can render justifying these distinctions on a practical level as either extraneous or convoluted).

Information relating to criminal activity of value to law enforcement varies in terms of the diverse range of sources from which data is sourced. Distinctions need be drawn so as to distinguish between the different types of information made use of in relation to preventing and investigating crimes. Traditionally, distinctions were made within the police sector such that a straightforward division could be drawn between sources of ‘hard data’ and ‘soft data’; in essence reflecting either the flow of data from either well-established sources or, conversely, based on vague indications about a person’s possible involvement in crime (the first category having conventionally been referred to as ‘hard data’, whilst the second constituted ‘soft data’).²²⁶

Today the availability of new technologies and the disparate range of data they provide mean that it is becoming more difficult to apply such a binary distinction as

²²⁵ See: Committee of Ministers, Explanatory Memorandum to Recommendation Rec (87)15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, 17 September 1987, Available at: <https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM>, paragraphs 26 & 27.

²²⁶ Project Group On Data Protection (CJ-PD), Second Evaluation Of The Relevance Of Recommendation No. R (87) 15 Regulating The Use Of Personal Data In The Police Sector, December 1998, Available At: [http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation\(87\)15_EN.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation(87)15_EN.pdf), p.6 *Note:* De Hert and Papakonstantinou note the difficulty of matching the police sector’s use of data based on uncertain facts or on assumptions and hearsay. The term coined by practitioners as ‘soft data’ refers very broadly to inferences and suppositions borne of subjective, partly conjectural analysis, as opposed to ‘hard data’ which covers defined, specific data including data subjects’ personal data) with the basic data protection principles, at least as determined by the provisions within the Framework Decision. See: Paul de Hert & Vagelis Papakonstantinou, The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for, *Computer Law & Security Review* 25 (2009) 403–414, p. 408

‘hard’ and ‘soft’ data. Moreover, objectively differentiating between different types of data is a far more complex task where disparate data sources may be combined to provide a synthesis report. Indeed, Framework Decision 2008/977/JHA provides a good example of how this difficulty has been acknowledged and subsequently formulated within the legal instrument concerned. Interestingly, in this context the preamble to the Framework Decision at the same time demonstrates the complications that arise where data protection principles established primarily to regulate the commercial sector are transposed into an instrument pertaining to the police and judicial sectors.

Paragraph 12 of the preamble to Framework Decision 2008/977/JHA illustrates this particular point distinctly; it qualifies the concept of accuracy pertaining to personal data in a specific sectorial (police and judicially-related) context: crucially, it qualifies exactitude and precision in terms of data quality as relative concepts based on the circumstances in question: “the principle of accuracy of data is to be applied taking account of the nature and purpose of the processing concerned.”²²⁷ The importance of this premise is all the more important where personal data is increasingly used in data mining and profiling activities in the police sector. The progressive widening of the scope of such activity has meant that profiling ventures to formulate depictions of suspect behaviours, abnormal or atypical patterns of contact with other parties and, perhaps especially problematic, unorthodox or wayward lifestyles. This sweeping approach may prove unfavourable where it is applied indiscriminately such that it is not linked to any enquiry into specific offences.

4.2 Law enforcement use of location data

The ever-improving precision of location tracking technology, coupled with the increasing integration of satellite-based geolocation in citizens’ mobile cellular devices, demonstrate that a review of the suitability of current data protection laws governing the processing of personal data in the police and judicial sector is timely.

²²⁷ Recital 12 to the Preamble of Framework Decision 2008/977/JHA. Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Whilst Directive 95/46/EC applies to all personal data processing activities in both the public and private sectors in the EU, its ambit is nonetheless limited as a legacy of the earlier pillar structure of the European Union, which necessarily influenced the drafting and scope of protection afforded by the data protection laws in the domain of law enforcement.²²⁸ Having implemented Data Protection Directive 95/46/EEC the Member States have not granted any significant additional powers to their respective independent supervisory authorities with regard to affording any supplemental oversight that might be given data protection in the police sector (although, of course, the Directive does not mandate police files be governed by its provisions). Interestingly, the Project Group On Data Protection highlighted this initial shortcoming in noting that in general terms an improvement in the supervision of law enforcement and the application of data protection rules with regard to the police should be contemplated.²²⁹

However, with the adoption of the Lisbon Treaty, and in view of the Commission Communications on the Stockholm Programme and the Stockholm Action Plan, which underscored the necessity of implementing a more comprehensive protection scheme that strengthens the protection of personal data across all EU policy areas (including those of law enforcement and crime prevention), the resolve to reform, modernize and widen the scope of the legal framework governing data protection in the EU has strengthened. In contrast, Framework Decision 2008/977/JHA has a relatively limited ambit in that it applies only to trans-border exchanges of personal data within the European Union (and thus excludes domestic data processing in Member States).²³⁰ The limited scope of Framework Decision 2008/977/JHA is at

²²⁸ Article 3(2), regarding the scope of the Directive, notes: “2. This Directive shall not apply to the processing of personal data: - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.” Directive 95/46/EC, Article 3(2).

²²⁹ As early as 1998 the Project Group On Data Protection (CJ-PD) underscored the need that adequate oversight be given data protection in the law enforcement sector, noting the indispensability of establishing a system of independent supervision over police files with effective powers to enforce data protection rules in case of non-compliance. *See*: Project Group On Data Protection (CJ-PD), Second Evaluation Of The Relevance Of Recommendation No. R (87) 15 Regulating The Use Of Personal Data In The Police Sector, December 1998, Available At: [http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation\(87\)15_EN.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation(87)15_EN.pdf), p.14

²³⁰ In negotiating the Framework Directive the EU Commission's Legal Service was requested an opinion as to the legality of its potential domestic application: whilst the Legal Service replied positively, this was not enough to reverse Member State objections, thus its scope was thereby limited

variance with other Council of Europe instruments pertaining to data protection and law enforcement activity; the distinction is absent from the following conventions and recommendations relevant to this area: Recommendation No. R (87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.:108) and the Additional Protocol regarding supervisory authorities and trans-border data flows (ETS No.:181). Furthermore, the 2012 review by the EU Commission of Framework Decision 2008/977 highlighted the difficulty in distinguishing in practice between cross-border processing of data under the Framework Decision and processing at the national level, and the related difficulty for law enforcement authorities in Member States to cope with different processing rules for the same personal data.²³¹

Whilst Framework Decision 2008/977/JHA constitutes progress toward common standards in the sphere of data protection in law enforcement and judicial cooperation into criminal matters, it nonetheless contains certain other weaknesses that should be taken in consideration where greater use of citizens' personal location data may be sought by law enforcement. For example, Article 3 of the Framework Decision 2008/977/JHA (concerning the principles of lawfulness, proportionality and purpose) and Article 5 (establishment of time limits for erasure and review)²³² provide data controllers and processors in the areas of the police and judicial sectors particularly wide latitude in interpreting the purpose limitation principle, as the provisions allow relatively wide scope to permit the further processing of personal data for a purpose other than that for which it was originally collected.

A further weakness of Framework Decision 2008/977/JHA, relevant in the context of location data processing within the police sector, is the absence of specific provisions

to cross border transfers. *See*: Paul de Hert & Vagelis Papakonstantinou, The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for, *Computer Law & Security Review* 25 (2009) 403–414, p. 410

²³¹ *See*: EU Commission, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, COM(2012) 12 final, 25.1.2012, Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, p.8

²³² Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

pertaining to two particular concerns; first, that the categorization of different personal data according to their accuracy and reliability be performed;²³³ and second, that a distinction should be drawn between categories of data subjects (suspects, witnesses, victims, convicted criminals, etc.).²³⁴ With regard to the first point, in discussing the challenges of developing a comprehensive approach on personal data protection the EU Commission indeed observed that a significant shortcoming of Framework Decision 2008/977/JHA is the absence of a provision that different categories of data should be distinguished in accordance with their degree of accuracy and reliability, where it noted that: “data based on facts should be distinguished from data based on opinions or personal assessments.”²³⁵ The second point, concerning categories of data subjects, is of particular relevance in respect of processing location

²³³ A requirement articulated in Principle 3.2 of Recommendation No R (87) 15, which states: “As far as possible, the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments.” *See*: Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector. *Note*: Article 8(1) of Framework Decision 2008/977/JHA circumvents addressing the verification of data quality directly by implementing such specific measures; rather it allows for competent authorities to adopt a more flexible approach, such that: “...competent authorities shall, as far as practicable, verify the quality of personal data before they are trans-mitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, up-to-dateness and reliability.”

²³⁴ The Project Group On Data Protection (CJ-PD) stated in its 1998 evaluation of Recommendation No. R (87) 15 that the use of data collected on unsuspected persons should be subject to greater review. The expert group added in the same December 1998 advisory briefing that particular consideration should be given the issue of providing notification to the persons about whom data the police have retained. *See*: Project Group On Data Protection (CJ-PD), Second Evaluation Of The Relevance Of Recommendation No. R (87) 15 Regulating The Use Of Personal Data In The Police Sector, December 1998, Available at:

[http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation\(87\)15_EN.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation(87)15_EN.pdf), p.2. In addition, it must be acknowledged that the 1987 Recommendation dealt with police data as perceived in the first half of that decade. As such, at that point in time intelligence files used in the police sector were not as advanced as those subsequently developed with the aid of evolving technologies. As recognized by the expert of the Netherlands on the CJ-PD panel, at that time data collection, processing and retention practices were in general significantly more limited: “the police held mainly data about the people they suspected of having committed a criminal offence. Things have changed since then. This raises the question of whether an additional international instrument dealing with certain specific questions in more detail would be useful.” *See*: Project Group On Data Protection (CJ-PD), Second Evaluation Of The Relevance Of Recommendation No. R (87) 15 Regulating The Use Of Personal Data In The Police Sector, December 1998, Available at:

[http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation\(87\)15_EN.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation(87)15_EN.pdf), p.3

²³⁵ *See*: EU Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4.11.2010, Available at:

http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, p.14

data where sufficient guarantees need be made in respect of the personal data of relating to those that are not suspected of participation in criminal activity.²³⁶

Recommendation No. R (87)15 should also be considered in this context in terms of the guidance it provides in relation to the introduction of new methods of data processing. In this respect the control and notification principle articulated under Principle 1 of Recommendation No. R (87)15 requires deliberation.²³⁷ In particular, Principle 1(2) of Recommendation No. R (87)15, pertaining to control and notification, states:

“New technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation.”²³⁸

As such, ongoing technical developments in cellular communication capabilities that have delivered increasingly more precise location data could, it may be argued, subject their use in processing personal data, where it is used in the police sector, to further scrutiny as required by this clause. Similarly, Principle 1(3) of Recommendation No. R (87)15 may also be applied in this context, where:

“The responsible body should consult the supervisory authority in advance in any case where the introduction of automatic processing methods raises questions about the application of this recommendation.”²³⁹

Indeed, the use of new technologies such as satellite-based surveillance in the police sector was highlighted at an early juncture in the deliberations of the review committee of Recommendation No. R (87)15 as requiring further examination. Moreover, the project group’s experts affirmed that the advent of new technologies

²³⁶ Principle 2.1 of Recommendation No R (87) 15, pertaining to data collection, affirms that: “The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence.”

²³⁷ Whilst all Member States have subscribed to the Council of Europe Recommendation No R (87) 15, which sets out the principles of Convention 108 for the police sector, this is not however a legally binding instrument.

²³⁸ Principle 1(2) of Recommendation No R (87) 15

²³⁹ Principle 1(3) of Recommendation No R (87) 15

“should be examined and, if appropriate, additional principles be defined,” so as to ensure that sufficient protection be given to the rights of data subjects.²⁴⁰ A further important consideration here regarding the use of location data concerns the weaker oversight of a data subject’s rights pertaining to data collection in Framework Decision 2008/977/JHA (when contrasted with the more robust provision intended to protect the fundamental right to data protection articulated in Recommendation No R (87)15): the earlier of the two instruments having affirmed:

“Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.”²⁴¹

4.3 Sensitive personal data in the police and judicial sectors

Article 6 of Framework Decision 2008/977/JHA provides that special categories of data receive specific safeguards as regards collection and processing in the police and judicial sectors. The scope of personal data considered sensitive is framed by way of the notion that it is data *revealing* or *concerning* characteristics, attributes or qualities pertaining to racial origin, political opinions, religious or other beliefs, health or sexual life. Importantly, this distinction therefore construes the applicability of the categorization of special types of data in a broad sense: the two terms ‘revealing’ and ‘concerning’ are decisive. Thus, in instances where location data may divulge information pertaining to sensitive areas of an individual's private life, consideration

²⁴⁰ Project Group On Data Protection (CJ-PD), First Evaluation Of The Relevance Of Recommendation No. R (87) 15 Regulating The Use Of Personal Data In The Police Sector, December 1994, Available At: [http://www.Coe.Int/T/Dgh/Standardsetting/Dataprotection/Em/1Evaluation\(87\)15En.pdf](http://www.Coe.Int/T/Dgh/Standardsetting/Dataprotection/Em/1Evaluation(87)15En.pdf), p.3, §16

²⁴¹ Principle 2(2) of Recommendation No R (87) 15. *Note:* In distinct contrast, the provisions set forth in Articles 3 and 4 of Framework Decision 2008/977/JHA, which relate respectively to the ‘Principles of lawfulness, proportionality and purpose’ and the ‘Rectification, erasure and blocking’ (of personal data) provide no such assurances for the data subject whose personal data is subject to processing in the framework of police and judicial cooperation in criminal matters. In addition, it should be noted too that in this context Recommendation No R (87) 15 also recommends: "The collection of data by technical surveillance or other automated means should be provided for in specific provisions" (Recommendation No R (87) 15, Principle 2.3). As such, the collecting of location data by either communications services providers or directly by law enforcement or other competent authorities utilizing cellular networks would fall within the scope of this requirement. No such corresponding requirement exists however within Framework Decision 2008/977/JHA.

is required as to what the data may reveal of features or characteristics implicit in our understanding of what these special categories inhere.²⁴²

In contrast, Directive 95/46/EC Article 8(5) provides broader scope for data processing of special categories of data, by both public and private sectors, through two additional inclusionary provisions (in conjunction with that of ‘criminal convictions’ first outlined within Convention 108, Article 6²⁴³ pertaining to the processing of personal data relating to ‘offences’ and ‘security measures’. Whilst it must be stated that this data processing is subject to the restrictions contained within the subsequent clause “carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards”,²⁴⁴ this arrangement however requires one to appraise the defensibility of such broad terms as “offences” and “security measures”.

Of further note is the fact that the provision makes no attempt to link the concept of an offence with the culpability or otherwise of the data subject; it is inexplicit as to the parameters that govern the remit for processing data relating to offences; thus it remains ambiguous as to how indirect a connection to an offence might exist which would nevertheless allow for personal data to be lawfully processed in accordance with this provision.²⁴⁵ In addition, the phrasing of the clause itself avoids connecting

²⁴² The phrasing of the scope of the provision pertaining to special categories of data follows that of the earlier data protection instruments drafted, such as Convention 108 and Directive 95/46/. For example, Article 8(1), Directive 95/46/EC states: “Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”

²⁴³ See: Council of Europe - ETS no. 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, Article 6 – Special categories of data: Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

²⁴⁴ Directive 95/46/EC Article 8(5) - Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

²⁴⁵ This particular point regarding the scope of Directive 95/46/EC Article 5 was commented upon by the Project Group On Data Protection in its second evaluative report of December 1998, which noted: “In paragraph 5 of article 8 about special categories of processing, appropriate safeguards are requested for all data relating to offences, whether they relate to convictions, to suspected persons, criminal intelligence or to any other personal data collected during the course of a criminal investigation.” See: Project Group On Data Protection (CJ-PD), Second Evaluation Of The Relevance Of Recommendation

the concept of an offence with criminal conduct i.e. the provision does not explicitly refer to ‘criminal offences’, only ‘criminal convictions’: the lacuna is therefore problematic insofar as the omission undoubtedly raises the question as to whether such a wide purview of the relevant exception was intended.

At this point we need also consider the authority granted by Directive 95/46/EC in respect of the processing of special categories of data in connection to security measures, which appears exceptionally broad where the term “security measures” is used to extend the permissibility of processing special categories of data where it relates to this criterion. Significantly, ‘security measures’ as a term is not defined within Directive 95/46/EC Article 2’s definitions, though the same term is confusingly used in other, apparently divergent, contexts in both Article 17 and Article 25 of the Directive in relation to *technical* security measures. Regrettably this omission renders the term somewhat indeterminate for the purposes of qualifying the scope of activities to which the standard applies.

5. Location data-based profiling and the risks to third parties

The use of location data in the prevention and investigation of crime by law enforcement raises specific concerns regarding third parties and their fundamental rights. In addition to the person (or persons) constituting the primary focus of investigation, monitoring activity may implicate others. It needs therefore be taken into consideration that in such instances third parties may be affected absent any evidence of their having committed an offence. In these cases, data relating to the respective parties should be differentiated as far as is possible so that the principle of purpose limitation might be respected. Further processing of personal data in this case should be limited to the extent that it is necessary for the purposes of a specified investigation into specified individuals, which would normally therefore exclude the practice of data mining and profiling the contacts identified in any primary analysis

No. R (87) 15 Regulating The Use Of Personal Data In The Police Sector, December 1998, Available at: [http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation\(87\)15_EN.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation(87)15_EN.pdf), p.5

conducted.²⁴⁶ Where traffic and location data processing may allow for individuals other than the primary suspect(s) to be identified, the same practices should apply.

Police use of location data potentially allows those conducting an investigation an extensive view of the other person's private lives in respect of their movements and interactions with associates. Any data processing-related decisions taken therefore that implicate these third parties and the use of their personal data need be justified; this consideration necessarily requires that a differentiation be made between the different sets of personal data relating to the individuals identified taking into account the purposes for which they are to be processed. Purpose limitation necessitates that processing of the data be conducted in a limited manner such that the purpose of such activity is targeted at providing information on the suspect (or suspects) under examination.

Furthermore, where processing of location data allows a party to identify and particularize behaviours of groups of persons in addition to the primary individual described as the 'data subject', the potential for discriminatory practices to occur must be considered. Analytical capabilities that allow for the mapping of associational relationships and interactions with third parties represent a genuine concern in terms of wider interferences in the fundamental rights of citizens within their respective communities. Conceivably, it is entirely reasonable to contemplate numerous criteria pertaining to either an individual's or group identity that could foreseeably be implicated by discriminatory practices stemming from the misuse of location data. Processing of location data could constitute a breach of the prohibition on discrimination where it constitutes an interference based on, for example, grounds such as: sex, race, colour, ethnic or social origin, religion or belief, political or any

²⁴⁶ Indeed, the Commission's 2010 communication concerning the development of a comprehensive approach to personal data protection noted this lacuna in respect of Framework Decision 2008/977/JHA. The Commission observed that this instrument contains too wide an exception to the purpose limitation principle. *See*: EU Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4.11.2010, Available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, pp.13-14

other opinion, membership of a national minority, property, disability or sexual orientation.²⁴⁷

The aforementioned grounds for which discrimination may occur could all conceivably be subject to identification where location data undergoes analysis as part of a data processing activity such as data mining or profiling. In this respect the Venice Commission has also called attention to a surveillance measure being unjustified if it is devised and/or used in a discriminatory way, for instance in order to register exclusively the criminal behaviour of some components of the population selected under specific criteria like their gender, their membership of a determinate ethnic group, ethnic minority, religious group etc. It affirmed that this data collection would only be admissible when performed for identification purposes.²⁴⁸ It should be recognized that the science of mobility tracking is in its infancy; consequently relatively little is yet known as to how these phenomena may raise further concerns as regards the discriminatory potential of the processing of location data.²⁴⁹

5.1 Third parties and location data: further considerations

Where data processing of location data risks linking third parties in respect of the primary data subject's associations, it may also be necessary to consider the means by which information can be considered to relate to another individual i.e. in what way does the necessary correlation exist that infers data identifying one individual also relate to another? In certain situations this is not always self-evident. In this regard the WP29 group has underscored how information that relates to one individual may relate to others in accordance with different 'elements' of its three-pronged approach,

²⁴⁷ For example, the provision within the EUCFR prohibiting discrimination states: "Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited." Charter Of Fundamental Rights Of The European Union (2000/C 364/01), Article 21

²⁴⁸ European Commission for Democracy for Law (Venice Commission), Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights study no 404, 9 March 2007, Available at:

[http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL\(2007\)014-e](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL(2007)014-e), p.13, §66

²⁴⁹ *See, for example:* Yves-Alexandre de Montjoye et al, Unique in the Crowd: The privacy bounds of human mobility, Nature.com - Scientific Reports 3, Article number: 1376, 25 March 2013, Available at: <http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html>.

such that the separate content, purpose, and results elements of specific data may each in turn reflect the fact that, in a single occurrence, information drawn from specified data pertains to numerous parties such that multiple data subjects are thereby distinguished.²⁵⁰ Therefore, the implication of such an eventuality is that the determination of the respective rights and interests of disparate parties may, in certain circumstances, prove a relatively elaborate process.

In this respect, then, it must be borne in mind that it is not a requirement that location data *per se* focuses on an individual for it to be considered that it relates only to her as personal data. Rather, it should be stated that the matter of whether data relate to a particular individual, or indeed to multiple individuals, should in each instance be resolved by reference to, and analysis of, the specific qualities of each data item. Correspondingly, this rationale demands that, where it is substantiated that a data item comprises information that pertains to different data subjects concurrently, it is necessary that due consideration should be given to the application of the relevant substantive provisions within the data protection framework to each of the parties concerned. Balkin has argued that surveillance need not process personal data considered particularly intimate or private — reflecting sensitivities that might fall within the scope of special categories of data under the relevant protective instruments, rather: “data mining technologies allow the state to record perfectly innocent behaviour that no one is particularly ashamed of and draw surprisingly powerful inferences about people’s behaviour, beliefs, and attitudes.”²⁵¹

In this context we must also consider the protection given under Article 8 of the ECHR the formation of relations with others; privacy encompasses more than the flow of information from the individual to others but also the relationships of which individuals partake:

“...it would be too restrictive to limit the notion to an “inner circle” in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle.

²⁵⁰ WP29, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, 20 June 2007, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf, p.11

²⁵¹ Balkin J.M., The Constitution in the National Surveillance State, 93 MINN. L. REV. 1, 2 (2008), p.12

Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.”²⁵²

Surveillance that targets information pertaining to a data subject’s relations with other parties, Regan suggests, is offered insufficient protection under the current legislative instruments.²⁵³ In this light, then, it could be asserted that in essence the principal problem with the basis of existing data protection safeguards is that, where they originate from the fair information practice principles, they lack sufficient concern for broader outcomes that affect third parties. Specifically, they place too great a focus on the data subject, and therefore lack sufficient emphasis on the role personal data can play in these scenarios affecting multiple parties.

6. Mass surveillance and bulk data retention of location data

Mass surveillance is not an entirely new phenomenon; indeed, the case law of the ECtHR attests to the inveteracy of extensive monitoring programmes in European States.²⁵⁴ Rather, advances in information technology have continued to supplement the ability of governments to collate increasingly larger amounts of information with much more efficiency.²⁵⁵ Cellular communications networks potentially allow law enforcement to collect and process large quantities of personal location and traffic data. The personal data collected in many instances could concern completely innocuous activities and be unrelated to any criminal activity but, nonetheless, still be retained by law enforcement. Recognition of the right to privacy of citizens infers that the State generally refrain from the indiscriminate monitoring of populations. Thus

²⁵² *Niemietz v Germany* (1992) 116 EHRR 97, §29

²⁵³ Regan, P.M., Response to Bennett: Also in defence of privacy. *Surveillance & Society* 8(4), 2011, Available at: <http://www.surveillance-and-society.org>, pp.497-498

²⁵⁴ See, *inter alia*: *Liberty And Others v. United Kingdom*, ECHR, Cited [2008] ECHR 568; *Rotaru v. Romania* [GC], no. 28341/95, § 54, ECHR 2000-V; *Weber and Saravia v. Germany* (dec.), no. 54934/00.

²⁵⁵ Of this phenomenon Citron has stated that the level of advancements recently witnessed in aggregation technology and advanced statistical analysis tools have enhanced the capacities of those who wield surveillance technology “to know us, often in ways that we do not know ourselves.” See: David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 67 (2013), Available at: http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2400&context=fac_pubs, p.85

the law must adequately define the basis upon which targets are identified for monitoring by a public authority authorised to conduct surveillance.

In this respect the Project Group On Data Protection reviewing Recommendation No. R (87) 15 highlighted its concerns regarding the seriousness of an interference mass surveillance by law enforcement may constitute; the review proposed strict limitations on generalized, unspecified searches of personal data retained by the police such that they should be allowed only in specific, limited circumstances. The expert group noted the disproportionate interference data surveillance checks or matching for the purposes of the suppression of crime may cause “vast amounts of persons possibly completely unrelated to any crime” and therefore any recourse to such powers by law enforcement must be limited to specific serious cases.²⁵⁶

The retention of personal data for police purposes is therefore problematic where it is extraneous to crime prevention and investigation and there exist no grounds for its continued storage. Storage of personal data in these instances is legitimate only for a time period commensurate with establishing whether or not the data is of relevance to the investigation: unless it is compatible in this sense it should not be retained or used for other purposes not explicitly permitted by law.

When location data are retained following processing in relation to unconnected investigatory procedures, the principles of purpose limitation and specification should be observed. Whilst it is not unreasonable that this data subsequently be utilized to investigate non-related criminal offences where the collected data manifestly evidences indications of criminal activity having been committed, a line evidently needs to be drawn as to where a limitation is placed on the practice. Establishing the boundaries of this restriction is not necessarily straightforward with regard to the police and judicial sectors. De Hert and Papakonstantinou unequivocally state that law enforcement’s use of personal data is fundamentally divergent from the commercial or other public sectors, noting ‘the police work differently’: “They keep track of criminals for most of their lives, correlate data from different sources, work

²⁵⁶ Project Group On Data Protection (CJ-PD), Second Evaluation Of The Relevance Of Recommendation No. R (87) 15 Regulating The Use Of Personal Data In The Police Sector, December 1998, Available At: [http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation\(87\)15EN.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/2Evaluation(87)15EN.pdf), p.14

on suspicion and hearsay, and store current data for no obvious reason other than it may prove extremely useful in the future.” The question thus arises as to whether these purported differences are so fundamentally divergent that they preclude greater harmonization between private, public and police sectors of data protection law.²⁵⁷

Difficulties increasingly arise in distinguishing appropriate limits where analysis of historical data sets may yield actionable information long after the personal data was first collected and processed. In addition, if there is to be a cause for the further processing of personal data, then law enforcement needs elucidate a sufficiently detailed justification based on legitimate indications that they believe such a basis exists: this could provide the rationale for a circular argument justifying increasing data retention.²⁵⁸ However, where these conditions can be fulfilled secondary processing can be regarded as fair and compatible with the original purpose. Purely speculative data processing (absent a relevant, defined objective), on the other hand, by definition lacks a reasoned justification. Thus, absent a specific legal provision authorizing such processing under domestic law, it would not be compatible with the premise that for police and judicial purposes the processing of personal data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected.²⁵⁹ Furthermore, in the context of secondary processing, special consideration should be given the rights of third parties (where personal data pertaining to persons other than the suspect have been collected in the course of an investigation): its use for investigations of possible further offences would not

²⁵⁷ See: Paul de Hert & Vagelis Papakonstantinou, The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for, *Computer Law & Security Review* 25 (2009) 403–414, p. 411

²⁵⁸ In *Campbell v. United Kingdom* the ECtHR again reiterated that, in the context of the interference into private life, the notion of necessity implies that any interference in respect of Article 8’s protections correspond to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued. In *Campbell* the notion of ‘reasonable cause’ was elucidated where it pertains to the scope and quality of information required: “What may be regarded as ‘reasonable cause’ will depend on all the circumstances but it presupposes the existence of facts or information which would satisfy an objective observer that the privileged channel of communication was being abused” (see, *mutatis mutandis*, the *Fox, Campbell and Hartley v. the United Kingdom* judgment of 30 August 1990, Series A no. 182, p. 16, para. 32). See: *Campbell v. the United Kingdom* [1992]. ECHR 13590/88, §48

²⁵⁹ Article 3, Framework Decision 2008/977/JHA. Note: Article 3, paragraph 2 of Framework Decision 2008/977/JHA elucidates the requirements that need be met should processing be permissible, where it shall be permitted in so far as:

- (a) it is not incompatible with the purposes for which the data were collected;
- (b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose.

normally be interpreted as being proportionate and in accordance with the principle of purpose limitation.

6.1 Notification and data subjects' access to information

A further issue requiring consideration is that of data subjects' rights in respect of notification. This is a particularly challenging problem where processing occurs in the police or judicial sector, and may be considering even more problematic where location data is concerned. Notification issues need also be reviewed where, in the context of criminal investigations and subsequent proceedings, the processing of data may also implicate third parties where personal data reveals information relating to other data subjects (for example, in the case of location and traffic data providing detailing the locality and timing of a meeting between two parties).

Article 16 of Framework Decision 2008/977/JHA provides that Member States be required to ensure their competent authorities inform data subjects that their data are being processed or transmitted to another Member State for the purpose of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties. As the instrument does not pertain to domestic processing, a data subject's right to notification is relatively limited. Moreover, the notification requirement of Article 16 of the Framework Decision does not specify in detail what kind of information needs to be given to the data subject: it leaves this decision to the Member States and to resolve how data subjects exercise their right of access — either directly to the relevant party, or respectively indirectly via a third party. Moreover, it has been noted that the Framework Decision lacks detail as to both the appropriate methods for informing the data subject²⁶⁰ or when possible exemptions for this provision are justified: where the right to information is generally granted this implementation has, according to Member States, varied considerably.²⁶¹

²⁶⁰ See: Framework Decision 2008/977/JHA, Recital 27, whereby: “The modalities of the right of the data subject to be informed and the exceptions thereto should be determined by national law. This may take a general form, for example, through the law or through the publication of a list of the processing operations.”

²⁶¹ EU Commission, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE

The weaknesses in the notification requirements that exist in Framework Decision 2008/977/JHA relative to those within Directive 95/46/EC²⁶² are not wholly surprising considering that surveillance monitoring is such that the entire efficacy of the measures deployed may be jeopardized were parties to be notified. The ECtHR indeed recognised in the case *Klass and others v Federal Republic of Germany*²⁶³ the practical limitations of requiring authorities to notify those subject to surveillance measures, where the Court questioned the feasibility of requiring subsequent notification “in all cases”, stating:

“The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance... such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents.”²⁶⁴

Thus the ECtHR held that the Article 8 interference into a citizen’s private life, either from the implementation of surveillance measures or merely from the existence of the requisite legislation that authorizes its deployment, is in principle justified under Article 8, paragraph 2, where: “the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the ‘interference’.”²⁶⁵ Nonetheless, Framework Decision 2008/977/JHA to an extent however acknowledges that data

COMMITTEE OF THE REGIONS, COM(2012) 12 final, 25.1.2012, Available at:

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, p.5

²⁶² Directive 95/46/EC's Article 12 provides for, *inter alia*, access rights guaranteeing the data subject certain safeguards in respect of their being able to obtain from data controllers; confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions.

²⁶³ *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978

²⁶⁴ *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §57

²⁶⁵ *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §58

subjects' rights risk serious interference in this regard; Recital 26 of the Preamble to the Framework Decision stipulates that:

“It may be necessary to inform data subjects regarding the processing of their data, in particular where there has been particularly serious encroachment on their rights as a result of secret data collection measures, in order to ensure that data subjects can have effective legal protection.”²⁶⁶

In addition, it should be noted that, with respect to the ECtHR's deliberations in *Klass*, a close review of the judgment reveals the Court having given due deliberation to provisions within the domestic legislation in question: “designed to reduce the effect of surveillance measures to an unavoidable minimum and to ensure that the surveillance is carried out in strict accordance with the law.”²⁶⁷ Furthermore, the Court acknowledged that, regardless of the quality of any enacted legislation governing surveillance measures, “the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system”; the particular caveat to this observation being that the Court need consider “the likelihood of such action and the safeguards provided to protect against it.”²⁶⁸

Consequently, it should be recognised that the precedent *Klass* establishes is necessarily limited in its scope of application; due consideration must be given to the distinct circumstances prevailing in the context of other surveillance regimes. Indeed, the Court noted that in its judgment it had arrived at its decision on the premise that: “In the absence of any evidence or indication that the actual practice followed is otherwise, the Court must assume that in the democratic society of the Federal Republic of Germany, the relevant authorities are properly applying the legislation in issue.”²⁶⁹ This proclamation therefore requires we reappraise its congruence with contemporary practice, such that we consider whether present-day monitoring is of a similar nature in its implementation.

²⁶⁶ Framework Decision 2008/977/JHA, Recital 26

²⁶⁷ *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §59

²⁶⁸ *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §59

²⁶⁹ *See: Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §59

It should be noted that in *Klass* the applicants also alleged a breach of Article 13 of the ECHR. The judgment in *Klass* is of particular interest where it considers the provision that an individual whose Convention rights “are violated” is to have an effective remedy before a national authority.²⁷⁰ In dispute was whether the entitlement to a remedy existed: “only if a “violation” has occurred.” It was noted though that this provision might prove unworkable should a person not first be able to establish a violation absent the means to assert a claim before a national authority to that effect. Taking this into consideration, the Court adopted a pragmatic approach to interpreting the remit of Article 13’s actual scope. Thus, in the Court’s view, the correct interpretation of Article 13:

“...requires that where an individual considers himself to have been prejudiced by a measure allegedly in breach of the Convention, he should have a remedy before a national authority in order both to have his claim decided and, if appropriate, to obtain redress.”²⁷¹

This interpretation of Article 13 gave the Court sufficient scope to then consider whether indeed there existed an unrestricted right to notification of surveillance measures. In this respect it affirmed that no unrestricted right to notification of surveillance measures can be deduced from Article 13 once the contested legislation, including the lack of information, has been held to be “necessary in a democratic society” for any one of the purposes mentioned in Article 8 (art. 8).²⁷²

The Court then elaborated on its rationale by referring back to its earlier deliberations in the case and ultimately rejecting the applicants’ complaint, noting that: “it is the secrecy of the measures which renders it difficult, if not impossible, for the person concerned to seek any remedy of his own accord, particularly while surveillance is in

²⁷⁰ Article 13, ECHR: Right to an effective remedy – “Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.”

²⁷¹ *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §64

²⁷² *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §68

progress.”²⁷³ Nonetheless, of particular remark is the observation that, in the Court’s judgment, it need articulate its underlying aversion toward monitoring, while it accepted its inevitability:

“Secret surveillance and its implications are facts that the Court, *albeit to its regret*, has held to be necessary, in modern-day conditions in a democratic society, in the interests of national security and for the prevention of disorder or crime.”²⁷⁴

That the Court should lament the need for surveillance in a democratic society in expressing its “regret” constitutes an acknowledgement that the malign influence and impact of surveillance on citizens’ fundamental rights is however unavoidable, damaging nonetheless. Furthermore, the principle of proportionality applies. Thus, where covert surveillance measures are implemented, consideration must be given to whether persons subject to monitoring could in essence still be informed, albeit at a later juncture. The Court noted in *Klass*, we may recall, that: “It is the secrecy of the measures which renders it difficult, if not impossible, for the person concerned to seek any remedy of his own accord, particularly while surveillance is in progress.”²⁷⁵ The Court’s guidance is such that it does not preclude notification outright; it merely vindicates the position held by the government in the case concerned that to do so in the course of an investigation employing covert surveillance would be counterproductive and defeat the very aim of the monitoring activity. There remains scope, therefore, for further deliberation as to how notification measures might be strengthened.

Where it is regarded as essential for certain categories of data controllers, such as communication service providers, to withhold information pertaining to their disclosing personal data of a data subject to law enforcement or the judicial authorities, this should be explicitly provided for by law. An overly encompassing

²⁷³ *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §68

²⁷⁴ *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §68. Note: *emphasis added*.

²⁷⁵ *Klass and others v Federal Republic of Germany*, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978, §68. Note: *emphasis added*.

provision that would enforce data controllers and processors to restrain themselves from disclosing information and allowing data subjects to ascertain whether they have been subject to surveillance measures by way of the authorities obtaining their communications data for processing would ordinarily be regarded as a disproportionate measure. If after monitoring data subjects are in principle to be informed as to the collection and processing of their personal data for the purposes of a targeted criminal investigation, then it needs be considered on which party the onus should reasonably be placed where the process needs first to be initiated. Under these circumstances there exists two possibilities: either the authorities may be placed in a position of responsibility by the legislation to inform the data subject in the first instance or, conversely, the requirement might otherwise be assigned to the data subject herself to initiate the notification request.

The latter option raises two immediate difficulties as regards its effective implementation. First, that the data subject is sufficiently informed of her rights as to the disclosure of the information she may request and, additionally, as to the appropriate method she need employ to initiate a notification procedure. Secondly, it presumes that the data subject is sufficiently well informed that she may instigate a request for notification with the appropriate party.²⁷⁶ The assumption that a data subject is cognizant of the various different entities in the law enforcement and judicial sectors that may have processed his personal data is problematic; providing for a right to notification requires that the process is made sufficiently accessible and uncomplicated for the citizen.

6.2 Collection of location data: applying the data minimization principle

Recognition of the importance of applying data minimization principles in respect of data collection within the police and judicial sectors is evident from the very first

²⁷⁶ *Note:* this point was also recognized in the Explanatory Memorandum to Recommendation Rec (87) 15, where it was noted that with reference to “police authorities” it should be borne in mind that: “depending on the legal system in question, different police forces can coexist. It may not always be easy to distinguish between them from the point of view of division of labour.” *See:* Committee of Ministers, Explanatory memorandum to Recommendation Rec (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, 17 September 1987, Available at: <https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM>, Preamble, Recital 23

conceptual provisions articulated within the relevant legal instruments drafted. Recommendation Rec (87)15 Principle 2, for example, requires *inter alia* that “collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence” (and that exceptions to this provision should be the subject of specific national legislation). In addition, collection of data by technical surveillance or other automated means should be provided for in specific provisions.²⁷⁷ These provisions intend thus to safeguard citizens from the indiscriminate collection of personal data by law enforcement.

Of further note in this regard, and of relevance where traffic and location data processing may furnish more sensitive information on an identified person, is the provision made within Recommendation Rec (87)15 Principle 2.4 in respect of special categories of data:

“The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organizations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.”²⁷⁸

Principle 2.4 regards the issue of special categories of data, and reflects the concern articulated in Article 6 of Convention 108 that the collection and storage of particular categories of data should be restricted. The phrasing of the provision is of particular interest as the terminology employed could possibly give rise to different interpretations. The principle, in fact, states that collecting data *solely on the basis* of the individual’s racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organizations not proscribed by law should be prohibited. This does not therefore preclude in practice the collection of all such data where another additional basis for the activity is given that may be justified (even absent the conditions articulated in the qualifying clause

²⁷⁷ Recommendation Rec (87)15, Principle 2(1),(3)

²⁷⁸ Recommendation Rec (87)15 Principle 2(4)

relating to a necessity borne of a particular line of enquiry). On this point it should also be noted too that the difficulty inherent to qualifying where personal data pertains to sensitive or ‘special categories’ of data is a complex issue: the provision refers to “collection of data concerning these factors”. It need be recognised, then, that notionally the term “concerning these factors” is indeed rather broad a classification, though it does of course allow for a degree of leeway should a more expansive interpretation be deemed appropriate to providing suitably encompassing safeguards to the protecting of an individual personal data.

In this respect the guidance given by the explanatory memorandum on the recommendation is particularly telling. The memorandum, which reaffirms that the collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence, states that Principle 2.4 should be interpreted such that:

“...In no circumstances should such data be collected *simply* in order to allow the police to compile a file on certain minority groups whose behaviour or conduct is within the law.”²⁷⁹

It is important, then, that we not overlook two peculiar details of this elucidation. Firstly, that the explanatory memorandum places a distinct emphasis on the term “simply” (which, atypically, it chose to italicize so as to accentuate its prominence) and, secondly, that it speaks only of a very limited potential of the misuse of such data in citing the possibility that files could in theory be compiled on minority groups. As such, the memorandum circumvents more detailed discussion of, for example, how the inappropriate processing of sensitive personal data could affect identified individuals (rather than consider more generally only the minority groups of which they might be a member).

The Article 29 Working Party has further stated in relation to the use of new technologies that allow for the monitoring of an individual’s movements: “data relates

²⁷⁹ Committee of Ministers, Explanatory Memorandum to Recommendation Rec (87)15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, 17 September 1987, Available at: <https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM>, para. 48.

to an individual if it refers to the identity, characteristics or behaviour of an individual or such information is used to determine or influence the way in which that person is treated or evaluated.”²⁸⁰ Furthermore, whilst minority groups may be considered particularly at risk, it should not be disregarded that, where special categories of data are concerned, all groups (including those that represent a majority in a population) are to be afforded equal protection.

Article 6 of Framework Decision 2008/977/JHA, in contrast, concerns the limitations placed on processing of special categories of data.²⁸¹ Thus, an important point to consider in this respect is how the Framework Decision differs from its antecedent, Recommendation Rec (87)15, as it specifically refers to processing (rather than the collection) of special categories of data. This distinction is of consequence where we consider how personal data collected outwith the law enforcement sector may subsequently be subject to secondary processing in a manner otherwise unforeseen by the party initially responsible for its collection.

7. Conclusions

Given the advances made in data processing capabilities, the term ‘personal data’ as framed in the applicable legal instruments requires a flexible interpretation. The analysis of complex data sets may furnish information relating to an individual far beyond the scope of the knowledge initially envisaged by the actions of the data controller by which the assessment of purpose was first considered. The adaptability of the provisions are a logical consequence of the recognition given to the wide scope that the notion of automatic processing of personal data embraces, such that the Directive as an instrument is required to be suitably encompassing in its purview.²⁸² Further appraisal should be applied to the scope of safeguards provided in respect of

²⁸⁰ Working Party 29, Working document on data protection issues related to RFID technology, 10107/05/EN WP 105, November 2005, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf, p.8

²⁸¹ Framework Decision 2008/977/JHA, Article 6 - Processing of special categories of data: The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade- union membership and the processing of data concerning health or sex life shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards.

²⁸² WP29, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, 20 June 2007, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf, p.8

provisionally ‘subjective’ elements of information that relate to an identified person. This is especially the case where location data may be processed in mapping and analysing mobility patterns. In this context it should be noted that the capabilities of technology to allow for increasingly sophisticated data manipulation were recognised, and thus have been articulated in provisions such as Recital 14 to the preamble of Directive 95/46/EC, which states:

“...given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data.”²⁸³

Whilst the provision refers to sound and image data in particular, the recital has been interpreted by WP29 such that the provision can be seen to encompass other forms of personal data so as to broadly include information pertaining to mood, inter-personal relationships and other aspects of human behaviour. In this respect it must also be taken into account that the processing of personal data also carries the capacity to generate information that is specific and uniquely different from other related personal data on an individual.²⁸⁴ As such, data controllers and processors need recognize the implications of this detail with regard to their wider data protection responsibilities. The next chapter looks in greater detail at the evolution of profiling capabilities in this regard. The review adopts a comparative approach and examines the recent development of social network analysis and its use in profiling, questioning how similar techniques applied in data analysis and modelling of behaviours based on the processing of data subjects’ location data might be applied. The review resolves to establish cognate issues in the two activities and discern where advances in relation to more widespread data processing of location data may stretch established methods of safeguarding of citizens’ privacy and right to personal data protection.

²⁸³ Recital 14 to the Preamble of Directive 95/46/EC

²⁸⁴ WP29, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, 20 June 2007, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf, p.8

Chapter 4: A Critique of Developments in Data Analytics: Applying Novel Profiling Techniques to Location Data

1. Introduction

This chapter places current developments in profiling capabilities based on personal data collection and processing into context as regards how these advancements may in turn influence future uses of location data. The analysis conducted in this section of the review takes a comparative approach, and appraises the recent evolution of social network analysis. This assessment aims to determine whether parallels may be drawn, and whether analogies with emergent processes that attempt to extrapolate information and develop profiles on individuals by processing location data prove tenable. The review places a specific emphasis on determining the suitability of utilizing location data in predictive analytics, and discusses how efforts to date, based on social network analysis as a basis, have exposed serious concerns where data processing risks considerable harm to citizens subject to these techniques. The potential to monitor patterns of mobility raises important questions in respect of how we contextualize more complex forms of profiling connected to the processing of personal data within the broader framework of safeguards to privacy and data protection.²⁸⁵

2. Current profiling capabilities

Interestingly, Lessig's scholarship relating code to the construal of normative frameworks has highlighted the importance of understanding the relationship mobility plays in shifting power between the different parties bound within hierarchical systems. Crucially, the ability to distinguish and classify, order between different

²⁸⁵ Wood and Graham have described surveillance in geographical terms as a "technocratic form of territoriality, the limiting of mobility through the construction of boundaries", further noting that it determines the value of particular spaces, and relationships to those spaces, through processes such as categorization and the maintenance of boundaries (notably for Wood and Graham, both spatially and in terms of identity), examination and enforcement.²⁸⁵

individuals has been eroded by the increasing fluidity and mobility of society. Therefore, Lessig forewarns that more invasive monitoring of mobility for the purpose of profiling would constitute retrogression.²⁸⁶

Concerns arising from monitoring, data collection and processing to profile and sort citizens, differentiation based upon the analysis of movement, inferences of association and interaction between different entities based upon the examination of location data, all require close scrutiny. Without sufficient oversight, poor decision making may lead to insufficiently qualified distinctions being made, thereby risking interferences in citizens' fundamental rights.²⁸⁷ Scholars such as Goffman have argued that the mere possibility of an interference in an citizen's privacy or data protection rights constitutes a tangible chilling effect on the individual, which in turn hampers the person in the unfettered creation of their identity, the possibility to experiment with different kind of roles and ultimately, the development of one's personality.²⁸⁸ Moreover, Blumenstock et al have indeed expressed concerns vis-à-vis the misappropriation of predictive capabilities to predict the unknown location of an individual when she is "off the grid" – envisaging a scenario in which a nefarious actor might use such techniques for ill.²⁸⁹ We need therefore understand whether location data mining techniques that rely on pattern recognition are apt to deliver reliable results and furnish evidence that meets the appropriate scientific standards.²⁹⁰ Furthermore, we need discern the role of subjective opinion in developing the means of analysis such techniques rely upon.²⁹¹ The capability to initiate behavioural profiles

²⁸⁶ Lessig, Lawrence. 1999. *Code and other laws of cyberspace*. New York: Basic Books, p. 155

²⁸⁷ Solove too has underscored the challenges posed by the tendency toward using empirical data analysis to supposedly eliminate non-commensurability and ambiguity, reducing intricate facets of life to simple categorisations that are more readily quantified; this penchant for simplification represents an overly reductive approach that risks grave miscalculations. *See*: Solove, Daniel J., *Privacy and Power: Computer Databases and Metaphors for Information Privacy*. *Stanford Law Review*, Vol. 53, p. 1393, July 2001. Available at: <http://ssrn.com/abstract=248300>, p.1425

²⁸⁸ *See*: Erving Goffman, *The Presentation of Self in Everyday Life* (Garden City, Doubleday & Company, 1959).

²⁸⁹ *See*: Blumenstock, Chokkalingam et al, *Probabilistic Inference of Unknown Locations - Exploiting Collective Behavior when Individual Data is Scarce*, ACM DEV-5 (2014), December 5–6, 2014, San Jose, CA, USA, Available at: <http://dx.doi.org/10.1145/2674377.2674387>, p.8

²⁹⁰ Gandy indeed asserts that profiling to form predictive models of human behaviour is premised on the flawed contention that the "identity of the individual can be reduced, captured, or represented by measurable characteristics." *See*: Gandy Jr, Oscar H. "Exploring identity and identification in cyberspace." *Notre Dame JL Ethics & Pub. Pol'y* 14 (2000), pp.1100-1101

²⁹¹ *See*: Murphy, E., 2007. *The new forensics: Criminal justice, false certainty, and the second generation of scientific evidence*. *California Law Review*, pp.721-797; *see also*: PCAST, *Report To The President - Forensic Science in Criminal Courts: Ensuring Scientific Validity*, September 2016,

based upon processing of location data reflects recent technological and methodological developments that portend an evolving paradigmatic shift in the way in which citizens' activities are monitored, measured and interpreted. Moreover, predictive modeling based upon the profiles rendered represents an aspect of surveillance that is particularly pertinent.²⁹²

At this juncture it is necessary to distinguish between surveillance that focuses on the individual, targeted surveillance, and broader monitoring of the population, which constitutes mass surveillance. For the purposes of this research, 'personal surveillance' is taken to mean the surveillance of an identified person. Use of the term mass surveillance is applied to the practice of monitoring groups of people²⁹³ and,

Available at:

https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf

²⁹² The 2007 report of the of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism provides a working description of the two principle types of profiling utilised by law enforcement and the intelligence services:

"Profiling is generally defined as the systematic association of sets of physical, behavioural or psychological characteristics with particular offences and their use as a basis for making law-enforcement decisions. Profiles can be either *descriptive*, i.e. designed to identify those likely to have committed a particular criminal act and thus reflecting the evidence the investigators have gathered concerning this act; or they may be *predictive*, i.e. designed to identify those who may be involved in some future, or as-yet-undiscovered, crime." *See*: UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 33. *See also*: Moeckli, Daniel, Human Rights and Non-discrimination in the 'War on Terror' (July 22, 2008). Daniel Moeckli, HUMAN RIGHTS AND NON-DISCRIMINATION IN THE 'WAR ON TERROR', Oxford University Press, 2008. Available at: <http://ssrn.com/abstract=1161103>, pp.197-215 and Moeckli, Daniel, Terrorist Profiling and the Importance of a Proactive Approach to Human Rights Protection (December 16, 2006). Available at: <http://ssrn.com/abstract=952163> or <http://dx.doi.org/10.2139/ssrn.952163>, pp.1-6

²⁹³ Of critical importance then as regards the use of predictive analytics is how we frame the notion of group characteristics - the term may potentially be interpreted in a wider sense than that which corresponds to a more determinate elucidation.

See: UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 38.

"In the view of the Special Rapporteur, data-mining initiatives based on broad terrorist profiles that include group characteristics such as religion and national origin may constitute a disproportionate and thus arbitrary interference with the right to privacy, guaranteed by article 17 of the International Covenant on Civil and Political Rights (ICCPR)." The ICCPR defines group only in the context of the "family" (Article 23) and "ethnic, religious or linguistic minorities" (Article 27). Article 26 of the ICCPR prohibits discrimination and outlines a non-exhaustive list of proscribed grounds for such treatment - including language, religion, political or other opinion (amongst other criteria), affirming that all persons "are equal before the law and are entitled without any discrimination to the equal protection of the law." Increasingly however 'group' may be interpreted more expansively. Thus, the point at issue is how in this particular context we are to determine the criteria for establishing which group characteristics might prove disproportionate in their application to distinguishable associations in the context of profiling.

most commonly, large groups.²⁹⁴ Customary distinctions such as these warrant reappraisal where developing technologies increasingly question how distinctions are made, and to what extent attributes or activities are ascribed to represent a collective or an individual. This is especially pertinent where online technologies may render this distinction between ‘individual’ and ‘group’ increasingly indeterminate.²⁹⁵

Varying definitions of the term ‘profiling’ exist. This observation reflects competing notions of a practice that may constitute a diverse range of activities directed toward developing and utilizing models distinguishing a range of traits and characteristics. Moreover, profiling takes place across different sectors and in a broad range of contexts, both of a commercial and non-commercial nature, and by a gamut of public and private actors.²⁹⁶ It is necessary too at this juncture to make certain conceptual and practical distinctions for the purposes of clarifying the scope of this research piece.

Profiling may be divided into different stages. Accordingly, the phases of developing a profile may be broken down into three parts, as: 1) Pre-profiling: the collection and storage of data; 2) Profile-making: the analysis of data collections in order to make profiles; 3) Profile use: the application of a profile in a specific case.²⁹⁷ The scope of the review made in this chapter of the study reflects the latter two aspects, for the purposes of attaining a more detailed understanding of the particular issues that pertain to the application of profiling in decision-making. This prioritization reflects an emphasis analysing the potential processing of personal location data for profiling, rather than the technical means by which it is collected, which is studied in more

²⁹⁴ *See, for example:* Roger Clarke, Information Technology and Dataveillance, November 1987, Available at: <http://www.rogerclarke.com/DV/CACM88.html>

²⁹⁵ The somewhat nebulous and indefinite nature of certain association evolving through the discourse enabled by online social networks is discussed in more depth by Glassman in ‘Occupying the Noosystem: The Evolution of Media Platforms and Webs of Community Protest’. *See* M. Glassman, Occupying the Noosystem: The Evolution of Media Platforms and Webs of Community Protest, Berkeley Planning Journal, 25(1), 2012, Available at: <http://www.escholarship.org/uc/item/5ws9b7f5>.

²⁹⁶ Accenture, Analytics in Action: Breakthroughs and Barriers on the Journey to ROI, 2013, Available at: http://www.accenture.com/SiteCollectionDocuments/us-en/landing-pages/analytics-in-action/accenture_analytics_in_action_survey.pdf, p.4 *See also*, for example: J.A. Roberts, Profiling Levels of Socially Responsible Consumer Behavior: A Cluster Analytic Approach and Its Implications for Marketing, Journal of Marketing Theory and Practice, Vol. 3, No. 4 (Autumn, 1995), pp. 97-117

²⁹⁷ *See:* Koops, Bert-Jaap, Some Reflections on Profiling, Power Shifts, and Protection Paradigms (June 2008), p.1, Profiling The European Citizen, Hildebrandt & Gutwirth, eds., Springer, 2008. Available at: <http://ssrn.com/abstract=1350584>

detail in the subsequent chapter. A focus is placed on the methodologies that pertain to behavioural profiling, reflecting the potentiality intrinsic to the processing of personal location data. Behavioural profiling involves collecting data (recording, storing and tracking) and searching in it for identifying patterns (with the help of data mining algorithms).²⁹⁸

3. Developing predictive profiling using location data for surveillance purposes – social network site analysis as an analogy

Predictive profiling employs probabilities-based analysis in order to identify suspects and target them for surveillance, noting that this practice constitutes an actuarial approach (in contrast to that of the explicitly heuristics-based method of descriptive profiling) as the method does not rely entirely on an evaluation of probabilities, but is contingent on the establishment of statistical correlations for the purposes of extrapolating where future activities of concern may take place.²⁹⁹

The distinction between *descriptive* and *predictive* profiling has to date evolved in accordance with established differentiations made between anticipatory or preparatory acts. Descriptive profiling relies upon information and evidence in connection to a specific occurrence or set of pre-existing circumstances, and is intended to distinguish parties likely to have engaged in specific acts of a certain nature connected with these scenarios, whereas predictive profiling resolves to identify, in advance of a future act, those individuals who may be predisposed toward engaging in unlawful activities for the purposes of prevention.³⁰⁰

While advances in computing may allow for more nuanced forecasting capabilities based on extrapolating trends and patterns from assembled data, such activity is premised on the assumption that future behaviour be predicated upon prior observation, qualifying and characterizing behavioural attributes and, in turn,

²⁹⁸ Claude Castelluccia, Behavioural Tracking on the Internet: A Technical Perspective, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Springer, 2012, p.21

²⁹⁹ Harcourt, B. E. (2003). The shaping of chance: Actuarial models and criminal profiling at the turn of the twenty-first century. *The University of Chicago Law Review*, 70, p.109

³⁰⁰ D. Harris, Profiles in Injustice: Why Racial Profiling Cannot Work (2003), pp. 10, 19-20, 26.

construing potentialities based upon ostensibly rational criteria. The inductive approach, when applied to behavioural profiling, to an extent depends upon the acceptance of the presumption that there exist a consistency of, and a correlation between, the behaviour of individuals (thus accepting there exists a homogeneity of ‘types’); and, finally, that there exists a reliability and stability in the data.³⁰¹ In this respect, of relevance is a consideration of the broader purpose behind surveillance. Clarke describes surveillance as:

“[T]he systematic investigation or monitoring of the actions or communications of one or more persons. Its primary purpose is generally to collect information about them, their activities, or their associates. There may be a secondary intention to deter a whole population from undertaking some kinds of activity.”³⁰²

The implementation of social network site analysis may furnish useful insight into how the future use of location data modelling and analysis could evolve. Social network analysis can provide a powerful set of tools for describing and modeling the relational context in which behaviour takes place, as well as the relational dimensions of that behaviour.³⁰³ Citizens today interact with online social network sites and transfer large quantities of their personal information in a manner that is unprecedented.³⁰⁴ Some indeed submit that citizens have been subject to a significant transformatory process in recent years, perhaps of an irreversible nature, as a result of our utilizing the technology to communicate and forge relationships.³⁰⁵

³⁰¹ Hammond S., *Offender Profiling Of Sexual Offences*, Broadmoor Hospital, 2007, p.3, Available at: http://www.ramas.co.uk/offender_prof.pdf

³⁰² Clarke R., *Information Technology and Dataveillance*, November 1987, Available at: <http://www.rogerclarke.com/DV/CACM88.html>,

³⁰³ C.T. Butts, *Social network analysis: A methodological introduction*, *Asian Journal of Social Psychology* (2008), 11, 13–41, p.13

³⁰⁴ Membership of social network sites such as Facebook, Google+ and MySpace have experienced exponential growth in recent years - a phenomenon that to date has evidenced few indications that an increasing reliance on the utility of these sites will wane. Nielsen, *State Of The Media: The Social Media Report 2012*, April 2012, p.2 Available at: <http://www.nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html>

See also: S. Lohr, *How privacy vanishes online*, March 17 2010, Available at: <http://www.nytimes.com/2010/03/17/technology/privacy.html>

³⁰⁵ Tene asserts: “This new generation of users consists of individuals who post and search for personal, often intimate, information online; communicate with friends and colleagues on social networks.” See: Tene, Omer, *Privacy: The New Generations* (November 17, 2010), *International Data Privacy Law*, 2010, p.17 Available at: <http://ssrn.com/abstract=1710688>

Whilst the surveillance of online social networks to counter the complex and asymmetrical nature of certain threats presented to security and public order by their misuse³⁰⁶ has motivated substantial research into the use of advanced information technology to analyze and counter these threats, the risks the use of these techniques may pose to fundamental rights remains inadequately explored. In addition, this analysis is especially opportune insofar as more complex interactive services are anticipated to appear, which will further harness the power of social connections and personal data.³⁰⁷

Advances in communication technologies, coupled with the wider availability of networked mobile devices, have further encouraged citizens to share location data and other forms of personal data.³⁰⁸ In this context we need consider how online communication relates not only to expression, but also to associational activity:

“The proliferation of online communities demonstrates that people participate in online communication not only for the content but also to interact with other communicators, especially those who share their interests or concerns.”³⁰⁹

³⁰⁶ A report prepared for the Research and National Coordination Organized Crime Division for Law Enforcement in Canada affirms: “Online social media sites can be used to coordinate criminal activities among networks of people who have never met each other offline, to identify criminal opportunities and to defraud.” See: R. Frank, C. Cheng, V. Pun, *Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities*, Research and National Coordination Organized Crime Division Law Enforcement and Policy Branch Public Safety Canada, Report No. 021, 2011, 2011, p.22, Available at: <http://www.sfu.ca/icrc/content/PS-SP-socialmedia.pdf>.

³⁰⁷ Claude Castelluccia, *Behavioural Tracking on the Internet: A Technical Perspective*, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Springer, 2012, p.27

³⁰⁸ In alluding to the complexity of the challenges associated with an increasing array of disparate communications technologies, the US Subcommittee on Crime, Terrorism, and Homeland Security reported: “It is no longer the case that the technology involved in communications services is largely standard. Now, communications occur through a variety of means, including cable, wireline, and wireless broadband, peer-to-peer and VOIP services, and third party applications and providers.” See: United States House of Representatives. Committee on the Judiciary. Subcommittee on Crime, Terrorism and Homeland Security. Hearing on: ‘Going dark: Lawful electronic surveillance in the face of new technologies’. Available at: http://judiciary.house.gov/hearings/printers/112th/112-59_64581.PDF, February 2011. Serial No. 112-59. U.S. Government Printing Office. Washington, p.5

³⁰⁹ Kim M., “The Right to Anonymous Association in Cyberspace: US Legal Protection for Anonymity in Name, in Face, and in Action”, (2010), p.52, Available at: <http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/kim.asp>

Increasingly, civil society engages in political activity not by traditional face-to-face associations but through online acquaintances such that campaigns and coalitions can less easily be defined by way of organized membership, policies and objectives.³¹⁰ Social media platforms thrive on both sharing causes and establishing causes to rally around.³¹¹ These associations represent a profuse range of different interest groups and affiliations, and indeed reflect the diversity and the plurality of opinions, convictions and beliefs that are represented in modern societies. Online social network sites have made collective activity more accessible at lower cost, while at the same time diminishing the importance of parties' geographical proximity to one another. Associations may develop and achieve growth at a pace heretofore deemed unthinkable prior to the advent of social media applications.

These changes afford minorities and smaller interest groups the ability to exercise more influence; scholars such as Acquisti and Gross have underscored that an increasing confidence in the use of mobile digital technologies, coupled with the self-reinforcing tendency of those utilizing online social networks to encourage ever greater transparency and disclosure, has magnified the effects of the utility of information sharing. This change has further challenged the conceptualisation of both public and private spheres as determined by distinctions drawn between online and offline environments.³¹²

The availability of increasingly sophisticated location-based services on mobile devices is also proving especially important in respect of their allowing individuals to communicate with previously unacquainted individuals.³¹³ This transformation

³¹⁰ D. Runtzen and J. Zenn, Association and Assembly in the Digital Age, *The International Journal of Not-for-Profit Law*, Volume 13, Issue 4, December 2011, Available at:

<http://www.icnl.org/research/library/files/Transnational/Assoc%20Assemb%20Digital%20Age.pdf>

³¹¹ Robin Thompson, Radicalization and the Use of Social Media, *Journal of Strategic Security* Volume 4 Issue 4 2011, p.176.

³¹² Alessandro Acquisti and Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, Privacy Enhancing Technologies Workshop (PET), 2006, Available at: <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf>, p. 1

³¹³ See: Boyd DB & Ellison NB (2007) Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-mediated Communication*. 13, 1, article 11. Available at: <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>

represents a significant shift in terms of the ubiquity of our interconnectedness toward others.³¹⁴

However, the benefits that stem from the use of services that utilize personal location data to connect individuals or groups wishing to communicate, can also function to promote or publicize unlawful activities and recruit others. In an allusion to this tendency the European Court of Human Rights noted in the *S. and Marper v. the United Kingdom* judgment:

“[B]eyond dispute that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today’s European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification.”³¹⁵

The further tendencies that Acquisti and Gross highlight in terms of the powerful networking effects of social network sites also, however, hint at its utility for those wishing to subvert its capabilities for illicit purposes.³¹⁶ The Appendix to the Recommendation of the Committee of Ministers to member states on the European Code of Police Ethics outlines as an objective of the police the detection of crime; surveillance activity of social network sites for the purposes of profiling thus falls within this remit.³¹⁷

The monitoring of the use of location-aware social networks has been classed as constituting a novel form of ‘open source intelligence’; in effect asserting that the method reflects an extension of established practices that simply take advantage of

³¹⁴ Boyd DB & Ellison NB (2007) Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-mediated Communication*. 13, 1, article 11. Available at: <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.

³¹⁵ *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 105, 4 December 2008

³¹⁶ A report by the Criminal Intelligence Services (CISC) of Canada in 2010 reported that criminal organisations use the technology “to communicate securely, conceal their activities, target victims, and locate skilled labour and valuable goods, such as large caches of stolen personal and commercial data.” The same report also noted that certain organised criminal networks “are exclusively virtual with illicit activities and communications occurring entirely online.” See CISC, 2010 Organized Crime Report, May 2010, Available at:

http://www.cisc.gc.ca/annual_reports/annual_report_2010/frontpage_2010_e.html

³¹⁷ Recommendation Rec (2001) 10 of the Committee of Ministers to member states on the European Code of Police Ethics, adopted by the Committee of Ministers 19 September 2001

newly available conduits for communication and information transfer.³¹⁸ This assertion discerns that a transition toward the surveillance of online social networks reveals a natural extension of a tradition of law enforcement seeking to appraise intelligence gathered from the growing number of overt, public information sources that exploit location data collection and processing.³¹⁹

The question therefore arises as to whether the fusion of this type of monitoring with predictive analytics could represent a fundamental shift stemming from its intrinsic capacity to accurately elaborate the dynamics of human mobility, interpersonal relationships and patterns of mobility.³²⁰ Development of these models would constitute a new capability that has to date proven particularly elusive to acquire.³²¹ In *Amann v. Switzerland* the European Court of Human Rights affirmed that the Swiss Government's contention that the storage of personal data could not be held to constitute an interference on Article 8 protections of the right to private life where: "the card contained no sensitive information about the applicant's private life", the latter "had not in any way been inconvenienced as a result of the creation and storing

³¹⁸ See, for example, the promotional material of software developers Paterva, which describes open source intelligence (OSINT) thus: "Open source intelligence (OSINT) is form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or classified sources)" See: Paterva, If this is Open Source - where can I get the source? 2017, Available at:

<http://www.paterva.com/web6/documentation/faq.php>

³¹⁹ The UK's Open Data Institute, for example, secured in early 2013 £10 million to research the use of 'open data' or 'open source intelligence' for the purposes of improving public security and the judicial system. See Open Data Institute, Knowledge for Everyone - Open Data Immersion Programme, 2013, Available at: <http://www.theodi.org/events/immersion-programme>.

³²⁰ Kayacik et al note that a user profile consists of temporal and spatial models based upon probability functions; each model focuses on establishing familiarity from different perspectives and detecting either specific temporal anomalies or location anomalies. See further: Kayacik, H.G., Just, M., Baillie, L., Aspinall, D. and Micallef, N., 2014. Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors, Available at: <https://arxiv.org/abs/1410.7743>, pp.1-3

³²¹ McCue, an authority on operational law enforcement and security analytics, argues that a significant amount of human engagement is required to ensure the accuracy of predictive analysis, casting doubt on the assertion that its use may always be less resource intensive than other means: "In general, analysts should expect to spend approximately 80% of their time preparing the data and 20% of their time analyzing it. While this sounds like a terribly unattractive prospect, if the data preparation is done well, huge benefits in the overall quality of the analysis can be reaped. Moreover, the analysts will gain additional insight into the data, which can further refine the analysis." See: C. McCue, *Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis*, (Oxford: Elsevier), 2007, p.93

of his card” was untenable. The Court further noted:

“The Court reiterates that the storing by a public authority of information relating to an individual’s private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding...”³²²

Oversight of the means by which information is acquired and disseminated within a society is integral to ensuring accountability, and functions to empower citizens in a democracy.³²³ Thompson hints at the possible benefits to law enforcement of embracing social network analysis where “every person with a cell phone and a social media application is a ground sensor capable of collecting and distributing raw, real-time intelligence.”³²⁴ Gibson too highlights the pivotal nature of this interdependency, noting that a democratic society should allow for the intelligence function to perform reciprocally, reflecting a two-way relationship with the public:

“The public trusts it and it creates trust in the collective mind of the public. The currency of exchange is information, in the broadest sense of the word. If that currency is restricted then trust diminishes with it.”³²⁵

Crucially, the question thus arises as to whether or not profiling personal location data pertaining to social networking activity and other online activities could constitute a profound transformation in terms of how society conceives of the parameters to which lawful surveillance may extend.³²⁶

³²² *Amann v. Switzerland* [GC], no. 27798/95, § 68, p.20, ECHR 2000-II

³²³ The “democratizing effects” effects of Internet discourse were highlighted in the judgment of the US case *ACLU v. Reno* in 1996: “It is no exaggeration to conclude that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country - and indeed the world - has yet seen. The plaintiffs in these actions correctly describe the “democratizing” effects of Internet communication: individual citizens of limited means can speak to a worldwide audience on issues of concern to them... [T]he Internet may fairly be regarded as a never-ending worldwide conversation.” - *ACLU v. Reno*, 929 F.Supp. 825 (ED.Pa. 1996), aff’d, 521 U.S. 844 (1997).

³²⁴ Robin Thompson, *Radicalization and the Use of Social Media*, *Journal of Strategic Security* Volume 4 Issue 4 2011, p.176

³²⁵ Stevyn Gibson, *Open Source Intelligence An Intelligence Lifeline*, *RUSI Journal*, February 2004, p.3, Available at: <http://www.rusi.org/downloads/assets/JA00365.pdf>.

³²⁶ Horvitz, a researcher at Microsoft Research, notes: “Large amounts of data are being collected in part because of the shift of many human activities to the Web – and that has made it easy to collect transactions and events of various kinds in stream with activities.” See: ‘A Golden Era of Insight: Big

Distinctions between the ‘private’ and ‘public’ may therefore risk being further obfuscated. For example, Briggs highlights the extent to which citizens’ social activities challenge the public-private dichotomy, noting that personal information may be made more accessible by a process of ‘social appropriation’:

“Developments of this type are interesting because they significantly enhance our ability to predict patterns of behaviour and personal preference in a way which is context sensitive... private histories can become public by a process of social appropriation. The power to combine such personal histories with rich contextual data suggests a future in which our daily habits and preferences can become highly accessible to others.”³²⁷

Similarly, Castelluccia forewarns of a danger whereby we drift unwittingly into a condition whereby surveillance of our behaviours becomes pervasive, tacitly accepting that our movements are subject to monitoring recorded and correlated for the purpose of determining whether our behaviour suggests a tendency to engage in malevolent pursuits.³²⁸

4. Profiling associations: data-based insights into relationships

In *Klass and Others v. Germany* the European Court of Human Rights accepted that the existence of legislation allowing for the surveillance of telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.³²⁹ The analysis of location data collected and processed by telecommunications service providers may also serve this purpose to provide law enforcement and other public services with valuable intelligence to inform decision-making.

Data’s Bright Future’, Microsoft Research, 15 February 2013, Available at: <http://www.microsoft.com/en-us/news/features/2013/feb13/02-15BigDataHorvitz.aspx>.

³²⁷ P. Briggs, *Future Identities: Changing identities in the UK – the next 10 years*, UK Government Office for Science, January 2013, p.5

³²⁸ Claude Castelluccia, *Behavioural Tracking on the Internet: A Technical Perspective*, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Springer, 2012, p.22

³²⁹ *Klass and Others v. Germany*, 6 September 1978, § 48, Series A no. 28

Recent events have further prompted debate as to whether the prospect the increasing use by public authorities of location data processing in social network analysis bodes well for civil society.³³⁰ Sandburg notes that this evolution reflects a maturation of existing practice vis-à-vis ‘relational surveillance’ to deliver deeper insight into suspect activity by investigating the membership and relational structures of online association.³³¹

The ECJ’s final judgment in the case *Digital Rights Ireland and Seitlinger and Others* proves especially enlightening where it specifically examines considerations pertaining to defining the intrinsic value of location data, and the extent to which it constitutes personal data in this context.³³² The reasoning of the decision is illustrative of how location data continues to prove challenging in its conceptualization vis-à-vis other types of metadata, particularly as regards profiling. These conceptual difficulties appear to manifest inconsistencies in terms of how specifically location data is deemed a relevant consideration with regard to the broader data protection concerns of the individual. Adequate regard must be given to the specificities of location data and how its distinct attributes call for particular consideration in determining data protection risks. The judgment notes that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, are of a nature that:

“...Taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, *daily*

³³⁰ See, for example, the 2011 HMIC report discussing the role of location data and social network analysis in tracking disturbances in public protest following the London riots of 2010. HMIC, *The rules of engagement - A review of the August 2011 disorders*, 2011, Available at: <http://www.hmic.gov.uk/media/a-review-of-the-august-2011-disorders-20111220.pdf>

³³¹ Katherine J. Strandburg, *Surveillance of Emergent Associations: Freedom of Association in a Network Society*, December 2007, p.1, Available at: http://works.bepress.com/katherine_strandburg/11

³³² Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014, Available at: <http://curia.europa.eu>

or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.”³³³

The court’s pronouncement is especially percipient for its observation that the processing of location data may furnish information that characterises many different facets of an individual’s daily activities; the dimensions of these aspects relating to the person concerned is such that, taken as a whole, the knowledge attained potentially provides a very graphic view into their private life, particularly in respect of detailed correlations between places, interactions and associations.³³⁴ Notably, the aforementioned citation refers to the possible interferences that may be drawn where the processing of location data takes place, and allow for the investigation of social relationships.³³⁵

It has been suggested that this escalation for profiling purposes may furnish potentially ‘destabilizing’ interpretative accounts of human interactions, thus describing a transformative process that risks societal disorientation.³³⁶ In contrast, scholars such as Cohen have however argued that a greater risk associated with such techniques is that they attempt rendering individual behaviors and preferences transparent by conforming them to preexisting frameworks: this approach may in turn distort and misrepresent: “And in seeking to mold the future, surveillance also shapes the past: by creating fixed records of presence, appearance, and behavior, surveillance

³³³ Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014, Available at: <http://curia.europa.eu>. Note: *emphasis added*.

³³⁴ Whilst the ECJ ruling does not raise the issue of location-based profiling directly, its criticism of Directive 2006/24 does however extend to criticizing the legislation’s failure to articulate specific limitations in respect of the use of the data retained, noting: “In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued.” Indeed, in this context, amongst various concerns as regards the wider ongoing use of retained data by law enforcement officials, that retained location data could be used for the purposes of profiling behaviours is an eventuality that is of legitimate concern. *See*: Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014, Available at: <http://curia.europa.eu>

³³⁵ Researchers have already begun analyzing data sets from cellular-network operators in Europe, with a view to understanding characteristics such as individual mobility. Reades notes that in one month, a single phone company’s call data records (CDRs) can exceed seven billion records. *See*: Jonathan Reades, *People, Places & Privacy - Using Finite State Machines to preserve privacy while data mining the cellular phone network*, March 2009, Available at: <http://www.ucl.ac.uk/~ucftb48/Privacy.pdf>, p.2

³³⁶ David M. Berry, *The Computational Turn: Thinking About The Digital Humanities*, Culture Machine, Vol 12, 2011, p.12, Available at: www.culturemachine.net

constitutes institutional and social memory.³³⁷ Harcourt too explains that profiling of this nature may lead to social conformity, marginalising those that deviate from the norm and thus imposing a coercive effect to yield and conform.³³⁸ As technology has evolved emphasis has shifted from data operations (storage, access and the processing of data) to the evolving sphere of data science; reflecting a growing interest in the computation of data for the purposes of understanding, analysing and, most critically, forecasting crime.³³⁹ The dynamics of this change suggest a steady transition from a research basis towards its operational deployment in law enforcement and intelligence services.

Social network sites in particular constitute an extremely attractive source of open source intelligence for location data for the construction of profiles precisely because of the level of trust placed in them by users. Consequently, both the quantity, and detailed granularity of, the information pertaining to an individual's activities relative to their personal location at any point in time is significant.³⁴⁰ However, the value of any insight produced is open to question.³⁴¹ Despite the broader recognition of social networking analysis as a concept, the medium remains poorly understood, both in terms of its practical applications and in respect of the theoretical basis upon which any analysis is conducted.³⁴² As with any analytical tool its use necessitates a studied

³³⁷ See: Cohen, Julie E., *Privacy, Visibility, Transparency, and Exposure*. University of Chicago Law Review, Vol. 75, No. 1, 2008; Georgetown Public Law Research Paper No. 1012068, p.186, Available at: <http://ssrn.com/abstract=1012068>.

³³⁸ See: Harcourt, Bernard E., *Against Prediction: Sentencing, Policing, and Punishing in an Actuarial Age* (May 2005). Univ. of Chicago, Public Law Working Paper No. 94. Available: <http://ssrn.com/abstract=756945>, p.36

³³⁹ See: D. Smith, *Real-time Big Data Analytics: From Deployment to Production, Revolution Analytics*, Available at: <http://www.revolutionanalytics.com/news-events/free-webinars/2012/real-time-big-data-analytics>

³⁴⁰ R. Frank, C. Cheng, V. Pun, *Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities, Research and National Coordination Organized Crime Division Law Enforcement and Policy Branch Public Safety Canada, Report No. 021, 2011, p.22*, Available at: <http://www.sfu.ca/icrc/content/PS-SP-socialmedia.pdf>

³⁴¹ Analysts such as Coleen McCue, an operational law enforcement and security analytics specialist, suggest that experience underscores the limits to the utility of new surveillance technologies, and that predictive profiling utilizing location data has clear limits to its application. See: C. McCue, *Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis*, (Oxford: Elsevier), 2007, p.320

³⁴² Analysts at the Cyber Behavior and Defense Institute of Artis Research affirm their belief that too often the limitations of analytical models remains unacknowledged, noting: "Even data-driven network analysis misses the mark by concentrating too heavily on descriptions of network structures without making clear statements about why and how they matter to the collective behavior under inspection. Possibilities are generated, but probabilities cannot be. All too often, the individual human element is either missing or misconstrued in both the approach and application to understanding." See: ARTIS Research, *Network Analysis*, 2010, Available at: http://artisresearch.com/page_id=2337

approach, which requires comprehension of both its utility and its inherent risks and limitations.

4.1 Mining data for the analysis of inter-personal associations

Increasing computational capabilities make it possible to apply analytics to larger and larger datasets and raise the possibility of employing data mining techniques to uncover ‘suspicious’ patterns of association.³⁴³ The use therefore of location data to discern suspect activity and investigate individuals, their membership of groups, their structure and attempt to predict future behaviours brings to the fore questions as to the permissibility of such activity. The application of data mining to personal location data from sites such as social networks constitutes a continuing development of the medium of relational surveillance.³⁴⁴ While conceptually relatively well established, nonetheless the assimilation of social network analysis into a potentially more expansive form of relational surveillance, anticipating the delivery of compelling new insight into behavioural observation based on individual patterns of movement, presents hazards. Relational surveillance, which aspires to explain the nature of interactions and their purpose, highlighting suspicious patterns of association, harbours inherent risks — particularly in respect of its tendency to interfere with associational activity and free expression. Established doctrine pertaining to the rights to freedom of association, developed with respect to the protection of traditional notions of freedom of association, potentially provide strong protection against overreaching relational surveillance.³⁴⁵

³⁴³ Ugander et al describe the relatively onerous and time-consuming nature of the analysis of social networks prior to the advent of their online counterparts, noting: “Historically, studies of social networks were limited to hundreds of individuals as data on social relationships was collected through painstakingly difficult means. Online social networks allow us to increase the scale and accuracy of such studies dramatically because new social network data, mostly from online sources, map out our social relationships at a nearly global scale.” See: J. Ugander, B. Karrer, L. Backstrom, C. Marlow, *The Anatomy of the Facebook Social Graph*, 18 November 2011, p.1, Available at: <http://arxiv.org/abs/1111.4503>

³⁴⁴ See, for example: A.L. Barabasi, *Linked: The New Science of Networks*, Perseus Group, 2002, and Carrington, P.J., Scott, J. Wasserman, *Models and Methods in Social Network Analysis*, Cambridge University Press, New York, 2005.

³⁴⁵ K. Strandburg, *Surveillance of Emergent Associations: Freedom of Association in a Network Society*, p. 1, in ‘Digital Privacy: Theory, Technologies, and Practices’ (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis and Sabrina De Capitani di Vimercati, eds., Auerbach Publications, 2008)

Relational surveillance for the purposes of profiling may be regulated so as to ensure the necessary protection of the burgeoning role of emergent associations in civil society that develop through both online and offline interaction. These associations increasingly play a role in citizens' lives and encourage wider dialogue and engagement in society. In particular, the immediacy and asynchronous nature of online communications render them an especially efficient and efficacious tool in connecting those people who once felt disassociated; allowing parties to organise, mobilize and recruit others through highly connective social networks in a process that frequently obviates the need for either hierarchy or refinement of a strategy.³⁴⁶ Ugander et al have observed the growing influence of social network sites in online communication, asserting: "As individuals bring their social relations online, the focal point of the internet is evolving from being a network of documents to being a network of people, and previously invisible social structures are being captured at tremendous scale and with unprecedented detail."³⁴⁷

Significant too in our consideration of networked platforms for social interaction is their ability to originate associations that emerge and develop with unparalleled rapidity, affording scope for citizens to interact and mobilize at a rate that corresponds to the speed at which the Internet facilitates and encourages the swift interchange of information. Strandburg highlights the heterogeneity of emergent associations generated by such interaction:

"They can remain loosely connected or coalesce into more traditional forms of organization with paid staff, centralized decision making, and so forth. In an emergent association, strategies, issues, and positions can be selected democratically or imposed by a central leadership, but can also self-organize out of the independent actions of individuals. The low cost and many-to-many

³⁴⁶ In 2002 Rheingold wrote with startling prescience of a future techno-cultural shift empowering collective action and reinvigorating mobilization and association through consumer devices that enabled greater connectivity between citizens. *See*: Rheingold, Howard, *Smart Mobs: The Next Social Revolution*, Basic Books, 2002.

³⁴⁷ J. Ugander, B. Karrer, L. Backstrom, C. Marlow, *The Anatomy of the Facebook Social Graph*, 18 November 2011, p.1, Available at: <http://arxiv.org/abs/1111.4503>

structure of modern communication technology facilitates experimentation and cooperation between different groups.”³⁴⁸

A further benefit of such platforms is their capacity to enable and embolden those who are otherwise unempowered or marginalized, lacking capacity to leverage influence or resources. Surveillance may therefore jeopardize equality. The prohibition of discrimination is enshrined in the International Covenant on Civil and Political Rights (ICCPR). Articles 2(1) and 26 may be engaged where profiling-related activity relating to associations between parties constitutes towards a discriminatory practice on the part of a State agency based on grounds, for example, of gender, religion, political or other opinions.³⁴⁹ Mobilization of citizens encourages a collective effort that enfranchises and capacitates those whose persuasions reflect minority identities or opinions.

In this regard, the provision within the UN Code of Conduct for Law Enforcement Officials should also be considered with respect to the guarantee furnished by Article 2 and its commentary, 2(a), with regard to the duty of law enforcement officials to respect and protect human dignity and maintain and uphold the human rights of all persons.³⁵⁰ Also relevant in this respect is the Council of Europe Convention of 1981

³⁴⁸ K. Strandburg, *Surveillance of Emergent Associations: Freedom of Association in a Network Society*, p. 3, in ‘Digital Privacy: Theory, Technologies, and Practices’ (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinouidakis and Sabrina De Capitani di Vimercati, eds., Auerbach Publications, 2008)

³⁴⁹ *See*: UN International Covenant on Civil and Political Rights (ICCPR). Article 2(1) affirms: “Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.” Article 26 states: “All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.” In addition, Article 14 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states: “The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.” The Charter Of Fundamental Rights Of The European Union also stipulates within Article 21 of the treaty that: “Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.”

³⁵⁰ The commentary refers also to, *inter alia*, the ICCPR and the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), both of which contain provisions outlining the prohibition of discrimination. *See*: UN Code of Conduct for Law Enforcement Officials, General Assembly resolution 34/169, adopted 17 December 1979.

for the protection of individuals with regard to automatic processing of personal data, in which the limitations to which this processing is subject are outlined. The Convention provides, *inter alia*:

“Article 5 – Quality of data

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

Article 6 – Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards.

(...).”³⁵¹

The relevance of the above-cited provision may relate to personal data where data processing may, inferentially, reveal information connected with an individual’s political opinions or other beliefs. The possibility of such discovery is significant particularly where the facilitation of pseudonymity and anonymity in nascent associations encourages the development of relationships that would less likely exist where participants feel deterred should their affiliation court attention. Individuals with marginalized identities may use anonymity and the intrinsic spatial separation afforded by online discourse as protective tools that aid their engagement and participation in online interaction.”³⁵² Jonas Lerman has expressed concern as to the systemic omission of those individuals whose lifestyles place them on the margins of society, and hence potentially prejudice their access to fair data collection and processing activities, noting that they may exist on the periphery due to “poverty,

³⁵¹ COE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted Strasbourg, 28.1.1981

³⁵² Kim M., “The Right to Anonymous Association in Cyberspace: US Legal Protection for Anonymity in Name, in Face, and in Action”, (2010), p.1, Available at: <http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/kim.asp>. Research has shown that participation in online associations is more highly valued by people with marginalized, concealed or stigmatized identities (for example, by those who may not feel able to disclose their sexual orientation publicly, or those with extreme political beliefs). *See*, for example: S Watt, M Lea, and R Spears, “How Social is Internet Communication? A Reappraisal of Bandwidth and Anonymity effects” in S Woolgar (ed) *Virtual Society?: Technology, Cyberbole, Reality* (2002) 61-62; K McKenna and J Bargh, “Coming out in the Age of the Internet: Identity ‘Demarginalization’ through Virtual Group Participation” (1998) 75 *Journal of Personality and Social Psychology*, 681-694.

geography, or lifestyle, and whose lives are less ‘datafied’ than the general population’s.”³⁵³ Crawford too has also voiced her unease over marginalisation, stating: “not all data is created or even collected equally, there are ‘signal problems’ in big-data sets—dark zones or shadows where some citizens and communities are overlooked or underrepresented.”³⁵⁴ Data-generating activities should be understood in the context therefore of mobility; as *Barocas and Selbst* observe, different groups within communities have differentiated access to, and relatively less fluency, in the new technologies.³⁵⁵ Others have expressed concern based in part on the inability of citizens to apprehend both the extent and significance of their online activity being tracked, which underscore the possible ramifications of a move toward a more prevalent or pervasive monitoring.³⁵⁶ Privacy and data protection concerns nonetheless also arise where citizens are generally aware of a surveillance capability of an installed technology, but are unable to discern how exactly their behaviour is being observed. This problem is further exacerbated by moves toward both the miniaturization and greater embeddedness of location sensing technologies, in addition to the greater precision in the capacity for data capture such devices now inhere.³⁵⁷

Surveillance that monitors the patterns of movement of citizens may risk constituting interference in the formation of associations. Location-based services allow for communication and the development of associations online through social networks sites that may evolve in a manner that is all but invisible in the offline world. Monitoring may engender a feeling of agitation amongst those being observed; those being watched may develop anxieties as to whether their interactions with others may

³⁵³ Lerman, J., “Big data and its exclusions.” *Stanford Law Review Online* 66 (2013), p.55

³⁵⁴ See: Kate Crawford, *Think Again: Big Data*, Foreign Policy (9th May, 2013), Available at http://www.foreignpolicy.com/articles/2013/05/09/think_again_big_data

³⁵⁵ Barocas, Solon and Selbst, Andrew D., Big Data's Disparate Impact (2016). 104 *California Law Review* 671 (2016). Available at: <https://ssrn.com/abstract=2477899>, p.14

³⁵⁶ Lockwood notes that whilst most of those using networked mobile devices are generally aware that their phone calls, text messages and other communications data are relayed by cellular towers and other channels of transmission, only a small minority appreciate the express precision of the location data the technology may impart to service providers and other parties to whom access is granted. See: S. Lockwood, Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, 18 *HARV. J.L. & TECH* (2004), pp.313-314

³⁵⁷ In this regard Uteck has asserted that the concealed nature of such technologies may in effect create an ‘embedded panopticon’ allowing for a pervasive and covert surveillance hidden in the environment. See: Uteck, Anne, *Ubiquitous Computing And Spatial Privacy* (March, 2009), p.89, *Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society*, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/799

be misunderstood, their associative behaviours misinterpreted.³⁵⁸ Even absent any anxiety, this intervention may nonetheless evince subtle changes to the individual's mental state (for instance, in respect of the sense of seclusion). The effect of seclusion requires further examination, such that we may apprehend the meaning of 'invisibility' and determine its relationship to locational privacy.

It would appear that the complexity of advancements in location-based technologies is such that citizens cannot reasonably be expected to comprehend the nuances of their implementation and operation. Moreover, it is becoming increasingly challenging to maintain a profile that guards the data subject from undesired disclosures.³⁵⁹ Enhancements in the methods made possible by geolocation thus may also more broadly influence how, henceforth, we draw the necessary distinctions in surveillance between that which is notionally observed imperceptibly and covertly, and activities that rely upon seemingly overt, conspicuous monitoring. This differentiation is particularly important in the realm of location data processing for the purposes of developing models of predictive behavioural profiling based on patterns of movement. Efforts to collate and analyze different individuals' personal location data for the purposes of discerning the composition of relationships between parties may pose a risk where it exposes and reveals entirely innocuous yet sensitive nascent relationships and interactions that would otherwise remain undetected.³⁶⁰

Recognizing this risk, Rachels highlights the importance of this concern with regards to the risk an interference might pose to the privacy of the individual and parties with whom they associate, stating that the requisite measure for privacy protection should assure individuals "...the important power to share information discriminately, which in turn enables them to determine not only how close they are to others, but the nature

³⁵⁸ See: Solove, Daniel J., *Reconstructing Electronic Surveillance Law*. *George Washington Law Review*, Vol. 72, 2004, p.1708 Available at: <http://ssrn.com/abstract=445180> or <http://dx.doi.org/10.2139/ssrn.445180>

³⁵⁹ See: Gelman, Lauren Amy, *Privacy, Free Speech, and 'Blurry-Edged' Social Networks* (November 1, 2009). *Boston College Law Review*, Vol. 50, No. 5, 2009, p.1329, Available at: <http://ssrn.com/abstract=1520111>

³⁶⁰ Rachels highlights the importance of this concern with regards to the risk an interference might pose to the privacy of the individual and parties with whom they associate, stating that the requisite measure for privacy protection should assure individuals "...the important power to share information discriminately, which in turn enables them to determine not only how close they are to others, but the nature of their relationships. See: Rachels, J., *Why Privacy Is Important*, in *Philosophical Dimensions of Privacy: An Anthology*, Ferdinand D. Schoeman, ed., Cambridge: Cambridge University Press, (1984), p.294

of their relationships.”³⁶¹ Uteck argues that circumstances, interpreted in accordance with given contextual considerations, establish the conditions by which we anticipate protection from intrusive interference, and notes that this expectation is a nuanced, contextual and fundamentally normative exercise.³⁶²

Thus we might surmise that surveillance activity discovering such relationships warrants particular oversight. The exposure of nascent associations to wider critical examination and inspection may constitute a chilling effect that serves to stymie critical debate in a democratic society. A particular concern therefore is the ostensible ‘discovery’ of associational patterns that may be in turn be classified in accordance with certain designations of behaviour. Exceptional care is needed where this analysis undertakes to resolve whether the development of these associations and interactions may herald a tendency to engage in unlawful activities. In these circumstances, the application of predictive profiling techniques proves pre-determinate and risks evidencing emergent associations before members even recognize or comprehend their own affiliations with others.

Should surveillance of this nature impose in this way upon the individuals connecting with one another and imparting information for fear of attracting unsolicited attention, citizens might well moderate their level of engagement and enquiry where they anticipate possible exploratory forays into their behaviours by the State. This hesitancy to participate in discourse and debate would likely prove the more consequential where topics may be perceived by some as reflecting subversive tendencies.

The repercussions of an overly intrusive approach are therefore considerable. In *Klass and Others v. Germany* the European Court of Human Rights stressed that States must exercise caution in their exercise of surveillance lest its use risk undermining the very democracy it use is intended to protect:

³⁶¹ Rachels, J., Why Privacy Is Important, in *Philosophical Dimensions of Privacy: An Anthology*, Ferdinand D. Schoeman, ed., Cambridge: Cambridge University Press, (1984), p.294

³⁶² Uteck, Anne, *Ubiquitous Computing And Spatial Privacy* (March, 2009), p.89, *Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society*, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/799

“Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.”³⁶³

Knowledge that social network site activity may be subject to an extensive regime of monitoring interactions with other parties could foster a growing reticence amongst users to debate. Individuals may feel inhibited and constrained by such a development, particularly where the degree of engagement (in terms, for example, of the level and frequency of interaction with another party) likely to invite suspicion and the advent of a more comprehensive mode of surveillance remains opaque.

4.2 Exploiting link analysis and patterns of association in predictive profiling

The implementation of data mining of location data utilizing predictive analytics capabilities may allow for the discovery of associational patterns within an identified network to distinguish between differences in the participatory engagement of different individuals.³⁶⁴ Another practice, link analysis, may be used in conjunction to extract underlying information pertaining to an individual’s subsidiary associations with less immediate groups.³⁶⁵ Lastly, the review of publicly available information such as that offered on social network sites may also incorporate data mining activity

³⁶³ *Klass and Others v. Germany*, 6 September 1978, § 49, Series A no. 28

³⁶⁴ McCue notes: “Predictive analytics encompasses a variety of model making tools or algorithms that can be employed to characterize historical information, which then can be used to predict the nature and likelihood of future events or occurrences.” See C. McCue, *Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis*, (Oxford: Elsevier), 2007, p.117

³⁶⁵ De Rosa notes that subject-based link analysis mines data sets to determine links between a subject and other people, places, or things. De Rosa further affirms that this technique is already being used for background investigations and as an investigatory tool in national security and law enforcement investigations. See: M. De Rosa, *Data Mining and Data Analysis for Counterterrorism*, March 2004, Center for Strategic and International Studies (CSIS), p.6, Available at: http://csis.org/files/media/csispubs/040301_data_mining_report.pdf

that ventures to recognize patterns that may aid in the identification of further groups that may share heretofore-unidentified association.³⁶⁶

A primary objective, then, of the use of metrics to analyze activity is to allow comparison between different attributes of the interactions of users and the inferred associative networks.³⁶⁷ A person's function in relation to others may be qualified by tallying the various connections made with different users, based upon a correlation of location, while their role may also be measured and determined by the degree to which interconnections between unassociated parties pass via an individual acting as a conduit. Furthermore, analytics may also attempt to qualify the value of an association by characterizing reciprocity (i.e. discerning the extent to which connections are either mutual or otherwise only one-way).

We need consider therefore the impact that the implementation of this use of location data for profiling online associations may have on citizens. In this context, therefore, we need reflect that the most recent scholarship on human relationships indicates that our traditional offline social networks are perhaps surprisingly less complex than we might imagine.³⁶⁸ The corollary of this phenomenon being that even a minimal implementation of these profiling capabilities warrants consideration as to its wider

³⁶⁶ A concern arises as regards the extent to which correlations may be drawn between associations and groups, or indeed to parties sharing a similar background. The notion of background, in particular, may in the context of profiling reflect a broad conceptualization. Data mining by way of pattern-based analysis for the purposes of profiling individuals manifestly operates on the basis of determining a shared background of some sort. Thus, recognizing this fact, more specifically a review of the permissibility of distinctions drawn on the basis of 'background' need be refined so as to effectively explicate which classifications of 'background' allow for non-discriminatory profiling. *See*: UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 40, which states: "The Special Rapporteur is concerned that profiling based on stereotypical assumptions may bolster sentiments of hostility and xenophobia in the general public towards persons of certain ethnic or religious background."

³⁶⁷ Seifert, J. W., *Data Mining And Homeland Security: An Overview*, CRS Report RL31798, 2006.

³⁶⁸ *See, for example*: Bakhshandeh, Reza, et al. "Degrees of separation in social networks." Fourth Annual Symposium on Combinatorial Search, May 2011, p.18, Available at: <http://www.aaai.org/ocs/index.php/SOCS/SOCS11/paper/viewFile/4031/4352>. *See also*: Newman M (2010) *Networks: An Introduction*. Oxford University Press; Easley D, Kleinberg J (2010) *Networks, crowds, and markets: Reasoning about a highly connected world*, (Cambridge University Press). Additional research in computational statistics validates the assertion that this clustering effect on social network sites can be substantiated empirically. Ugander et al note the predominance of clustering on the Facebook social network site, which underscores the potentiality of even limited use of data mining capabilities in online social network site analysis to subject a disproportionately large number of citizens to surveillance activity. *See*: J. Ugander, B. Karrer, L. Backstrom, C. Marlow, *The Anatomy of the Facebook Social Graph*, 18 November 2011, p.13, Available at: <http://arxiv.org/abs/1111.4503>

effects. For instance, Strandburg has warned that: “Targeted link analysis and pattern analysis, which rely on entire networks of communications patterns, thus have the potential to sweep in a very large number of individuals and their associations in short order.”³⁶⁹

The use of link analysis-based profiling in a predictive context to pre-emptively intervene to prevent harmful activities through data mining implicates not just the individual under suspicion but also, crucially, that of his or her contacts, the acquaintances of these contacts, and so forth.³⁷⁰ Thus, whereby the approach undertakes to identify a more extensive web of interrelationships in which the individual of primary concern is embedded, associates are immediately implicated. However, in doing so, the actor engaged in the data mining activity may identify entirely innocuous relationships.³⁷¹ The analysis therefore aims as its objective the development of a more extensive depiction of the wider context of the initial, narrower conditions of an association.

The use of link analysis in profiling activity thus presents significant concerns as regards the extent to which this processing of location data may reveal and contextualize entirely innocent associations. As such, its effect may be to harbour the potential to inhibit and curtail free association, especially insofar as it may expose a suspect’s relations with other individuals and groups that are perhaps marginalized or in some other way socially or politically disfavored. The accuracy of the profiles created, which may be subject to further data processing using predictive analytics to model future behaviour, is a further important issue that needs to be considered. The results of link analysis, in particular, may obscure underlying inaccuracies pertaining

³⁶⁹ Katherine J. Strandburg, *Surveillance of Emergent Associations: Freedom of Association in a Network Society*, December 2007, p.6, Available at: http://works.bepress.com/katherine_strandburg/11

³⁷⁰ C. McCue, *Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis*, (Oxford: Elsevier), 2007, p.119

³⁷¹ For example, a person communicating with others via a social network site that is suspected of involvement in extremist activity may communicate with groups of people whose characteristics and behaviours vary considerably. Besides maintaining contact with members of an extremist group, she may also use the same mode of communication to liaise with family members and associates in a religious organization. Here, links analysis could be utilised to discern how a broader profile of the suspect and their association with others. While belonging to one group does not necessarily preclude membership in the other (for example, in the aforementioned case, being both a member of an extremist group and being a fellow believer in a religious sect) the use of links analysis is intended to adequately differentiate and discriminate such that the qualities of an association, its nature, be made evident within a wider context.

to the relationships depicted by the qualification of different associations. For example, where assumptions are made as to how user accounts are utilised (that there be a presumption that a login is used by a single individual, as the data subject, being a very real and relevant example in this context, for instance) there exists a discernible risk that the analysis will render intrusive models of associations and related behavioural activity.

The impact of misinterpretation in respect of possible interferences into the right to personal data protection is therefore clearly evident. The aforementioned example (that of several individuals using the same login — perhaps for reasons that are perfectly irreproachable — such as for efficiency or other rationales based on the manageability of a limited resource e.g. Internet connectivity, access to computing resources, financial cost, etc.) reflects a reality that must not be overlooked.

As such, the difficulties and impediments to modeling associations and developing insight into behaviour based on the processing of location data, presents certain risks that cannot be ignored. Individuals erroneously identified by such methods of analysis in profiling may suffer significant interferences. For example, should a suspect associate with several different, unrelated groups (again, we might take consider a targeted individual who maintains relations with an extremist group, a moderate political organization and a religious sect) profiling may manifest a categorization of an associate belonging to a legitimate parliamentary lobbying group as an extremist: the delineation between extremist group/political activist organization/religious sect having been obfuscated.

A further risk lies in the misinterpretation of personal data collected for analysis, insofar as the medium of social networks allows for users to interact in ways in which we are only beginning to understand the context. Studies have begun to identify norms, rules and behaviours that dictate communication via online platforms differs significantly from how we communicate offline and, for example, argue that there exists already an “online disinhibition effect” such that the invisible and anonymous

qualities of online interaction lead to disinhibited, more intensive, self-disclosing and aggressive uses of language.³⁷²

4.3 The specific risks inherent to pattern-based profiling

Pattern-based approaches to identifying and qualifying the nature of associations seek first to identify associated groups using an algorithm that identifies cluster-types. Then, in a second stage, the method probes for potential signatures attributable to the type of group that are of interest.³⁷³ Where specific signatures are confirmed the known networks can be examined to discern whether any matching associations may be exposed.

Thus of crucial importance in determining the acceptability of this approach is the precision of the clustering algorithm implemented to chart and depict the associational groups within the wider body of data, including location data, collated and examined; ultimately the exactitude and validity of each search being a reflection of the accuracy of the model utilized to identify groups of interest.³⁷⁴ The 2007 report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism notes: “Detailed profiles based on factors that are statistically proven to correlate with certain criminal conduct may be effective tools better to target limited law-enforcement resources.”³⁷⁵ Whether in this context

³⁷² See: J. Suler, ‘The online disinhibition effect’, *Journal of Cyberpsychology and Behaviour* 7, no. 3, 2004, pp. 321–6. See also: J. Suler, ‘The psychology of cyberspace: the online disinhibition effect’, <http://users.rider.edu/~suler/psycyber/disinhibit.html>.

³⁷³ J. Millar, *Core Privacy - A Problem for Predictive Data Mining* (March, 2009), p.104, *Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society*, New York: Oxford University Press, 2009; Available at: *On the Identity Trail - Lessons From the Identity Trail*, <http://idtrail.org/content/view/799>.

³⁷⁴ Strandburg argues that the algorithms developed for the clustering of associations with large networks are inappropriate when analysing social network sites, venturing to proclaim that they are “not particularly accurate” and “computationally expensive” and slow. Strandburg further notes: “To some extent these difficulties are inherent in the closely connected structure of social networks, which renders associations difficult to disentangle and mistaken identifications inevitable.” See: K. Strandburg, “Surveillance of Emergent Associations: Freedom of Association in a Network Society,” in *Digital Privacy: Theory, Technologies, and Practices* (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis and Sabrina De Capitani di Vimercati, eds., Auerbach Publications, 2008), p.8

³⁷⁵ UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 33

the correlations established meets the requirement for being “statistically proven” remains subject to conjecture.

Exceptional prudence is required when conducting profiling of behaviour using pattern-based network analysis, especially where the inferences drawn are then utilised to extrapolate the behaviour that is then exhibited via a predictive approach.³⁷⁶ Data mining that applies pattern-based searches to elaborate sequences and arrangements from large datasets attempts to discover implicit correlations. Efforts to pinpoint, intercede and prevent future activity through the application of pattern-based data mining must acknowledge the limitations of this method in this distinct context.³⁷⁷

In conducting profiling to uncover these associations, and then parse the multitude of interconnections that are revealed, one may disclose and give prominence to an array of lawful and permitted groups in addition to those that potentially harbour a disposition toward criminality. Certain groups that are identified in this manner may legitimately desire to minimise their exposure. With justification, such associations may affirm that this differentiation and identification constitutes an interference in the fundamental rights of the persons concerned. The impact of this discovery and identification must be subjected to review, so as to determine whether this interference meets the requirement by which the interference is necessary in a democratic society: for example, in the interest of public security. The notion that a legitimate association would not fear its exposition, regardless of the narrowness of

³⁷⁶ Boyd notes the perils of becoming too reliant on an unfailing belief in the authenticity of trends extrapolated from data: “It is the kind of data that encourages the practice of apophenia: seeing patterns where none actually exist, simply because massive quantities of data can offer connections that radiate in all directions.” *See*: Boyd, Danah and Crawford, Kate, *Six Provocations for Big Data - A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, September 2011, p.5 Available at: <http://ssrn.com/abstract=1926431>.

³⁷⁷ Rubinstein et al note the large data sets needed to make pattern-based analysis viable, hinting at its possible intrusiveness in requiring data generated by the lawful activities of citizens: “Because terrorists do not ‘stand out,’ intelligence and law enforcement agents want to do more than rely exclusively on investigations of known suspects. The new goal is to search “based on the premise that the planning of terrorist activity creates a pattern or ‘signature’ that can be found in the ocean of transaction data created in the course of everyday life. Accordingly, to identify and preempt terrorist activity, intelligence agencies have begun collecting, retaining, and analyzing voluminous and largely banal transactional information about the daily activities of hundreds of millions of people.” *See*: Rubinstein, Ira, Lee, Ronald D. and Schwartz, Paul M., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*. *University of Chicago Law Review*, Vol. 75, 2008; UC Berkeley Public Law Research Paper No. 1116728. Available at: <http://ssrn.com/abstract=1116728>, p.261

the confines by which this information is divulged, is unreasonable: to otherwise suggest to the contrary would be to affirm that any interaction between two parties might reasonably be subject to scrutiny.

Determining the significance of respective associative groups for the purpose of applying predictive methods is therefore problematic. Appreciable difficulties exist in developing coherent strategies that duly recognize the novelty of forecasting scarce and highly sporadic acts (such as those associated with atypical events linked to serious crime, being just one such example) that can be applied with the requisite accuracy. Prior research however reminds us that that our associations with one another are highly contextualized, and thus the interpretation of the information attributable to these interactions may of necessity be complex. In this respect, Fung asserts:

“Responses to information are inseparable from their interests, desires, resources, cognitive capacities, and social contexts. Owing to these and other factors, people may ignore information, or misunderstand it, or misuse it. Whether and how new information is used to further public objectives depends upon its incorporation into complex chains of comprehension, action, and response.”³⁷⁸

A critical issue is thus how profiling activities determine the appropriate paradigm to comprehend the relational structure (or structures) of divergent groups implicated in activities that might warrant surveillance by public authorities. In order that profiling activity reduces any predilection that it unfairly identifies legitimate associations, it must clearly make distinctions between the relational structures of a group implicated in unlawful activity and that of group engaging in permissible activities. However, such a presumption proves simplistic and untenable. A trait such as a disposition

³⁷⁸ Fung, Archon, Mary Graham, and David Weil. *Full Disclosure: The Perils and Promise of Transparency*. New York: Cambridge University Press, 2007, p.187. *See also* DEMOS, #Intelligence, 2012, Available at: http://www.demos.co.uk/files/_Intelligence_-_web.pdf?, at p.58, where the authors note: “[C]ontext is especially important for security and intelligence work because of the need for a high degree of confidence in information, the value of predictive and explanatory analyses, and the consequences of making errors.”

toward communicating in a covert or surreptitious manner could easily be apparent in both types of association.

Those who may be subject to discrimination (for example, based on ethnicity, sexual orientation, immigration or employment status or political opinion) could also favour seemingly clandestine modes of communication. In this regard, with respect to profiling conducted by police authorities, Article 49 of the European Code of Police Ethics stipulates that investigations made by law enforcement officials prove impartial and be suitably sensitive to citizens' requirements, stating:

“Police investigations shall be objective and fair. They shall be sensitive and adaptable to the special needs of persons, such as children, juveniles, women, minorities including ethnic minorities and vulnerable persons.”³⁷⁹

Pattern analysis must therefore evidence sensitivity toward these distinctions. An indiscriminate use, and reliance upon, the application of data mining techniques to data collated from social network sites results in the monitoring of a broad range of persons not suspected of any wrongdoing. When combined with other factors influencing the motives for profiling activities, some of these people will be further subject to intrusive surveillance merely on the basis of the profiling itself, again without any suspicion of wrongdoing on their part.

Indeed, also of importance here is whether the distinctions drawn are suitably specific, or rather reflect broader “profiles that reflect unexamined generalizations,” such that this practice reflects a disproportionate interference.³⁸⁰ Relevant to this context as regards policing is Recommendation No. R(87)15 on regulating the use of personal data in the police sector places on the collection of personal data. The appendix to the recommendation affirms that this activity should be limited to reflect the intention of suppressing a specific criminal offence, rather than reflect a broader preventative mandate of an unspecified description. The Appendix to

³⁷⁹ Recommendation Rec(2001)10 of the Committee of Ministers to member states on the European Code of Police Ethics, adopted by the Committee of Ministers 19 September 2001.

³⁸⁰ UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 34

Recommendation No. R(87)15 regulating the use of personal data in the police sector (adopted on 17 September 1987) states, *inter alia*:

“Principle 2 – Collection of data

2.1 The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation. ...”³⁸¹

Placing an unwavering faith in the capacity of any novel method to deliver unprecedented insight has in the past proven mistaken.³⁸² Where law enforcement errs by discouraging legitimate association its actions may quickly generate mistrust amongst the public. Mistrust generates suspicion and puts at risk the acceptance of a surveillance technique by citizens.

Interference in a person’s freedom of association can in turn foster a broader ambivalence in society that undermines minority groups’ entitlement to acceptance and equal treatment at the hands of public authorities. Poorly conceived investigations that expose undisclosed associations, however discretely conducted, are not without their injured parties. The 2007 report of the Special Rapporteur also highlighted the process of profiling practices that single-out persons for enhanced law enforcement attention may contribute to the social construction of groups to whom which suspicion may more generally be applied, noting: “This stigmatization may, in turn, result in a feeling of alienation among the targeted groups.”³⁸³

³⁸¹ Council of Europe, Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector, 17 September 1987

³⁸² McCue notes the manifest deficiencies in much of the data used in the context in question: "Regardless of how perfect a data set might seem to be, it almost always has some shortcomings. In law enforcement and intelligence analysis, the data and information generally are anything but perfect." See C. McCue, *Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis*, (Oxford: Elsevier), 2007, p.82

³⁸³ UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 57

5. Profiling location data: drawing inferences in relation to special categories of data

Directive 95/46/EC Article 13 allows for Member States to adopt legislative measures to restrict the scope of obligations and rights with respect to, *inter alia*, the processing of personal data to safeguard the prevention, investigation, detection and prosecution of criminal offences: thus in a domestic setting data processing in the area of police and judicial cooperation in criminal matters may be exempted from its provisions.

Council Framework Decision 2008/977/JHA³⁸⁴ in part attempts to address certain lacunae in respect of the existing legal framework for data protection in the EU, and provides for the protection of personal data that is processed in the framework of police and judicial cooperation in order to prevent, investigate, detect or prosecute a criminal offence or execute a criminal penalty. The Framework Decision has limited effect in respect of the domestic setting in the sense that where data originates and is processed within a Member State its provisions do not apply. In essence, then, it cannot be qualified as a comprehensive framework as its provisions do not have general application. However, in the context of satellite-based and internet-enabled geolocation provisions pertaining to the cross-border transfer of data processing, its provisions shall be applicable in assessing compliance with its data protection requirements.³⁸⁵

In particular, Article 6 of the Council Framework Decision 2008/977/JHA, which refers to the processing of special categories of data, is relevant where personal data processing may elicit information directly pertaining to circumscribed special categories such as political opinions, religious or philosophical beliefs or trade-union membership, or indeed data concerning health or sex life. The provision does not explicitly refer to location or mobility-related data; rather we need consider how it might in effect constitute a proxy as representative of other sensitive data based on an

³⁸⁴ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Available at: http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/jl0018_en.htm.

³⁸⁵ Framework Decision 2008/977/JHA Preamble, recital 7 states: "The scope of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States."

individual's choices. For example, a citizen visiting a mosque or sexual health clinic³⁸⁶ might represent such a case whereby their chosen movements afford a data controller into other aspects of a person's private life based on the data collected.³⁸⁷

Furthermore, Article 8, which concerns the verification of the quality of data that are transmitted or made available, needs also be examined. As has been discussed earlier in this review, there exist various identified deficiencies and performance issues in terms of both the accuracy and integrity of location detection and the capture of location data. Questions thus immediately arise as to how inaccurate or incomplete location data may be flagged, or indeed whether any capability to verify the quality of personal location data is employed before they are transmitted or made available.³⁸⁸

6. Qualifying and assessing the risks: the implications for location data use in profiling

Profiling activity has an appreciable impact on both individuals and communities. Earlier discussion has highlighted the positive enabling and empowering role that online interaction can play, particularly as regards the disfavoured, and those that feel impeded or at risk from expressing themselves in more traditional fora.³⁸⁹ Knowledge

³⁸⁶ In Opinion 13/2011 on Geolocation services on smart mobile devices Working Party 29 alluded to the problems that may result from inferences drawn from behavioural patterns, which: "... may also include special categories of data, if it for example reveal visits to hospitals and religious places... These profiles can be used to take decisions that significantly affect the owner." See: WP29, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN WP 185, 16 May 2011, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, p.7

³⁸⁷ Council Framework Decision 2008/977/JHA of 27 November 2008. Article 6 states:

"Processing of special categories of data: The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards." Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Available at:

http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/jl0018_en.htm.

³⁸⁸ Council Framework Decision 2008/977/JHA of 27 November 2008. Article 8 states: "The competent authorities shall take all reasonable steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, the competent authorities shall, as far as practicable, verify the quality of personal data before they are transmitted or made available."

³⁸⁹ See *Redfearn v The United Kingdom*, no. 47335/06 §56, where the European Court of Human Rights affirms the protections afforded by Article 11 of the Convention also pertain to the safeguard of

that interaction and associative behaviour is subject to monitoring can therefore perform a potentially damaging role in allowing individuals to explore and express their identities. Furthermore, one should remain mindful that the disfavoured, especially those whose views and opinions reflect insubstantial minority positions in a pluralist society, are frequently the least empowered in their ability or inclination to protest any such violation of their rights.³⁹⁰ Errors could inhibit free association.

As discussed earlier, new technologies may materialize unconventional forms of associations that are less likely to emerge and be nurtured in other spheres of interaction. In this context it is especially important that we understand how limitations on free association may hinder and restrict a burgeoning milieu in which the exchange of discourse and the imparting of ideas can prove facilitative in a society facing rapid change.

Fundamental rights are indivisible; the nexus of free expression with the freedom to associate and assemble acknowledges this interdependence. In *Vogt v. Germany*, for example, the ECtHR noted: “The protection of personal opinions, secured by Article 10 (art. 10), is one of the objectives of the freedoms of assembly and association as enshrined in Article 11 (art. 11).”³⁹¹ Paradigmatic shifts, brought about by innovations in technology, raise interesting challenges to existing conceptual formulations of rights relating to free association.³⁹² Established distinctions made in delineating the notions of ‘expression’ and ‘association’ may be subject to reevaluation in the light of technological advancement. The synthesis of these two elements could be seen to represent a type of expressive association, reflecting this interrelationship.

associations based on less appealing views or opinions: “the fact remains that Article 11 is applicable not only to persons or associations whose views are favourably received or regarded as inoffensive or as a matter of indifference, but also those whose views offend, shock or disturb.”

³⁹⁰ The value of fora in which groups that represent minority interest can interact was highlighted in an International Civil Liberties Monitoring Group report, which noted that a minority group had experienced “alienation, marginalization and ... a sense of psychological internment.” The value of fora in which groups that represent minority interest can interact was highlighted in an International Civil Liberties Monitoring Group report, which noted that a minority group had experienced “alienation, marginalization and ... a sense of psychological internment.” See International Civil Liberties Monitoring Group, *Anti-Terrorism and the Security Agenda: Impacts on Rights, Freedoms and Democracy*, February 17, p.5, 2004, Available at: http://quakerservice.ca/wp-content/uploads/2011/05/ReportICLMGPublic_Forum.pdf.

³⁹¹ *Vogt v. Germany* (1996) 21 EHRR 205, (17851/91) §64

³⁹² See, for example: J. Ugander, B. Karrer, L. Backstrom, C. Marlow, *The Anatomy of the Facebook Social Graph*, 18 November 2011, Available at: <http://arxiv.org/abs/1111.4503>.

Furthermore, we must consider how emerging associations, such as those that may quickly evolve through online networks, rarely exhibit the orders or hierarchies that previously proved a consideration in scoping an individual or collective right.

It is also necessary to consider the constraint of free expression profiling may impose. In disclosing the existence and constitution of associations, profiling may inhibit interaction. In addition, imprecision in profiling also harbours the potential to mistakenly render an individual an associate of a group or affiliation incorrectly. In this context, in the case of *S. and Marper v. the United Kingdom* the deliberations of the Strasbourg court provide an applicable frame of reference by which to assess the possible conflict that profiling activity of this nature might inhere. The Court held in the *Marper* case that blanket and indiscriminate nature of the power of retention was not proportionate, and did not strike a fair balance in respect of the rights of the individuals concerned.³⁹³ As such, this approach represents a serviceable precedent by which we might measure the probability that extensive and indiscriminate profiling would similarly be judged as a disproportionate interference. The precedent proves instructive where it highlights the extent to which prior technological change has compelled courts to deliberate the adaptation of jurisprudence to novel scenarios. In *S. and Marper v. the United Kingdom* the Court held that:

“Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today.”³⁹⁴

Consequently, the evolution of technology with regard to profiling based upon the processing and analysis of location data unquestionably engages the review of the applicability of preexisting models in relation to changing models of associational behaviour. Existing doctrine however provides us with substantial guidance as to how we may evaluate the permissibility of demands by a public authority to appropriate

³⁹³ *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 119, 4 December 2008

³⁹⁴ *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 71, 4 December 2008.

information on individuals or groups pertaining to patterns of associational and aligned behaviours that risk interference in fundamental rights.³⁹⁵

While the courts have frequently been required to resolve the issues presented by evolving surveillance techniques to date case law has dealt almost exclusively with more conventional notions of membership and association. In *Kopp v. Switzerland* the ECtHR stated with regard to the necessary precision of laws where they pertain to evolving technologies: “Law’s “foreseeability” as to meaning and nature of applicable measures: As interception constituted a serious interference with private life and correspondence, it had to be based on a “law” that was particularly precise, especially as the technology available for use was continually becoming more sophisticated.”³⁹⁶

Importantly, with emergent associations and, with respect to the means by which such groups form, the new capabilities implicit in mobile technologies to assist the formation of new collectives from disparate members do not necessarily represent a replication of the type of activities to which the courts have thus far deliberated and delivered an opinion. The approach demonstrated by the European Court of Human Rights in *Hasan and Chaush v Bulgaria* provides a suitable illustration of this point, where the affirms prior assertions that: “The Court recalls that religious communities traditionally and universally exist in the form of organised structures.”³⁹⁷ The rationale heretofore elucidated thus appears especially inflexible. From the outset, particularly problematic would appear the premise that “religious communities *universally* exist in the form of organised structures”. The statement therefore calls into question how the Court may apply the established precedent where future freedom of thought or conscience-related cases are considered.

The rights of freedom of expression, freedom of religious worship and freedom of association and assembly are interwoven but distinct. These freedoms may cultivate a pluralism that is congenitally sceptical of state orthodoxy. Of course, this is not to

³⁹⁵ See *Amann v. Switzerland* [GC], no. 27798/95, § 46, ECHR 2000-II, where the Court affirms: “Such interference breaches Article 8 unless it is “in accordance with the law”, pursues one or more of the legitimate aims referred to in paragraph 2 and is, in addition, “necessary in a democratic society” to achieve those aims.”

³⁹⁶ *Kopp v. Switzerland*, no. 23224/94 (1998), p.iii.

³⁹⁷ *Hasan and Chaush v Bulgaria*, no 30985/96, 2000 [ECtHR] §62.

immediately suggest that prior precedent proves inflexible, or that existing doctrine be supplanted. Imperative to the assessment of whether the practice of applying predictive analytics to discern the existence of, and nature of, associations between individuals is the notion that an interference resulting from the use of this surveillance technique should fulfill a legitimate aim. Where the process is deployed lacking a specific, identified objective then it may be considered an arbitrary and therefore unlawful imposition on the fundamental rights of those subject to surveillance. A determining factor in this consideration is whether profiling proves efficacious in its implementation, and is proportionate in terms of the impact of the interference.

In *Malone v. the United Kingdom* the ECtHR held that it was incumbent upon the State to ensure that any interference surveillance constitutes is proportionate:

“...Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.”³⁹⁸

Indiscriminate use of profiling for the purposes of substantiating a more general predisposition toward possible future engagement in less serious crimes, or to ascertain more generalized information as regards a propensity for types of association that correlate with statistically significant tendencies or inclinations toward engaging in a broader spectrum of criminal activity, would be unlikely to meet this standard.

³⁹⁸ *Malone v. the United Kingdom*, no. 8691/79 (1984), pp. 32-33, §§ 67-68

Lowering the threshold proves problematic where it is suggestive of an acceptance that extensive and universal surveillance, such as that envisaged by the comprehensive use of social network site monitoring, would be justified. The analysis of citizens' patterns of mobility could foreseeably contribute towards public safety and security with the increasing ubiquity of mobile devices fostering the capability to generate ever more detailed maps of human mobility. Nonetheless, we must still ascertain how we balance its impact and possible interference into communities where we allow for a technology that, if left unchecked, could result in the widespread pre-emptive monitoring of individuals' associations with each other.

The acceptability of a technology employed for the purpose of gathering intelligence must depend on the degree to which it is capable of delineating legitimate and non-legitimate activities; its capacity to differentiate is of foremost concern where an inability to adequately distinguish subjects citizens to a disproportionate risk of infringement of their fundamental rights. Critically, the correlations that the analysis of social network sites may yield are quite unlike the type of associational information that may be extrapolated from data by more conventional means (that previously required human resources to laboriously sieve through data and identify connections).³⁹⁹

Contemporary data mining techniques allow for efficiencies that may produce detailed depictions of structures behind behaviours in a way that differs considerably from prior benchmarks. Furthermore, data mining now furnishes the capability to reveal relationships within associations that even those within the loosely knit structure subject to analysis are themselves likely to be unaware of. This eventuality cuts to the very heart of whether we continue to appreciate and uphold the constitutive values recognition of freedom of association embodies. A method that conspicuously advertises entirely legitimate associations proves to be problematic. As such, the determination of the reasonableness of any profiling must include an evaluation as to whether it reflects a proportionate interference in accordance with the law, and is

³⁹⁹ In this regard it should be noted that the DEMOS report on open source intelligence asserts: "Social media does not fit easily into the policy and legal frameworks that guarantee to the public that intelligence activity in general is proportionate, accountable, and balances various public goods, such as security and the right to privacy." *See*: DEMOS, #Intelligence, 2012, Available at: <http://www.demos.co.uk>, pp. 9-10.

necessary in a democratic society. In this regard the ECtHR reaffirmed the basis for this limitation on the encroachment of the State into fundamental rights, stating:

“Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power.”⁴⁰⁰

In conducting such a review, however, one must remain mindful of retaining a suitably objective standpoint in determining the strain unwarranted monitoring places on citizens’ inclination to freely share their thoughts and explore relationships with other parties. This is particularly the case where it threatens to expose intimate and expressive associations. The risk of chilling these interactions cannot be dismissed as either imperceptible or an acceptable consequence of monitoring.

Notwithstanding these risks, recognition of this encroachment into individuals’ personal lives nonetheless continues to be jeopardized by suggestions that citizens’ simply disregard the value of confidentiality in their associations with each other. In this context, a critical aspect of the challenge to rights protection is therefore the notion that we allow the erosion of our entitlement to secure our personal communications from intrusion without fear that this be construed as reflecting a desire to conceal. Posner makes the assertion that, indeed, this impulse is but a pretext; the real motive being subterfuge:

“What they want, I think, is mainly something quite different from seclusion: they want more power to conceal information about themselves that others might use to their disadvantage.”⁴⁰¹

Whilst it may be said that ‘those with nothing to hide may rest at ease’, we need to reflect on whether we would wish to have to justify each and every action or decision for which we are responsible in everyday life; if we accept this premise we risk instigating a shift in practice that irrefutably sanctions a pervasive and penetrating

⁴⁰⁰ *Malone v. the United Kingdom*, no. 8691/79 (1984), pp. 32-33, §§ 67-68

⁴⁰¹ R.A. Posner, *The Economics of Justice*, Cambridge, Mass., Harvard University Press, 1981, p.271

role for the conduct of ubiquitous surveillance of associations. Individuals may foster associations they wish to conceal simply because they find them to be an embarrassment, or otherwise would rather others didn't know. Evidently, to accept this reality is not just to attest that certain persons have a hidden agenda of which society should genuinely be concerned, justifying a consequential suspicion that would warrant placing their interactions with others under observation. On the contrary, it suggests recognition that each of us must remain unfettered by an obligation to expose, explain or justify our every legitimate association. The notion that profiling of social media data is not intrusive as computers are inanimate is overly simplistic. Calo offers a lucid articulation of the perils of such an approach in noting: "Machines are perfectly competent to comb through private information and use it to make automatic decisions that affect us in tangible and negative ways."⁴⁰²

In effect, whether pattern-based analysis of social network site data proves permissible is partly contingent on the precision of the algorithm employed and its capacity to distinguish between those associations relevant to an investigation and those that are innocuous. Further complicating this issue is that data mining and pattern analysis of location data is still a nascent field of study.⁴⁰³ In addition, another factor requiring consideration is that of the notion of 'hidden associations'; to date, relatively little knowledge has been developed as to how these organizations effectively function in terms of their modes of association. As such, gaining reliable insight from credible analytical research using quantitative analysis is hampered where pertinent data is acutely absent.

Mitigation of this paucity of information cannot simply be achieved by anticipating a more indiscriminate use of these tools in the hope that they will identify a broader range of associations from which one might 'pick' those that appear to warrant further examination. The result would reflect a wholesale and indiscriminate dragnet, which in effect would constitute an expansive and indeterminate search for any association between individuals however innocuous. To accept such an approach would be to

⁴⁰²M. Ryan Calo, *The Drone As Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29 December 12, 2011, Available at: <http://www.stanfordlawreview.org>, p.21

⁴⁰³ See: J. Ugander, B. Karrer, L. Backstrom, C. Marlow, *The Anatomy of the Facebook Social Graph*, 18 November 2011, Available at: <http://arxiv.org/abs/1111.4503>.

agree to subject all online social network site interactions to review: an unfavorable proposition given the level of intrusion it would represent.

The European Code of Police Ethics should in this context be considered in respect of its provision whereby: “Police organisations shall be ready to give objective information on their activities to the public, without disclosing confidential information.”⁴⁰⁴ If pattern-based analysis is to be broadly implemented for the purposes of profiling, its efficacy must be made subject to review: transparency is essential in building public trust.

Similarly, targeted link analysis that exploits the processing of personal location data for the purpose of analysing patterns of mobility and associated interactions based on proximity to other parties to predict future behavioural outcomes should also be approached with great caution. Inferences drawn as to future behaviour of an individual, based on historical associations with other individuals and groups, remains problematic: the accuracy of this approach, based on current scientific, is relatively low.⁴⁰⁵ As link analysis necessitates the review of a distance associations — mining data relating to connections of the second or third order, rather than immediate connections — it therefore represents a considerably more intrusive means of discovery than prior methods which would target more traditional lists and directories pertaining to membership or affiliation.

Significantly, this form of analysis encroaches on the fundamental rights of those individuals who are themselves not directly subject to a specific search for information, but fall within the scope of enquiry simply for having established in some way a distant connection with those that have.

One immediately discernible problem therefore with such broad approaches to determining suspicious activity is their extensive sweep, which constitutes a markedly

⁴⁰⁴ Recommendation Rec(2001)10 of the Committee of Ministers to member states on the European Code of Police Ethics, adopted by the Committee of Ministers 19 September 2001.

⁴⁰⁵ McCue argues that link analysis in profiling activity requires human intelligence to deliver meaningful results: “Link analysis tools can be used to identify relationships in the data... There are some limitations to link analysis; however, domain expertise and a good understanding of the concept behind link analysis can help the analyst interpret the results.” C. McCue, *Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis*, (Oxford: Elsevier), 2007, p.119

disproportionate approach. While the method intends to depict the wider context of a person's associations in relation to one another, it however proves problematic as it unavoidably divulges the attributes of a large volume of innocent associations.⁴⁰⁶ At issue here, then, is the relative proximity of different individuals in relation to one another (and thus the relative strength of the ties of the association). Whereas it may be considered reasonable to conduct an analysis that reveals the nature of those immediately in direct communication with a suspect, revealing the wider networks of association is clearly intrusive in most circumstances and reflects a disproportionate interference.

Any shift toward greater integration of predictive analytics in profiling populations in Europe should only occur where sufficient procedural and operational safeguards are held to adequately protect fundamental rights. In addressing the concerns previously outlined we need reflect as to how we draw distinctions between and, indeed, conceptualize the interdependence of fundamental rights. Recent advances in technology have heralded new capabilities that necessitate our contemplating how we distinguish this interrelationship of fundamental rights including privacy, freedom of association, freedom of thought and conscience, and the prohibition of discrimination. The indivisibility, interdependence and interrelatedness of rights evoke the criticality of our recognizing the intrinsic value of protecting human dignity.⁴⁰⁷

Accepting this principle reflects an appreciation that impeding one right may in turn restrain the enjoyment of another, and hinder the fulfillment of providing the

⁴⁰⁶ Lyon argues that pervasive monitoring of social network sites raises fundamental questions as to social justice: "Ordinary people may feel that they are more vulnerable to intrusion, the use of searchable databases for categorizing and profiling means that deeper questions of power are involved... which means that such surveillance is implicated in basic questions of social justice, to do with access, risk distribution and freedom." *See*: D. Lyon, *Surveillance, Power, and Everyday Life*, Oxford University Press, New York, 2007, p.15

⁴⁰⁷ Regarding the interdependence of rights such as those pertaining to expression and association see, for example, UN Human Rights Committee General Comment 25. Whilst the UN Human Rights Committee General Comment 25 addresses more specifically Article 25 of the ICCPR (relating to the rights of individuals to participate in the public affairs), it nonetheless specifies that freedom of association "is an essential adjunct to the rights protected by article 25."⁴⁰⁷ General Comment 25 also attests to the role of association in facilitating the conduct of public affairs where: "Citizens also take part in the conduct of public affairs by exerting influence through public debate and dialogue with their representatives or through their capacity to organize themselves. This participation is supported by ensuring freedom of expression, assembly and association." *See*: UN Human Rights Committee, General Comment No. 25: The right to participate in public affairs, voting rights and the right of equal access to public service (Art. 25) (1996) at para. 26

conditions under which a person may satisfy their developmental, physical, psychological and spiritual needs. Furthermore, we need also consider the role of participation and inclusion in society, in addition to the principle of equality between individuals — the prohibition of discrimination — as integral to a democratic society, and indeed entirely necessary for its continuing development. Absent this realization there exists a heightened risk by which the conditions for rights infringement may develop.

In this context the difficulties and exceptions the implementation of predictive profiling may present requires our anticipating how existing precedent may guide our formalizing a coherent, lucid response that effectively articulates the parameters which it may be utilised and regulated. Our response therefore necessitates an appreciation as to how the individual rights are framed and distinguished from one another.

Profiling using predictive modeling techniques based on the collation of personal location data risks clearly risk infringement of both an individual's right to privacy. Enabling the enjoyment of this right places an incumbent duty upon states to prevent unlawful or arbitrary interferences with privacy.⁴⁰⁸ Predictive profiling by a public authority would prove especially problematic should it require mass data collection. A crucial distinction requiring further examination is the premise by which public authorities might seek to justify the assertion that the use of 'open source intelligence' obviates the requirement to duly consider the right to respect for private life, including private communications, in relation to the right to establish and develop relationships.⁴⁰⁹

⁴⁰⁸ Article 17 of the ICCPR states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence..." and affirms "Everyone has the right to the protection of the law against such interference or attacks."

⁴⁰⁹ Article 8, European Convention on Human Rights: (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others; Article 7, Charter Of Fundamental Rights Of The European Union: Everyone has the right to respect for his or her private and family life, home and communications.

In *Uzun v. Germany* the ECtHR reiterated its approach toward Article 8 protections in respect of ‘private life’ being such that the term was not susceptible to exhaustive definition, noting:

“Article 8 protects, *inter alia*, a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life”.”⁴¹⁰

According to the Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data “personal data” is defined as any information relating to an identified or identifiable individual: and, of particular note with regard to Article 2 is the stipulation that the definition denotes: “automatic processing” includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.⁴¹¹

Justifying monitoring based on classifying data from openly shared communications through location-based social network sites is problematic. A means of classification proves a questionable where it is based on an inherently nebulous and indefinite concept as ‘open source information’.⁴¹² In *Perry v. The United Kingdom* the ECtHR held that the applicant could not have reasonably expected that he would be subject to surveillance, even in the police station to which he had been brought. The Court stated:

“Whether or not he was aware of the security cameras running in the custody suite, there is no indication that the applicant had any expectation that footage was being taken of him within the police station for use in a video

⁴¹⁰ *Uzun v. Germany* (no. 35623/05, 2 September 2010), § 43, p.11

⁴¹¹ COE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted Strasbourg, 28.1.1981: Article 2 – Definitions - For the purposes of this convention: (c) “automatic processing” includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.

⁴¹² See, for example: DEMOS, #Intelligence, 2012, Available at: <http://www.demos.co.uk>

identification procedure and, potentially, as evidence prejudicial to his defence at trial.”⁴¹³

This principle thus sits awkwardly with the assertion that monitoring by law enforcement officials of ‘public’ internet-based communications would not constitute an interference. The level of intrusion would in part depend upon the intent (i.e. the rationale and purpose) of the analysis of the data; to suggest that it is the type of data alone that will govern the level of intrusiveness is overly reductive. In short, the basis — the reasoning on which a decision is based — for which the action of monitoring is conceived proves indispensable for gauging the level of intrusion. Absent this consideration the result would be to justify a disproportionately intrusive activity by law enforcement, public security or intelligence services based on the premise that another institution used the same ‘open source social media intelligence’.⁴¹⁴ Moreover, a rationale that attempts to categorize and render interpersonal communications as public dialogue, bereft of the privacy protections existing legal provisions furnish, are unsound. Accepting such a shift would be to begin to institute a line of reasoning that undermines a principle of the inviolability of our personal communications absent a sound, compelling justification for the intrusion.

Similarly, implementing analysis of patterns of mobility to monitor and prevent crime based on a blanket and insufficiently selective method likely cannot constitute a proportionate response. Should the surveillance target serious crime that poses a distinct threat to national security or public safety, for example, its implementation still requires that it be achieved in a measured way, incorporating steps to curtail and minimise the impact on human rights where appropriate.

⁴¹³ *Perry v The United Kingdom* (2003) ECHR App. no. 63737/00, § 43, p.10

⁴¹⁴ By way of example, the DEMOS report elaborates a ‘two route solution’ by which the use of social network analysis can be classified as surveillance or ‘non-surveillance’ activity, noting: “We believe this can be achieved through the creation of two routes for government bodies to manage the safe exploitation of social media data. The first route is non-intrusive, open source SOCMINT, which can be conducted on a similar basis to academic institutions and commercial companies, with conditions relating to anonymity and data protection. The second route would be for the state to use specific powers of access intended to result in the identification of individuals, either by personal characteristics or the URLs associated with their social media use. This is ‘SOCMINT as interception and surveillance’.” See: DEMOS, #Intelligence, 2012, Available at: <http://www.demos.co.uk>

The focus of predictive analytics in discerning from frequently disparate and unrelated data possible threats means that our qualifying whether it represents a proportionate response is a particularly difficult task. Further, it proves complicated to articulate whether it is reasonable and necessary in a democratic society to implement an intrusive measure or action that characteristically provides its own rationale only after having established a suspicion i.e. *ex post facto*. An expansion of this principle would perhaps risk allowing for any monitoring activity, should it eventually discern grounds upon which it could be justified (absent any initial foundation). As such, the impact of such a precedent could clearly prove a destabilizing factor in society were this dispensation to be abused.

The potential for monitoring implementing predictive analytics to overreach the prohibition on discrimination is, in certain regards, rather subtle where it may be perceived as constituting a sweeping and inclusive method (and thus be less inclined to exhibit a bias). The nuances and subtleties in the practice of surveillance are constitutive to discriminatory procedures. A particular risk arising in the utilization of predictive analytics is that those persons conducting monitoring fail to appreciate the decision-making processes integral to the surveillance software in question. Thus we need remain mindful of the possibility that discriminatory practices may become embedded and perpetuated within the profiling activity. Crucially, care should be taken to ensure that interpretative modes integral to predictive analytics do not veil questionable practices that foster discriminatory actions. Absent a vigilant approach monitoring activity may in fact exacerbate and further magnify existing inequalities and thereby undermine a central tenet of human rights protection.

The use of predictive analytics using location data to discern and develop future profile-based associations for the purpose of discerning a propensity to be involved in unlawful activity may furnish benefits, but also has evident pitfalls. Greater transparency is needed with regard to the reliability, performance and operation of systems deployed by law enforcement and the intelligence services that integrate predictive analytics in operational decision-making.

It is therefore critical that we understand the implications for society of the adoption of new surveillance technologies. This remains a complex challenge for the courts. As

an example, in *Uzun v. Germany*, the ECtHR provided a simplified and erroneous account of the manner in which satellite-based navigation systems function (in this case the system GPS). The Court made several claims unsupported by scientific fact. The Court asserted:

“GPS is a radio navigation system working with the help of satellites. It allows the continuous location, without lapse of time, of objects equipped with a GPS receiver anywhere on earth, with a maximum tolerance of 50 metres at the time.”⁴¹⁵

In actual fact the system frequently cannot allow for the “continuous location, without lapse of time”, of objects equipped with a GPS receiver.⁴¹⁶ In addition, the specific qualification “without lapse of time” is also questionable.⁴¹⁷ Furthermore, the system cannot currently allow for location of the GPS receiver “anywhere on earth”, nor has this ever been the case: satellite coverage remains insufficient for this to be held to be true, even in the present day. This brief example provides cause for reflection as regards the accuracy of the precedents that may be established where technologies are described in an overly simplistic manner.

Central to this anxiety is the disquiet that this form of surveillance engenders a genuine transformation in the extent to which monitoring of our associations and relations could begin to permeate our society. Pervasive monitoring of this sort could chill association and disrupt social interactions, engendering changes in our behaviour.⁴¹⁸ The intrinsic value of free association in a democratic society is subject to interpretation, where different perceptions place a contrasting emphasis on the value of individual and shared identities. Our identities however are in part relational;

⁴¹⁵ *Uzun v. Germany* (no. 35623/05, 2 September 2010), § 13, p.3

⁴¹⁶ To achieve this the receiver must locate 4 satellites, which is frequently not achievable even within Europe (depending upon the location and time of day). Also, even where this can be achieved, it may only be achieved with an initial time delay (during which period locational data will not be available).

⁴¹⁷ The signals are delayed; the algorithms used may only approximate this time delay. The algorithms may indeed provide a close fit, but not necessarily the exact indication of a location in all instances.

⁴¹⁸ In *Uzun v. Germany* the applicant complained that a less intrusive form of surveillance (GPS-based location-based monitoring) constituted a form of observation that reflected “his total surveillance”. A parallel may be drawn with the pervasiveness of the surveillance capability inherent to social network analysis may represent. See: *Uzun v. Germany* (no. 35623/05, 2 September 2010), § 41, p.10

meaning that they are shaped by social interactions and, crucially, by way of both the consciousness of ourselves, and our sentience toward others' observation.

7. Conclusions

As the analysis in this chapter has evidenced, new profiling technologies can be implemented inconspicuously, such that we may be entirely unaware of the knowledge generated automatically within the profiles created. Moreover, citizens subject to profiling may be altogether oblivious of the benefits and risks engendered by the creation of profiles based on personal location data. With location data being generated in greater quantities, based upon the proliferation of devices that inhere the capability to track our individual movements, this profusion of data that may be correlated with other personal data allows for a paradigmatic shift in terms of the construction of personalized knowledge. Data analysis always presumes subjectivity; by their very nature algorithms are reductive and formulated on a selective basis vis-à-vis distinct perspectives and beliefs.⁴¹⁹ As Sunstein has remarked too, the social meanings of actions are very much a function of existing social norms.⁴²⁰ Part of the difficulty, then, in creating profiles stems from our comprehension of how perpetual shifts in norms may in turn institute a reflexive transformation in the significance of our own actions. Sui and Goodchild have underscored a further paradox, that of self-referentiality, which is especially pertinent to our discussion here of profiling; the scholars noting: “The tools and technologies we deploy to study society have increasingly become part of the society we try to study using those same tools. This technological self-referentiality... will inevitably make it impossible to provide technical solutions to social problems.”⁴²¹ Ideally, prototypes, such as have been suggested by Kahneman and Tversky, would be available to model representative examples of harms in order that individuals could make complex judgments prior to

⁴¹⁹ Indeed, Bowler and Star concur in noting that: “Values, opinions and rhetoric are frozen into code.” See: Bowker, G. and Leigh-Star, S. (1999) *Sorting Things Out*, Cambridge, MA.:MIT Press, p.35

⁴²⁰ Sunstein C. R., On the Expressive Function of Law, *University of Pennsylvania Law Review* 144:5 (1996) Available at: <http://scholarship.law.upenn.edu>, p.2022

⁴²¹ See: Sui, D.Z. and Goodchild, M.F., 2003. A tetradic analysis of GIS and society using McLuhan's law of the media. *The Canadian Geographer/Le Géographe canadien*, 47(1), p.14

the initiation of specific data processing practices.⁴²²

If abused, profiling based on monitoring mobility through location data collection and processing may precipitate a form of social control whereby influence is improperly exerted over individuals, with populations subject to segmentation based on the perceived threat its constituent associations may pose to public security.⁴²³ A further fundamental concern is whether the processing of personal location data in predictive systems could reinforce discriminatory practices by public authorities. For example, records of incidents of anti-social behaviour may over-represent particular neighbourhoods or groups; a greater reliance on collecting and processing location data coupled with an increased reliance on predictive systems could result in the perpetuation and amplification of pre-existing biases.⁴²⁴ The potential therefore exists for interferences in individuals' rights where predictions suggest their future actions will correlate with the skewed results that originate from a biased sampling. Moreover, the subsequent effect in terms of the harm effected individuals may be further exacerbated by decisions that limit contact and associations, further prejudicing analysis and denying persons future life opportunities based on unsound generalisations.⁴²⁵

Profiling using predictive techniques may irrevocably disrupt the pathways of serendipity that foster individual experimentation and innovation; whilst this may result in more linear, orderly imperatives being achieved, a more harmonised society may not necessarily engender a greater degree of understanding, or indeed better advance political and intellectual wellbeing. The processing of personal location data by public authorities could allow for the monitoring of deviations in patterns of

⁴²² See: Cass R. Sunstein, John M. Olin Law & Economics Working Paper No. 165 (2D Series), Public Law And Legal Theory Working Paper No. 33, Hazardous Heuristics, Available at: <http://www.law.uchicago.edu/Lawecon/index.html>, p.14

⁴²³ Rosen argues that pervasive monitoring, such as is constituted by widespread use of social network site analysis by law enforcement, threatens the values of equality in ways that could transform the relationship between citizens and their government. See: J. Rosen, *The Naked Crowd: Reclaiming Security And Freedom In An Anxious Age*, 2003, Available at: <http://www.law.fsu.edu/faculty/2003-2004workshops/rosen.pdf>, p.27

⁴²⁴ See: OpenDemocracy, Chris Jones, Predictive policing: mapping the future of policing? June 10 2014, Available at: <https://www.opendemocracy.net/opensecurity/chris-jones/predictive-policing-mapping-future-of-policing>

⁴²⁵ For further discussion of the accumulative effect of the compounding of statistically biased samples, see: Barocas, Solon and Selbst, Andrew D., *Big Data's Disparate Impact* (2016). 104 *California Law Review* 671 (2016). Available at: <https://ssrn.com/abstract=2477899>, pp.12-16

mobility and behaviours, such that authorities could in future abuse this capability in strengthening civic and political power by harassing minorities and stigmatizing unwanted behaviours.

Concerns have been voiced as to the long-term repercussions that may flow from the reliance of an ever-greater number of applications on the use of location data for predictive purposes. Further research into the impact of the existing uncertainties as regards data quality is critically important.⁴²⁶ Deployment of this evolving technology requires therefore a coherent and unambiguous vision. The next chapter will examine how this roll out is already evolving, by way of the integration of the Internet of Things (IoT) into established sensing networks.

⁴²⁶ Indeed, the NCHRP has commented in detail as to the level of uncertainty present in the spatial attributes of location data, stating: “Any measures of uncertainty must consider that uncertainty varies through space and time and is context sensitive. This has important implications for modeling. For example, users in a rapid decision-making environment may not have the time or interest to request a view of each of the individual measures of uncertainty. Important measurement issues thus relate to aggregating individual measures of uncertainty.” *See*: NCHRP, *Quality and Accuracy of Positional Data in Transportation*, 2003, Available at: http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_506.pdf, p.14

Chapter 5: The Internet of Things: A Paradigmatic Shift for the Significance of Location Data

1. Introduction

The miniaturization of embedded location sensing technologies, added to a greater precision in data collection, is creating the possibility of greater participation in a more connected, networked society for citizens; this phenomenon heralds fresh challenges for the protection of privacy and personal data.⁴²⁷ This concern is not entirely unfamiliar, for successive generations of information technology applications have created certain disquiet amongst citizens in respect of their personal data being subject to more extensive processing.⁴²⁸

As a relatively new paradigm of the Internet's development, research on the Internet of Things is still at an early stage.⁴²⁹ The concept of the 'Internet of Things' (IoT) appears at first glance somewhat indistinct and indeterminate, however, IoT is on the threshold of integration into the everyday lives of citizens in Europe and, as shall be

⁴²⁷ Negroponte has advanced his conviction that the information society renders each generation progressively 'more digital' than its predecessor. *See*: Negroponte, N., *Being Digital*, New York: Alfred A. Knopf, 1995, p.231

⁴²⁸ Moreover, in a 2012 impact assessment conducted in conjunction with a review of the Directive 95/46/EC, the Commission indeed highlighted the heightening of the risk posed by the insufficient awareness, and loss of control and trust of citizens: "it is increasingly difficult for individuals to be aware of the processing of the data related to them and the risks linked to such processing, to maintain control over their own data and, ultimately, to assert their rights *vis-à-vis* data controllers." *See*: EU Commission, COMMISSION STAFF WORKING PAPER - Impact Assessment, General Data Protection Regulation and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC (2012) 72 final, Available at: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf. *See, also*: Joint Research Centre of the Commission and the Institute for Prospective Technological Studies, *Future bottlenecks in the information society*, June 2001, Available at: http://ec.europa.eu/justice/data-protection/document/studies/files/200106_ipts_itre_en.pdf, p.93; *See, also*: EU Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4 November 2010, Available at: <http://eur-lex.europa.eu/LexUriServ>, pp2-3.

⁴²⁹ *See, for example*: Shen Bin, Liu Yuan & Wang Xiaoyi, *Research on Data Mining Models for the Internet of Things*, IEEE 2010 International Conference on Image Analysis and Signal Processing, Available at: <http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5469149>

illustrated in the ensuing discussion, this fundamentally transformative process by which monitoring and communications achieves and even greater ubiquity and pervasiveness in our society inheres significant new challenges to data protection and privacy as regards the collection and processing of location data.⁴³⁰ In simple terms the ‘Internet of Things’ refers to the ability of everyday objects to connect to the Internet and to send and receive data.⁴³¹ For purposes of this review, the term IoT is used to refer to ‘things’ such as devices or sensors (excluding computers or cellular phones) that connect, communicate or transmit information with or between each other via the Internet. The concept of IoT is pivotal to the further development of the use of location data.⁴³² With IoT to become omnipresent, its scope of influence will extend so as to influence the exercise of every citizen’s fundamental rights.⁴³³ The evolving technologies associated with IoT portend the collection and processing of personal data in many different spaces, at any time and in many different forms, including a diverse range of personal location data. Furthermore, the increasing portability of devices heralds an era where information as to the geographical location

⁴³⁰ The WP29 has qualified the necessity of examining the role of “smart things” being developed so that, beyond legal and technical compliance, the consequences for society at large, and in terms of the protection of fundamental rights specifically, may be appraised. Indeed, the WP29 has stated that whilst the deployment of devices requires the uniform application of the legal data protection framework, the nature of the societal challenges this task presents are such that to ensure the necessary level of compliance considerable attention needs be given the identification and analysis of critical new data protection risks that lie within the ecosystem of IoT. The significance of which, in terms of the application of the existing legal framework, has been confirmed by the WP29 whereby in its opinion on IoT it underscored the gravity of the risk of unlawful surveillance, highlighting that it constituted a pronounced risk in respect of the products and services these technologies offer. As such, it forewarned that in this context compliance with the existing legal framework is “key to meeting the legal, technical but also, since it relies on the qualification of data protection as a fundamental human right, the societal challenges described”. *See*: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.3

⁴³¹ Federal Trade Commission, Internet of Things - Privacy & Security in a Connected World, FTC Staff Report, January 2015, Available at: <http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>, p.i.

⁴³² The CASAGRAS Project defined the Internet of Things as: “a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and involving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.” *See*: EU Commission, Factsheet on privacy, data protection and information security, March 2013, Available at: http://ec.europa.eu/information_society/newsroom, p.1

⁴³³ Evans notes in this context that IoT represents the “next evolution of the internet, taking a huge leap in its ability to gather, analyze, and distribute data that we can turn into information, knowledge, and, ultimately, wisdom.” *See*: Dave Evans, Cisco Internet Business Solutions Group, The Internet Of Things: How The Next Evolution Of The Internet Is Changing Everything, (2011), Available at: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, p.2.

of individuals can be obtained in real time by a multiplicity of different methods.⁴³⁴ One of the key challenges in convincing citizens to adopt emerging IoT technologies is the protection of their fundamental rights, particularly those pertaining to the protection of personal data and privacy.⁴³⁵ From the very outset of the development of IoT, concerns regarding privacy and data protection have been widespread, particularly as embedded sensors may be discreetly hidden, enabling the tracking of the individual's movements, behavioural habits and ongoing preferences and characteristics.⁴³⁶

2. The challenges of IoT to personal data protection principles

The implementation of IoT raises questions as to how long-standing concepts of data protection relating to basic precepts such as prior notice, choice, access, accuracy, data minimization, security and accountability should be applied as IoT technologies are developed.⁴³⁷ In this context we thus need consider the specific challenges that arise in connection with the collection and processing of location data and the application of the existing regulatory framework. The ECtHR case of *Uzun v. Germany*⁴³⁸ provides relevant guidance in our consideration of the effect of monitoring on the citizen in its review of the use of surveillance using a tracking device. The Court affirmed that the monitoring of movement, and the subsequent

⁴³⁴ For example, by using geospatial navigation data (such as GPS), WLAN network broadcast data, and through the mapping of communication network antenna information.

⁴³⁵ Whilst the International Telecommunication Union (ITU) employs the term “user” in its discussion of IoT “challenges and concerns”, which it determines include “concepts of data request and data consent risk becoming outdated”, it would appear questionable whether user is the appropriate term to employ in this context. The ITU states: “Invisible and constant data exchange between things and people, and between things and other things, will occur unknown to the owners and originators of such data.” This infers a person consciously availing themselves of something, or is operating or utilizing it; thus the term “user” would appear to inhere a degree of intent or purpose on the part of the individual concerned, as opposed to unconscious or unwitting utilization, which is more appropriate in the circumstances the ITU describes. *See*: ITU, *The Internet of Things - Executive Summary*, November 2005, Available at: www.itu.int/osg/spu/publications, p.8.

⁴³⁶ Auby asserts too that the development of mapping and mobility support tools could provide public authorities with indications as to the everyday habits of citizens and the places they frequent. *See*: Auby J.B., *Smart Cities And Private Lives: The Impossible Union?* 20th October 2016, FT.com, Available at: http://capgemini.ft.com/trend-checking/smart-cities-and-private-lives-the-impossible-union-_f-89.html?

⁴³⁷ *See*: Federal Trade Commission, *Internet of Things - Privacy & Security in a Connected World*, FTC Staff Report, January 2015, Available at: <http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>, pp. ii-vii.

⁴³⁸ *Uzun v. Germany* (no. 35623/05, 2 September 2010)

processing of the data obtained thereby, amounts to interference in one's private life protected by Article 8 of the Convention. In particular, the judgment highlighted the specific capabilities of the monitoring technology with regard to its capacity to log movement patterns, noting that the surveillance:

“... Systematically collected and stored data determining, in the circumstances, the applicant's whereabouts and movements in the public sphere. They further recorded the personal data and used it in order to draw up a pattern of the applicant's movements, to make further investigations and to collect additional evidence at the places the applicant had travelled to...”⁴³⁹

This is an especially pertinent topic as the utility of the IoT devices being developed is largely dependent upon the increasing precision, augmentation and diversification of localisation services.⁴⁴⁰ Localisation services depend upon location data and capitalize on the premise that information relating to the individual is more relevant, and hence more valuable, where it is linked to their location.⁴⁴¹ As such, location awareness is integral to the effectiveness of networked devices and services.⁴⁴²

⁴³⁹ *Uzun v. Germany* (no. 35623/05, 2 September 2010), at §51

⁴⁴⁰ The IoT environment is characterised by the pervasiveness of sensors that collect a multitude of personal data types of individuals as they move through (IoT) environments; as noted in a EU Commission review on the implications for personal data protection and privacy: “IoT systems might therefore reveal information on individuals, their habits, *location*, interests and other personal information and other preferences stored for ease of use in systems.” See: EU Commission, Factsheet on privacy, data protection and information security, March 2013, Available at: http://ec.europa.eu/information_society/newsroom, p.3. Note: *emphasis added*

⁴⁴¹ See: Joint Research Centre of the Commission and the Institute for Prospective Technological Studies, Future bottlenecks in the information society, June 2001, Available at: http://ec.europa.eu/justice/data-protection/document/studies/files/200106_ipts_itre_en.pdf, p. 104

⁴⁴² Indeed, the significance of the issue of location data and the subsequent triggers applied by the provisions of the EU legal instruments which confer the obligations incumbent upon data controllers and data processors to protect individuals' privacy and right to data protection was highlighted very early on in the development of mobile communications networks. In this context it should be noted that the Commission identified that mobile phones constituted terminal equipment for which additional measures might be required in such situations where processing specific information would require certain supplementary safeguards. Furthermore, the Commission also noted that individual consent was imperative where the processing of location data was concerned. That these two specific points should have been raised in respect of the development of the use of mobile phones reflects the acknowledgement at an early stage of the technology's development that the possible risks inherent to the collection and processing of location data were immediately perceptible. See: EU Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4 November 2010 Available at: <http://eur-lex.europa.eu/LexUriServ>, p.5

It is vital therefore to conduct a detailed examination of the implications of IoT to the collection and processing of location data, and to our understanding of the evolving challenges novel location-aware applications and services increasingly exhibit. An initial concern is how best to apply safeguards where existing formulations that delineate the scope and the nature of privacy protections prove challenging to apply; emerging technology developments frequently elude straightforward classification. In turn, advances in information technology question how we draw distinctions between the self, our location and our immediate environment; the tenability of conceptual and contextual assumptions that relate to the temporal and spatial parameters of privacy are in consequence also placed under examination.⁴⁴³ In the context of ‘private life’, the European Court of Human Rights has recalled that the notion is a broad one, which is not susceptible to exhaustive definition.⁴⁴⁴ Furthermore, of relevance too within this context is the ECtHR having asserted that: “Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities.”⁴⁴⁵

In *P.G. and J.H. v. United Kingdom* the ECtHR further affirmed:

“There are a number of elements relevant to a consideration of whether a person’s private life is concerned in measures effected outside a person’s home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities, which are or may be recorded or reported in a public manner, a person’s reasonable expectations as to privacy may be a significant, though not necessarily conclusive factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same

⁴⁴³ Many different ways of defining privacy in relation to the physical environment and the individual sphere have been attempted. The concern of identifying possible overlapping spheres of privacy as they relate to the individual has presented scholars with the prospect of elucidating how aspects of a person’s privacy interrelate, and how we conceptualize the notion of privacy as it relates to the physical body and the surrounding environment. Seeking to distinguish the different realms that engage privacy, Rosenberg determines that it may be distinguished in respect of three distinct spheres, whereby geographic privacy constitutes the protection of the immediate sphere surrounding the person; privacy of the person refers to the respect and the protection of the individual’s mind and body, whilst informational privacy concerns the control of what personal data can be gathered, stored, processed or selectively disseminated, and how this should be achieved. *See*: Rosenberg, Richard. *The Social Impact of Computing*, Ch. 9: Privacy and Freedom of Information), Academic Press, Boston, MA., 1992.

⁴⁴⁴ *Niemietz v. Germany* (16 December 1992, Series A no. 251-B) §29

⁴⁴⁵ *Rotaru v Romania* (App No 28341/95), §43

public scene (e.g. a security guard viewing through close circuit television) is of a similar character. Private life considerations may arise however once any systematic or permanent record comes into existence of such material from the public domain.”⁴⁴⁶

Of further note in our review of the interference in the right to privacy the systematic monitoring of the location of an individual may constitute, the Court noted in the *Uzun* case with regard to the severity of the interference:

“In the Court’s view, GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings.”⁴⁴⁷

Noteworthy, then, in the citation above from the *Uzun* ruling is the applicability of the precedent it establishes with respect to the susceptibility of systematic positioning of a person to yield more detailed information on a person’s conduct, opinions or feelings than might have been conceived by the Court. Here, the principal point of contention with the ruling thus pertains to the assertion that other methods of, in particular, visual surveillance, might disclose more information *as a rule*. Furthermore, the ECtHR’s *Uzun* judgment provides guidance in respect of concerns pertaining to the time period over which monitoring is applied. The pervasiveness of sensing devices, their utility and frequency of engagement in use are necessary considerations.

Monitoring activity, whether overt or covert, must meet the Strasbourg court’s tests pursuant to the reasonableness of interferences allowed for under Article 8(2), whereby it noted surveillance was “tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.”⁴⁴⁸

⁴⁴⁶ *P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 57.

⁴⁴⁷ *Uzun v. Germany* (no. 35623/05, 2 September 2010), at §52

⁴⁴⁸ *Klass and Others v. Germany*, 6 September 1978, § 42, Series A no. 28

2.1 A focus on personal devices and the ‘quantified self’

IoT technologies continue to expand as convergence and synergies with other technology developments allow for data to be collected and processed in new ways, however, the review here necessarily focuses on recent innovations that constitute a direct continuation of the development of personal mobile devices and an extension of personal location data collection and processing.⁴⁴⁹ This assessment therefore retains as its principal consideration technical developments in two distinct, though related spheres; ‘wearable computing’ and the use of devices that enable the ‘quantified self’.⁴⁵⁰ These two areas of interest reflect a continuation of the evolution in technical capacities that allow discrete measurements through data collection and processing that may relate to intimate aspects of an individual’s personal life.⁴⁵¹ The ‘quantified self’ is a concept of self-monitoring and represents a development of particular interest in that evidence is emerging that in a diverse range of contexts individuals are increasingly being encouraged or coerced to share personal data collected by digital devices.⁴⁵² Concerns have thus arisen as to the implications of a broader exploitation

⁴⁴⁹ The approach thus excludes from its review a broader evaluation of more extensive applications and issues associated with the implementation that relate to developments such as, for example, networked transportation and ‘smart cities’. Whilst indeed the progression of these infrastructure-based developments is important for the wider execution and fulfillment of the capabilities of IoT as a whole, an exhaustive review of each discrete technology would prove burdensome.

⁴⁵⁰ The term ‘quantified self’ is frequently used to describe the activity of self-tracking and constitutes a development of long established concepts in information technology of personal analytics and self-informatics. Quantified self devices report quantitative indicators relating to a person’s physical activities and commonly collect and process location data. Lupton asserts that the personal data captured by the use of such devices thus constitutes a novel form of self-monitoring whereby the individual engages in a process constituting a dynamic and persistent ‘reflexive surveillance’ of their own behaviour. *See, for example:* Lupton, Deborah, *Self-Tracking Modes: Reflexive Self-Monitoring and Data Practices* (August 19, 2014). Available at: <http://ssrn.com/abstract=2483549> or <http://dx.doi.org/10.2139/ssrn.2483549>; Lupton, Deborah, *You Are Your Data: Self-Tracking Practices and Concepts of Data* (December 4, 2014). *Lifelogging: Theoretical Approaches and Case Studies about Self-tracking*, edited by Stefan Selke, Springer, Forthcoming. Available at: <http://ssrn.com/abstract=2534211>

⁴⁵¹ Dodge and Kitchin underscore the potentiality of wearable devices gathering location data and other personal data to challenge established data minimization practices, noting: “As such, the present ability to capture and store vast amounts of information is inspiring a vision of pervasive computing that generates ubiquitous information of the present, that is kept to become a continuous record of the past.” Martin Dodge & Rob Kitchin, *CASA Working Paper 92, The ethics of forgetting in an age of pervasive computing*, 1 March 2005, Available at: <http://www.bartlett.ucl.ac.uk/casa/publications/working-paper-92>, p.3. *See, also:* Nafus D., Sherman J., *This One Does Not Go Up to 11: The Quantified Self Movement as an Alternative Big Data Practice*, *International Journal of Communication* 8 (2014), Available at: <http://ijoc.org/index.php/ijoc/article/viewFile/2170/1157>, pp. 1784–1785

⁴⁵² Lupton, Deborah, *You Are Your Data: Self-Tracking Practices and Concepts of Data* (December 4, 2014). *Lifelogging: Theoretical Approaches and Case Studies about Self-tracking*, edited by Stefan Selke, Springer, Forthcoming. Available at: <http://ssrn.com/abstract=2534211>, pp.5-8

of this personal data by both public and private actors, and how effective oversight of data collection and processing might evolve.⁴⁵³ Wearable Computing refers to objects and clothes worn that incorporate embedded sensors.⁴⁵⁴ The prevalence of wearable computing devices shall likely expand rapidly, with the technology extending the utility of ordinary objects.⁴⁵⁵ Access to data collected by wearable devices is supported by the availability of applications created by developers, which may in turn significantly broaden the scope of data processing activities.

3. Determining personal from non-personal data: IoT and location data

With the increasing prevalence of IoT devices it can be difficult to determine how personal data is distinguished from non-personal data.⁴⁵⁶ Applying the existing legal framework for personal data protection to IoT presents challenges where one necessarily distinguishes between personal and non-personal data. Information that identifies, or is reasonably likely to identify an individual (either directly or indirectly) should be differentiated from information that does not. It has been established that data collected and processed by personal devices such as cellular

⁴⁵³ Certain wearable fitness devices incorporate sensors that sense types of motion whilst collecting location data, allowing for the detection of different types of physical activity and the possibility of detecting and diagnosing health-related injuries and conditions. *See*: Peppet S. R., *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, Vol. 93 *Texas Law Rev.* 85, Available at: <http://www.texasrev.com/wp-content/uploads/Peppet-93-1.pdf>, p.102

⁴⁵⁴ Raji et al note the broad nature of personal information pertaining to an individual that can be inferred from personal data collected: “Networked body-worn sensors and those embedded in mobile devices we carry can collect a variety of measurements about physical and physiological states, such as acceleration... By applying sophisticated machine learning algorithms on these data, rich inferences can be made about the physiological, psychological, and behavioral states and activities of people.” *See*: A. Raji et al., *Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment*, in *CHI 2011: Proceedings Of The Sigchi Conference On Human Factors In Computing Systems* 11, 11 (2011), Available at: <http://pie.eng.usf.edu/wp-content/uploads/2011/12/raji-chi2011.pdf>, p.1

⁴⁵⁵ ‘Wearables’ may include cameras, microphones and sensors that can collect and process data through access to networked services. *See*: WP29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.5. *See also*: Clarke, Roger, *The Regulation of Point of View Surveillance: A Review of Australian Law* (August 17, 2012). *UNSW Law Research Paper No. 2012-37*. Available at: <http://ssrn.com/abstract=2134878>, p.2; Mann S. (1996) 'Smart Clothing: The Shift to Wearable Computing' *Communications of the ACM* 39, 8 (August 1996) pp. 23-24, Available at: http://www.eyetap.org/papers/docs/acm_comm96.pdf

⁴⁵⁶ *See*: EU Commission, *Factsheet on privacy, data protection and information security*, March 2013, Available at: http://ec.europa.eu/information_society/newsroom, p.2

phones, for example, falls within this scope.⁴⁵⁷ Thus location data pertaining to the locality and trajectory of a device's movements would also constitute personal data in respect of the user.⁴⁵⁸ In the ECtHR's review as to the admissibility of *Weber and Saravia v. Germany*⁴⁵⁹ the Court's judgment further reinforces the notion that, should a public authority process an identifiable person's location data, this would constitute an interference in the right to privacy, noting it:

“...Takes the view that the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Article 8.”⁴⁶⁰

However, the application of the existing legal framework of data protection with regard to an individual's devices which may be deemed 'less personal' than that with which we are currently familiar (contrasting a tablet computing device with, for example, a fitness monitor that records a user's (or, indeed, several users) journeys and exercise activity on a bicycle. In the latter case, it remains open to debate whether the datasets from the device constitute personal data concerning the device's multiple users.⁴⁶¹

⁴⁵⁷ The WP29 notes with respect to personal cellular phones, for example, that: “It seldom happens that a person lends such a device to another person.” See: WP29, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN WP 185, 16 May 2011, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, p.7

⁴⁵⁸ See: WP29, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN WP 185, 16 May 2011, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, p.7

⁴⁵⁹ *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI

⁴⁶⁰ *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI

⁴⁶¹ The United Kingdom's Information Commissioner's Office (ICO) notes that is increasingly evident that the functionality of the applications of certain devices constituting IoT could collect and process personal data such that the processing might prove intrusive to an individual's privacy. Interestingly, of particular note, and in fact of some concern, in the initial guidance provided by the ICO is the lack of distinction drawn between devices and applications: distinguishing between the two is vital where recommendations by a data protection agency are intended to furnish clear and concise guidelines as regards addressing data protection issues. See: ICO, The Information Commissioner's response to Ofcom's consultation 'Promoting investment and innovation in the Internet of Things, October 1st 2014, Available at: <https://ico.org.uk/media/about-the-ico/consultation-responses/2014/2512/ico-response-to-ofcom-consultation-on-internet-of-things-20141001.pdf>

Furthermore, this issue is rendered more complex where there exists a potential mismatch in terms of what a user understands as to the device's capabilities (particularly in respect of the rather nebulous and intangible aspects of its sensing capacities combined with data processing and, possibly, networking ability that necessarily inheres an ability to share personal data with other entities) and how it behaves in practice.⁴⁶² Especially significant in this regard are emerging technologies that allow for increasingly precise sensing of mobility allowing for the monitoring of an individual's health.⁴⁶³ Absent sufficient efforts to inform users, an appreciable risk exists that individuals using such devices may be insufficiently informed as to how data from such devices is collected and processed.⁴⁶⁴ Indeed, data protection authorities have highlighted particular concerns in respect of the risks of divergence, and of the profusion of different data controllers now collecting and processing personal data; such developments raise the threshold for the assurance of adequate safeguards to personal data.⁴⁶⁵

Differentiation between types of location data, and whether such data constitutes 'personal data' is rendered more complex where one determines the primary concept

⁴⁶² See: ICO, The Information Commissioner's response to Ofcom's consultation 'Promoting investment and innovation in the Internet of Things', October 1st 2014, Available at: <https://ico.org.uk/media/about-the-ico/consultation-responses/2014/2512/ico-response-to-ofcom-consultation-on-internet-of-things-20141001.pdf>

⁴⁶³ The FTC refers to the risked involved in the direct collection of "sensitive" personal data in referring to "precise geolocation" data, which it affirms allows for inferences to be drawn in respect of an individual's "habits, locations, and physical conditions over time"; See: Federal Trade Commission, Internet of Things - Privacy & Security in a Connected World, FTC Staff Report, January 2015, Available at: <http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>, p.14 See, also: FTC, Consumer Generated and Controlled Health Data, 7 May 2014, Available at: http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

⁴⁶⁴ Moreover, recent research has shown that movement data collected by inertial sensors (for example, gyroscopes and accelerometers embedded within IoT devices) may be processed for evaluating aspects of personal health related to mobility, such as an individual's gait or physical activity. The same data may also reveal sensitive medical conditions such as seizures that the individual concerned may wish to keep private. See: A. Rajj et al., Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment, in CHI 2011: Proceedings Of The Sigchi Conference On Human Factors In Computing Systems 11, 11 (2011), Available at: <http://pie.eng.usf.edu/wp-content/uploads/2011/12/raij-chi2011.pdf>, p.1; See also: K. Lorincz, B. Chen, G. Challen, A. Chowdhury, S. Patel, P. Bonato, and M. Welsh. Mercury: A Wearable Sensor Network Platform for High-Fidelity Motion Analysis. In ACM SenSys, 2009. Available at: <http://www.eecs.harvard.edu/~mdw/papers/mercury-sensys09.pdf>

⁴⁶⁵ See, for example: ICO, The Information Commissioner's response to Ofcom's consultation paper 'Promoting investment and innovation in the Internet of Things', October 1st 2014, Available at: <https://ico.org.uk/media/about-the-ico/consultation-responses/2014/2512/ico-response-to-ofcom-consultation-on-internet-of-things-20141001.pdf>

of *agency* in respect of how data is collected.⁴⁶⁶ In the context of surveillance, long-established criteria for establishing distinctions between the monitoring of persons (both in terms of individuals and groups) versus physical objects are now subject to review where even the term ‘device’ in itself is open to question.⁴⁶⁷ Whether data is ‘personal data’, and how one establishes whether any associated location data collected or processed falls within the remit of existing data protection legislation is potentially subject to a significant paradigmatic shift.⁴⁶⁸

In the past, a connected device capable of gathering location data might reasonably have been assumed to be a relatively discreet, personal piece of equipment associated with a specific individual (an obvious example being a mobile cellular phone); an assumption that devices with embedded sensors challenge in allowing location tracking of the data subject. Relevant too in this context is the Strasbourg Court’s linkage of timespan in relation to proportionality, underscored in *Uzun* in the assertion of the requirement that: “The duration of a measure of surveillance via GPS also had to be proportionate.”⁴⁶⁹ Research has shown that much shorter timespans of mobility monitoring of citizens is capable of rendering an extremely detailed and nuanced representation of a person’s private life.⁴⁷⁰

⁴⁶⁶ Meints notes in this respect that not only is the accuracy of data questionable in many cases, but also that “the accuracy of linkage to a specific individual in the case of personal profiling. This can be a severe problem if a personal profile is created on basis of data which is only thought to belong to the specific person, but in fact belongs to others.” Thus a profile that is assigned to a specific person may constitute a hybrid or, indeed, even be entirely constructed from another individual’s data. *See*: FIDIS - Future of Identity in the Information Society, “D7.4: Implications of profiling practices on democracy and rule of law”, 5 September 2005, Available at: <http://www.fidis.net/resources/fidis-deliverables/profiling>, p.49

⁴⁶⁷ Gleeson M., ICO raises awareness of the privacy implications of the Internet of Things, 1st September 2014, Available at: <http://www.lexology.com/library/detail.aspx?g=99ea0f7c-5c18-4f2f-b98f-9f650f33fc40>. *See also*: Andrew Patterson, The Internet of Things: what is it and what does it mean for you?, 21 August 2014, Available at: <https://iconewsblog.wordpress.com/2014/08/21>.

⁴⁶⁸ Dodge and Kitchin have noted the potential for ‘life-logs’ to provide a record that includes every action and material expression of a data subject’s life, including therefore a highly nuanced record of location data pertaining to a person’s daily movements, stating: “A life-log is conceived as a form of pervasive computing consisting of a unified, digital record of the totality of an individual’s experiences... Such a life-log will constitute a new, pervasive socio-spatial archive as inherent in its construction will be a locational record; it will detail everywhere an individual has been.” *See*: Martin Dodge, Rob Kitchin, CASA Working Paper 92, The ethics of forgetting in an age of pervasive computing, 1 March 2005, Available at: <http://www.bartlett.ucl.ac.uk/casa/publications/working-paper-92>, p.2

⁴⁶⁹ *Uzun v. Germany* (no. 35623/05, 2 September 2010), at §59

⁴⁷⁰ *See*: Louail, Thomas, et al. “From mobile phone data to the spatial structure of cities.” *Nature, Scientific reports* 4 (2014); Gonzalez, M. C., Hidalgo, C. A., & Barabasi, A. L. (2008). Understanding individual human mobility patterns. *Nature*, 453(7196), 779-782; Louail, Thomas, et al. “Uncovering the spatial structure of mobility networks.” *Nature Communications* 6 (2015).

Indiscriminate use of location monitoring absent any specific prior suspicion would likely constitute a reasonably serious interference in the right to privacy.⁴⁷¹ The ECtHR case law has affirmed that the notion of being “necessary in a democratic society” in respect of a surveillance activity must be considered to infer that the interference corresponds to a pressing social need and is proportionate to the legitimate aim pursued.⁴⁷² Thus, in assessing proportionality one must also consider whether other, comparatively less intrusive, methods of investigation could prove to sufficiently effective while constituting a lesser interference in the fundamental rights of the individual.

With regard specifically to the *Uzun* case, the GPS receiver in question was attached to a car: whilst the judgment speaks of “... the grounds required for ordering a person’s surveillance via GPS...” care is therefore needed in drawing direct analogies between the possible monitoring capabilities of IoT sensors and a tracking beacon (in the case of *Uzun*) placed on a vehicle: this distinction is vital with regard to any evaluation as to the severity of an interference into a citizen’s private life.⁴⁷³ In addition, in connection with the aforementioned point, we need also appraise any limitations as to the inferences we may draw from the judgment in *Uzun* where the case concerned use of a GPS-based vehicle tracker; the assertion that: “GPS surveillance must be considered to interfere less with a person’s private life than, for instance, telephone tapping” requires reappraisal where we need consider evidence that current location tracking has evolved so as to provide for highly nuanced detail of behaviours pertaining to activities associated with one’s private life.⁴⁷⁴ Furthermore, the *Uzun* judgment notes in particular that the GPS surveillance “...affected him essentially only at weekends and when he was travelling in *S.*’s car” such that “...he cannot be said to have been subjected to total and comprehensive surveillance”; whereas, in contrast, IoT devices may provide the means to conduct monitoring in a far more persistent, and thus invasive, form.⁴⁷⁵

⁴⁷¹ See: *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 125, ECHR 2006-XI

⁴⁷² *Uzun v. Germany* (no. 35623/05, 2 September 2010), §78

⁴⁷³ See: *Uzun v. Germany* (no. 35623/05, 2 September 2010), at §70

⁴⁷⁴ See: *Uzun v. Germany* (no. 35623/05, 2 September 2010), at §72

⁴⁷⁵ See: *Uzun v. Germany* (no. 35623/05, 2 September 2010), at §80

Furthermore, the increasing prevalence of devices with acutely precise embedded sensing technologies can produce highly detailed, unique records that afford greater scope to identify attributes of a specified individual. These identifiers may then be utilised in location analytics (such as examining people's interactions with spaces and how long they dwell in certain places) or in analyzing individuals' temporal-spatial trajectories and patterns of mobility.⁴⁷⁶

In this context, Recital 26 of the Data Protection Directive (95/46/EC) needs also be considered, paying particular attention to the term "identifiable": "whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." This clause pertinent where aggregate location data based on notionally 'anonymized' datasets may be used, especially where one considers recent evidence as to the relative ease by which individuals' identities may be discerned from relatively little information as to their regular patterns of movement.⁴⁷⁷ Whilst anonymization can protect privacy, analysis of location data has shown that identities may however be inferred from such supposedly anonymous data. Where approximate locations of an individual's home and workplace can both be deduced from a location trace, persons can be re-identified relatively easily. Public records (voter registration data, for example) may provide sufficient information to identify persons based on details of addresses matched to mobility data.⁴⁷⁸

⁴⁷⁶ See: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.8

⁴⁷⁷ See: Yves-Alexandre de Montjoye et al, Unique in the Crowd: The privacy bounds of human mobility, Nature.com - Scientific Reports 3, Article number: 1376, 25 March 2013, Available at: <http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html>. This scientific study of mobility notes that even in a dataset where the location of an individual is specified hourly, four spatio-temporal points are enough to uniquely identify 95% of the individuals. Gruteser and Liu note that in continuous location-tracking prior movement data can help infer where the individual will make future visits; they characterise the challenge principally as ensuring locational privacy is sufficiently protected where suppression of location updates occurs in only a few sensitive areas. Disclosure-control algorithms can protect an individual's sensitive locations, yet the difficulty in protecting privacy lies in ensuring visits to 'sensitive areas' remain undisclosed whilst the technical means employed not unnecessarily decrease availability of location information in 'insensitive areas', which users consent to disclose (as it would likely degrade the quality of the service they receive). See: Gruteser, M.; Xuan Liu, "Protecting privacy, in continuous location-tracking applications," Security & Privacy, IEEE , vol.2, no.2, pp.28,34, Mar-Apr 2004, Available at: <http://ieeexplore.ieee.org>, pp.29-30

⁴⁷⁸ Golle and Partridge note that home and work locations may be joined with employment directories, tax records or any other public or private dataset available to map locations to identities. See: Philippe Golle and Kurt Partridge, On the Anonymity of Home/Work Location Pairs, 2009, Available at: <http://xenon.stanford.edu/~pgolle/papers/commute.pdf>, p.4

3.1 IoT-specific challenges to the safeguard of the rights to privacy and personal data protection

The relevant legal framework at the EU level for assessing the data protection and privacy issues pertaining to the use of such devices is to be found in Directive 95/46/EC⁴⁷⁹ in conjunction with the subsequent provisions specified in Directive 2002/58/EC (as amended by Directive 2009/136/EC).⁴⁸⁰

An initial examination of the functions and operation of IoT requires contextualizing the application of the provisions set forth under Article 4 of Directive 95/46/EC that refer to the use of “equipment” in respect of the processing of personal data and the establishment of jurisdiction for the national law applicable.⁴⁸¹ Noteworthy in this context is the absence of a descriptive definition of the term “equipment” in Article 2 of the Directive. Nonetheless, in this context a review of the Preamble to Directive 95/46/EC proves insightful for its capacity to illustrate the extent to which the language, and hence the remit of the Directive itself, is grounded in the conceptualization and scope of data processing and data protection as understood at the time of it entering into force. This point is perhaps most aptly illustrated by the extent to which the provision made in Recital 2 of the Preamble clearly attempts to articulate a fundamental precept by which data-processing systems are “designed to serve man”: in the light of the evolving capabilities of nascent IoT technologies this premise, whilst not necessarily being now subject to dispute *per se*, nevertheless constitutes a basic tenet worthy of further examination, not least with respect to how our appraising we now understand the intrinsic values and purposes of technologies, and how indeed these traits might engage fundamental rights.⁴⁸²

⁴⁷⁹ Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

⁴⁸⁰ Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

⁴⁸¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data - Article 4

“National law applicable

(c) the controller is not established on Community territory and, for purposes of processing personal data *makes use of equipment, automated or otherwise*, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.”

Note: *emphasis added*.

⁴⁸² Recital 2 of Directive 95/46/EC.

It should be noted in this respect that the flexibility of the language of Directive 95/46/EC in respect of the recitals of the preamble was purposefully chosen so as to allow its articulations to be applied to divergent situations and scenarios in which the use of technologies engage fundamental rights, including those which could not be foreseen when the Directive was adopted.⁴⁸³ In the case *Biriuk v. Lithuania* the ECtHR rearticulated the principle that the effective respect for private or family life could be subject to broad interpretation. However, it also reaffirmed its position that the provisions of the Convention guaranteed rights be understood such that safeguards are both functional and efficacious in their application:

“The Court reiterates that, as regards such positive obligations, the notion of “respect” is not clear-cut. In view of the diversity of the practices followed and the situations obtaining in the Contracting States, the notion’s requirements will vary considerably from case to case... The Court nonetheless recalls that Article 8, like any other provision of the Convention or its Protocols, must be interpreted in such a way as to guarantee not rights that are *theoretical or illusory* but rights that are *practical and effective*.”⁴⁸⁴

Similarly, it might also be observed that the assumptions and premises that support the Directive’s affirmations as to the requirement that data processing contribute to social progress and the well-being of individuals now too demand reappraisal in the light of technological advancements.⁴⁸⁵

⁴⁸³ Recital 26 to Directive 95/46/EC, for example, was purposefully written to articulate that the concept of personally identifiable information be interpreted in a broad sense, and that this allows for Directive to be applied in a wide range of data collection and processing operations. Nonetheless, whilst effective in ensuring that the Directive is suitably flexible and encompassing, the approach however complicates the application of the Directive in cases where it is not immediately evident how it is to be strictly applied. *See*: EU Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4 November 2010 Available at: <http://eur-lex.europa.eu/LexUriServ>, p.5

⁴⁸⁴ *Biriuk v. Lithuania*, No. 23373/03, § 37, 25 November 2008. Note: *emphasis added*.

⁴⁸⁵ In particular, it should be noted that recital (2) of the preamble to Directive 95/46/EC affirms: “Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and *social progress*, trade expansion and the *well-being of individuals*;” Note: *emphasis added*.

3.2 The relationship between personal data, location and time (temporal aspects)

In essence, Article 2 of Directive 95/46/EC broadly seeks to establish definitions in respect of two categories.⁴⁸⁶ With respect to conceptualizing ‘personal data’, it outlines that the concept concerns specific factors pertaining to the data subject’s “physical, physiological, mental, economic, cultural or social identity”. Whilst, with regard to the data subject’s ‘consent’, the provision subsequently affirms that a data subject’s ‘consent’ pertains to the “freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.” These definitions thus relate to determining the parameters for classifying types of information (and how they are connected to an identified or identifiable person) and to the notion of an individual’s consent to data processing.

Article 2 of Directive 95/46/EC is notable too for its elucidation of the meaning of ‘personal data’, which clearly constitutes a central precept to the broader application of the framework of data protection law. Applying these concepts to location data we need understand the interpretation of the text: ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.⁴⁸⁷ Article 2 is therefore pertinent to our appraising the inter-relationship between *identity* and *information* as identifiers; especially as regards factors such as the physical, social and physiological state of the individual: they are concurrently disparate, contrastive and yet in certain contexts also correlative.⁴⁸⁸ Discerning how Article 2(a) applies in

⁴⁸⁶ Article 2, ‘Definitions’, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

⁴⁸⁷ Article 2(a) of Directive 95/46/EC

⁴⁸⁸ Interestingly, the WP29’s discussion of the advent of new IoT applications and services vis-à-vis the applicability of Article 2 of the EU Data Protection Directive is rather lacking in specificity and thus provides a somewhat opaque attempt at elucidation; it articulates a quite incoherent description of how stakeholders are offering new applications and services through the IoT “through the collection and the further combination of this data about individuals – whether in order to measure the user’s environment- specific data “only”, or to specifically observe and analyze his/her habits”. See: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.4

the context of IoT is also important for our cognizance of the issues that arise from location data acquired by connected devices, in that one needs appreciate how information *relates* to a data subject.⁴⁸⁹ Discerning whether a natural person is identifiable, or may be identified, indirectly is becoming more difficult to determine, especially with respect to personal location data.

In the case *Google Spain and Google*⁴⁹⁰ before the ECJ the Court referred to its earlier ruling in *Lindqvist* in noting that the term ‘processing’ be given a broad interpretation as regards the provision contained within Article 2(b) of Directive 95/46/EC.⁴⁹¹ The court’s subsequent deliberations in respect of the scope of operations that fall with Article 2(b) of Directive 95/46/EC are such that its articulation as to the broad purview notion of ‘processing’ inheres indicates that operators of IoT systems should infer that their data operations are very likely to be classified as ‘processing’ within the meaning of that provision within the Directive.⁴⁹² Paragraph 32 of the *Google Spain and Google* judgment is especially apposite to our discussion of the scope of responsibilities of data processors and controllers in that it reaffirms the significance of the provisions made within Article 2(d) of Directive 95/46, which defines ‘controller’ as “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the

⁴⁸⁹ In a broader context it must be noted that the WP29’s opinion on IoT is rather confusing for the very broad conclusions it draws, where it links, respectively: unspecified sensors “embedded in *common, everyday* devices - “things”” to the “notions of “pervasive” and “ubiquitous” computing”, and then in turn establishes that these indicate that the “IoT *usually implies* the processing of data that relate to identified or identifiable natural persons, and therefore qualifies as personal data in the sense of article 2 of the EU Data Protection Directive.” The WP29’s explanation as to the basis for the broad applicability of Article 2(a) to IoT also lacks the necessary precision as regards specific detail regarding the criteria by which the data collected from embedded sensors constitutes personal data. Clearly, qualifying that IoT “usually implies” a type of activity covered by the scope of Directive 95/46/EC absent distinct examples of data collection by a sensor is too ambiguous an assertion. Noteworthy, then, is the contrast of the certitude of the approach expressed in the aforementioned example with the hesitancy of WP29 to expand upon their own projections as to how IoT data collection is developing: “At this stage, the extent to which the IoT will develop is impossible to predict with certainty. This is in part because the question of how the transformation of all the data possibly collected in the IoT into something useful, and hence commercially viable, remains largely open.” See: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, pp.4-5. Note: *emphasis added*.

⁴⁹⁰ *Google Spain and Google*, C-131/12, EU:C:2014:317

⁴⁹¹ Directive 95/46/EC, Article 2(b): Definitions - For the purposes of this Directive: (b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

⁴⁹² *Google Spain and Google*, C-131/12, EU:C:2014:317, §28

processing of personal data’.”⁴⁹³ It should be noted too that the Court asserts the importance of considering the party responsible for determining the “purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity” shall be considered a data controller in respect of that processing pursuant to Article 2(d).

Furthermore, the Court reasserted its willingness to underpin the importance of the rights of the data subject, which proves pertinent to our understanding how it might view similar concerns that arise where parties are engaged in operations relating to the processing of data from IoT-enabled networks. It stated that the wording of the provision within the Directive was clear, so as to ensure “broad definition of the concept of ‘controller’, effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.”⁴⁹⁴ The judgment further underscored this point vis-à-vis the depth of the responsibility attributed operators in noting that the “person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.”⁴⁹⁵ As such, the ruling clearly indicates the Court’s belief that Directive 95/46/EC should be interpreted so as to provide steadfast and concrete protections to the data subject in terms of the processing of their personal data.

Location data inheres the capacity to divulge information linking mobility and trajectories. That it may act as such as a proxy for other types of personal data has only recently become the subject of significant research (the relative lack of enquiry in this sphere reflecting the historical scarcity of location data and its lack of precision). In essence, central to this point of contention is our comprehending the correlation between location data and personally identifiable information, and how we

⁴⁹³ *Google Spain and Google*, C-131/12, EU:C:2014:317, §32

⁴⁹⁴ *Google Spain and Google*, C-131/12, EU:C:2014:317, §34

⁴⁹⁵ *Google Spain and Google*, C-131/12, EU:C:2014:317, §38

understand how devices *relate* to a natural person. Perhaps this association between device and person appears incongruous because the very term “Internet of *Things*” employs two terms (both ‘Internet’ and ‘things’) that give the impression of a concept that is inherently impersonal. Furthermore, IoT represents a sea change for our application of the existing data protection framework to device sensing; the framework having largely been conceived of and developed over the past three decades in which the advent and subsequent maturation of ‘personal computing’ largely shaped our perceptions of how we interact with devices. The notion of the ‘personal’ vis-à-vis our relationship with information technology is now subject to change, where this transformation reflects the evolution of two foundational aspects of surveillance and monitoring. Firstly, developments in sensor technology have precipitated far-reaching changes in the acuity and sensitivity of our actions and behaviour. Second, equally important have been the advances in connectivity and communications that allow for the networking of sensing units to distribute more widely the data collected for processing.

The processing of personal data relating to elements of physiological identity of identifiable persons is becoming progressively more widespread where the sensing abilities of devices inhere increasingly more exacting and precise measurements of movement. Indeed, the levels of detail to which the spatial aspects of the temporal-spatial location of an individual can be measured call into question how we define ‘location data’. ‘Location data’, as a term, is deficient where it fails to articulate the critical temporal dimension the data itself intrinsically inheres. These two coexisting elements of location data are integral to its fundamental utility; absent either of the two constituent parts (whether either the spatial or the temporal component) location data is far less valuable in terms of its potential to allow for extrapolations and deductions to render relevant information. This is particularly true as regards data processing that aims to discern specific characteristics pertaining to individual identity, especially those of an abstract or intangible nature (linked to, for example, cultural, social and mental faculties relating to individual personalities).

The second category of definitions articulated within Article 2 of Directive 95/46/EC reflect the requirement that the respective parties connected to the processing of personal data are defined with sufficient resolution for the purposes of interpreting the

Directive's provisions. As such, the omission of a definition of the term "equipment" can be seen to reflect the necessity of preserving in the Directive a 'technology neutral' position.⁴⁹⁶ By adopting such an approach the legislation eschews the possibility of technological developments potentially rendering a distinct classification listing the relevant apparatus to which it applies becoming obsolete. Such an omission is, however, not surprising; indeed, one of the foremost challenges any framework governing data protection issues faces is the necessity of retaining, and balancing, adequate specificity in articulating the scope of its provisions whilst allowing for sufficient flexibility for its future application and interpretation in the light of advances in technological capabilities.

Recital 38 of Directive 95/46/EC articulates a foundational principle of data protection, namely that for processing to be fair "the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, *bearing in mind the circumstances of the collection*".⁴⁹⁷ It must be noted that in the context of IoT relating to the collection and processing of data, the qualification as to the relevant scope of application of the provision such that 'the circumstances of the collection' must be considered is especially important. The inclusion of the provision indicates the pertinence of carefully appraising context and conditions. Where one considers technological developments in the evolution of sensing devices that relate to the collection and processing of location data, the ambit of the clause is perhaps too limited in terms of its scope. More appropriate in the light of recent technological advancements would be an assertion that considers the necessity of 'the circumstances of the collection and *processing*'.

Contextualizing the interpretation of Recital 38 of Directive 95/46/EC in respect of

⁴⁹⁶ In this respect it should be noted that the preamble to Directive 95/46/EC clearly articulates this broad, encompassing nature of this approach so as to avert the possibility that processes involving data processing appurtenant to the ambit of the Directive are made subject to its provisions, notably in recital (27), which states: "Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the *techniques used*, otherwise this would create a serious risk of circumvention". Note: *emphasis added*. Directive 95/46/EC, Recital (27).

⁴⁹⁷ Directive 95/46/EC, Recital 38: "Whereas, if the processing of data is to be fair, the data subject must be in a *position to learn* of the existence of a processing operation and, where data are collected *from him*, must be given accurate and full information, *bearing in mind the circumstances* of the collection;" Note: *emphasis added*

the operation of the IoT ecosystem presents several distinct quandaries as regards an apposite elucidation of the protections afforded the data subject. Paradoxically, Recital 38 articulates the notion that the data subject be placed *in a position to learn of the existence of a processing operation* for the *processing* of data to be fair. Whereas the recital in question indeed notes that this consideration be appraised “bearing in mind the circumstances of the collection”, it would nevertheless appear significant, then, that the singular reference here is to that of processing of data, rather than having it infer a parallel obligation in respect of affording the data subject access to information as to the extent of data collection activity. Those making use of a device (critically, as regards IoT, whether either in the *passive* or *active* sense of the term) have a right to expect that the collection and processing of personal data is consistent with the context in which the data subject concerned provides it.

Furthermore, we might also consider at this point the extent to which placing a data subject “in a position to learn of the existence” of an operation is to be meaningfully put into effect. In essence, by what manner might the relevant parameters reasonably be established to ensure the uniform practical application of this requirement of the provision? Whilst perhaps appearing at first glance a somewhat abstruse point to contemplate, the notion too of placing a ‘data subject in a *position* to learn’ also presents a dilemma when framed within the context of locality: how should this discovery and, subsequently, the process of providing relevant, accurate information, be effectively delivered in practice? Conceivably, the term ‘position’ in this regard is conspicuous; for it hints at the predicament of establishing the most appropriate opportunity (both in the temporal and spatial sense) for the data subject concerned to be made aware of the existence of such an operation. The affirmation that this requirement be appraised ‘bearing in mind the circumstances of collection’ thus provides negligible resolution of this obvious challenge.

In addition, a further issue arises with respect to the association between the data subject with a connected device that senses, monitors and communicates has evolved. Whilst initially a provision that makes reference to “where data are collected from him” might appear innocuous, in the context of IoT it may however prove equivocal nonetheless. At question is the relationship between the device and the individual, the data subject, and the extent to which both entities inter-relate, and the notion of

agency as it corresponds to an action or intervention. In essence, the problem stems from the effective determination of whether data are collected *from him*, i.e. the data subject. The functionality of devices and, equally important, the scope of diversity of the services they connect to, continue to both proliferate such that it is increasingly difficult for specialists, let alone the layperson, to determine whether and how data are collected. Thus, in certain cases the *circumstances of collection* may be difficult to determine with the required resolution to establish the extent of any association between a device with the data subject i.e. how might the two relate in terms of a connection, such that data collection is in essence '*from him*'.

3.3 Purpose specification principle and use limitation

In this discussion we need also further consider Recital 38 of Directive 95/46/EC with reference to other guidance given earlier in the Preamble of the Directive. In particular, Recital 28 of the Preamble to Directive 95/46/EC is especially important, for it relates to the two principles of the purpose specification principle and use limitation as applied to both collection and processing of personal data. With IoT the purposes of establishing whether the data is 'adequate, relevant and not excessive in relation to the purposes for which they are processed' is particularly pertinent to location data.⁴⁹⁸ The process of qualifying and quantifying whether the data in question meets these criteria is rendered considerably more complex when we take into consideration that the purposes for which processing takes place are, in respect of location data, changing rapidly. While our understanding of the intrinsic value of location data is still very much incomplete it remains difficult to resolve how *explicit*, i.e. the level of specificity required, should be addressed in terms of the collection and processing of location data.

⁴⁹⁸ Directive 95/46/EC, Recital 28:

“Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;”

4. Contextualizing consent in relation to IoT functionality

An important issue with respect to the collection of location data by an IoT device's sensors regards the manner in which feedback from the devices may be displayed to the data subject, and how this information relates to the totality of the personal data collected by the sensors themselves. Frequently the functionality limits the device such that it reveals only aggregated displayable data and, as such, this restricts the ability of the data subject to develop a comprehensive understanding of the extent of the personal data being processed.⁴⁹⁹ In these instances a data subject is afforded only limited scope to make informed decisions in relation to the collection and processing of their personal data; this lack of transparency thus inhibits the quality of the user's consent, where they may not be sufficiently informed as to the types of data processing of location data being performed as a result of their using a particular device.

The issue of consent largely centres on reasonable awareness that one's location and movement may be subject to surveillance and clear prior notification as to the basis on which monitoring by a public authority may lawfully occur. The particular issue in question highlights the applicability of the ECtHR's established precedent pertaining to 'secret measures' (articulated by the ECtHR in *Halford v. United Kingdom*: "the context of *secret measures* of surveillance or interception of communications by public authorities")⁵⁰⁰ and distinctions drawn between covert/overt monitoring. A challenge exists in so far as location data constitutes personal information, though it may be seen as qualitatively different from other data pertaining to more immediately tangible aspects of a person's identity, such as name, age, gender, etc.

A justifiable concern exists as to indeed whether information pertaining to one's location, and to mobility, is made available in a truly consensual manner – as such, at the 'initiative' of the user and based on their having given informed consent in the

⁴⁹⁹ A number of studies have shown that users are given insufficient information and insight into how data collection and processing occurs. Often users are unaware how a device accesses location data via sensors, and what resources an application utilises to process this it. For the individual concerned this lack of transparency contributes to the risk of interferences with their rights to privacy and personal data protection. See: Bal G., *Revealing Privacy-Impacting Behavior Patterns of Smartphone Applications*, 2012, Available at: <http://mostconf.org/2012/papers/15.pdf>, pp.1-2.

⁵⁰⁰ *Halford v United Kingdom* (1997) 24 EHRR 523, § 49. Note: *emphasis added*.

knowledge as to how their carrying of a mobile device indeed allows for location tracking to take place. More broadly, this issue also pertains to the public/private dichotomy and access to location data as a whole by public authorities, where use may be made of aggregated and anonymized data for the purposes of crime prevention using predicative techniques, in addition to monitoring of pre-selected suspects using personal data specific to an individual.

The concerns raised by the EDPS in respect of the indiscriminate gathering of data (in contrast to collection by a public authority whereby an individual is targeted based on an identified suspicion) are especially pertinent as concerns the modeling of movement patterns based on the use of location data made available to law enforcement. The agency has argued in its opinion on ‘Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)’ that there is a: “...need to rethink and possibly redefine the right balance between law enforcement purposes and safeguarding fundamental rights of the individuals... when information is gathered through surveillance methods outside of a concrete criminal case, also the context of fundamental rights protection changes.”⁵⁰¹ The agency also underscored the need to further examine the consequences for public security vis-à-vis the trend toward widespread, systematic and proactive surveillance of ‘non-suspected individuals’ in respect of its actual efficacy in combatting criminal activity.

Purpose limitation is also a significant additional consideration as a basic tenet of applicable data protection law, insofar as only under certain strict conditions should personal data be used for purposes other than for which the data were originally collected.⁵⁰² In this regard the ECtHR has noted that their must exist appropriate

⁵⁰¹ EDPS, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council entitled ‘Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)’, 29 April 2013, Available at:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-04-29_EIXM_EN.pdf, p.6

⁵⁰² EDPS, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council entitled ‘Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)’, 29 April 2013, Available at:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-04-29_EIXM_EN.pdf, at §35

safeguards for the purpose of limiting the use of the information obtained to what is necessary to serve the purpose of strategic monitoring.⁵⁰³

Thus the absence of easily understandable information notifying a data subject as to the purposes for which a data controller collects, processes and disseminates data directly challenges a basic principle of data protection - that of purpose specification (whereby the purposes for which personal data are collected should be specified not later than at the time of data collection; and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. IoT devices and services need therefore incorporate the means to ensure that such notice is provided, and to specifically articulate the purpose or purposes for which personal data, including location data, are to be used. Absent this notification, a data subject would be insufficiently informed as to the scope of data processing performed by a specific device or associated service. This deficiency represents an appreciable impediment to substantiating a data subject's accession to the collection and processing of personal data. Under these conditions the consent provided by a data subject cannot be relied upon as a legal basis for the corresponding processing of data as required in accordance with EU data protection law.

The ECtHR held in the case of *Copland v. United Kingdom*⁵⁰⁴ that information of a less than notionally private nature (in *Copland* telephone bills freely available to other parties which provide information as to another's conduct) did not infer that Article 8 guarantees to the right to privacy did not apply, rather that: "The mere fact that these data may have been legitimately obtained... in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (ibid.). Moreover, storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1."⁵⁰⁵ Even where it might be inferred that location data is 'freely made available' (for example, to the telecommunications operator)⁵⁰⁶ where

⁵⁰³ See: *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 122, ECHR 2006-XI

⁵⁰⁴ *Copland v. the United Kingdom*, April 3, 2007 ECtHR

⁵⁰⁵ *Copland v. the United Kingdom*, April 3, 2007 ECtHR, § 43

⁵⁰⁶ Yim, Y. B. Youngbin; & Cayford, Randall. (2001). Investigation of Vehicles as Probes Using Global Positioning System and Cellular Phone Tracking: Field Operational Test. UC Berkeley: California Partners for Advanced Transit and Highways (PATH). Available at: <http://escholarship.org/uc/item/0378c1wc>, pp.5-8

citizens are aware as to service providers collecting such information, nevertheless those concerned however still enjoy the privacy guarantees enshrined within Article 8. The separation of law enforcement and private sector activities, whereby dedicated public authorities perform law enforcement tasks and private actors are to be solicited on a case-by-case basis to communicate personal data is, as established practice, increasingly subject to revision. Whether this premise remains the extant model for cooperation has been raised most recently by the EDPS, which highlighted in its April 2013 opinion the changing nature of the relationship between private and state actors in the role of monitoring: “There is now a tendency to require that private actors cooperate with law enforcement authorities on a systematic basis.”⁵⁰⁷

A further consideration linked to the quality of consent provided by data subjects in relation to the use of IoT devices reflects the frequent inability of the individual concerned to accurately gauge the quality of the data collected and processed by the device or service being exploited.⁵⁰⁸ The data subject is unable in such cases to provide consent where they cannot meaningfully apprehend and qualify the standard of data quality, and determine whether the level of precision delivered meets their expectations (considering too that this lack of insight might also occur in conjunction with further deficiencies as regards the quality of consent).⁵⁰⁹ Indeed, the trend toward

⁵⁰⁷ EDPS, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council entitled 'Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), 29 April 2013, Available at:

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-04-29_EIXM_EN.pdf

⁵⁰⁸ Peppet contends that citizens need not be worried about the collection of sensor data, only that they be concerned as to how data is processed, noting: “Accuracy, however, is really not the problem with Internet of Things sensor data. One’s Fitbit, driving, or smart home sensor data are inherently accurate - there is little to challenge. What is more questionable are the inferences drawn from such data.” However, Peppet fails to take into consideration the simple prospect that sensing errors may arise from, for example, software flaws or basic malfunctions in data capture hardware. These imperfections would result in inaccuracies. *See*: Peppet S. R., *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, Vol. 93 *Texas Law Rev.* 85, pp. 85-103 Available at: <http://www.texasrev.com/wp-content/uploads/Peppet-93-1.pdf>, p.128

⁵⁰⁹ Indeed, the WP29 expert group’s Opinion on the Internet of Things highlighted deficiencies in the accuracy of location data collected, particularly where inferences are drawn in connection with diagnostics that correlate physical condition and an individual’s mobility patterns with the data subject’s personal health. For example, the WP29 has cited recent analyses that have “challenged the real accuracy of the measures and of the inferences made from them” in respect of devices incorporating embedded sensors that monitor an individual’s personal movements. *See*: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.6, In addition, analysts have highlighted the difficulty in developing algorithms competent in accurately capturing a person’s individual movements based upon

conducting analysis using increasingly more precise location data utilizing ever more refined scales for spatial measurements gives rise to additional concerns in terms of ensuring data quality.⁵¹⁰ Data processing and analysis becomes yet more complex still when we introduce the data relating to environmental factors captured by IoT and take into account environmental influences on human actions and behaviour. There is no simple universal criterion to define the appropriate parameters for determining the necessary degree of accuracy for many of the factors technology developers are looking to gauge.⁵¹¹

4.1 Consent, control and information asymmetry

At the heart of concerns as to whether IoT-generated location data can be subject to effective oversight by the existing legal framework is the issue of whether the developments in technology constitute a fundamental recasting of the nature of the relationship between the different actors concerned: the data subject, the data controller, and the data processor.

the detection of changes in position in three dimensional space by geopositioning sensors in personal devices; currently, based solely on recording these movements, algorithms are frequently unable to differentiate between even quite dissimilar types of human movement, such as walking backward or skipping. *See*: Wired.com, Why Fitness Tracker Calorie Counts Are All Over the Map, 17 August 2012, Available at: <http://www.wired.com/2012/08/fitness-trackers/>. In addition, one wearables device manufacturer and service provider states that miscalculations are to be expected when tracking a user's movements based upon a known variety of factors influencing the accuracy and reliability of GPS-based location data. *See*: MapMyFitness, Android GPS Recording Help, Available at: <https://support.mapmyfitness.com/hc/en-us/articles/200117874>.

⁵¹⁰ When making measurements, resolution is imposed across the dimensions relevant to location data, including space and time in the form of discretisation. Crucially, there has been little acknowledgement that this imposition results in a loss of information that contributes to uncertainty as to the accuracy of the variable or phenomena being described. Indeed, the effects of discretisation are likely to be more substantial than measurement error. Whilst research on location data collection has tended to focus on measurement errors, the impact of discretisation may in many cases be more substantial in terms of its overall impact on the accuracy of judgments drawn from the analysis of location data. *See*: Chrisman, N., "The Role of Quality in Information in the Long Term Functioning of a Geographic Information System." *Proceedings of Auto-Cartography*, Volume 6, 1983, pp. 303–312; *See also*: Sinton, D.F., "The Inherent Structure of Information as a Constraint to Analysis: Mapped Thematic Data as a Case Study." *Harvard Papers on Geographic Information Systems*. Vol. 6, 1978, pp. 43–59. The NCHRP also notes: "The primary sources of error associated with positional data are acquisition or measurement, processing, transformation, and presentation or visualization. Regardless of the measurement technique and referencing system, data will be observed with error." NCHRP, *Quality and Accuracy of Positional Data in Transportation*, 2003, Available at: http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_506.pdf: Forward to the NCHRP Project 20-47(01), p.61

⁵¹¹ *See*: Bernasco, W., *Putting Crime in its Place: Units of Analysis in Geographic Criminology*, Dordrecht: Springer, 2008, p.38

To date, a significant proportion of the analysis on IoT has sought to underscore that the difficulties in applying the existing legal framework to the protection of personal data and privacy are so deep-rooted as to call into question whether in fact it is apt to satisfactorily regulate the use of new devices and services. However, often this evaluation is based upon only the most cursory or marginal review of real-life scenarios. Where parties speak of ‘information asymmetry’ in relation to the dissonance between data subjects and the controllers of data collected by IoT services and devices, they might reflect whether this is too one-sided an approach.⁵¹² Clear examples of technology use are essential in exemplifying these specific points; absent definitive examples (and an elucidation of the context, by way of a credible scenario) the immediate appraisal that results is too imprecise and approximate to be of value. The intrinsic limitations of adopting such a generalized approach are distinctly evident in the rather unwieldy guidance given with regard to “IOT-pushed data” (notwithstanding the particularly esoteric term, which in itself is problematic), where data subjects are, the WP29 experts group suggests, submitted to “a risk of lack of control and excessive self-exposure for the user”.⁵¹³ This line of reasoning is in turn rendered all the more opaque where the challenges in safeguarding personal data protection in relation to IoT are regrettably conflated with those of other technical developments and emerging technologies such as cloud computing and big data.⁵¹⁴

⁵¹² For example, the WP29 adopts a resolutely negative approach in seeking to illustrate the possible deficiencies in the existing data protection framework in its speculation as to how established instruments will ensure data subjects’ rights and interests are safeguarded. Illustrating this point, the WP29 is rather suppositious in its affirmation that: “More generally, interaction between objects, between objects and individuals’ devices, between individuals and other objects, and between objects and back-end systems will result in the generation of data flows that can hardly be managed with the classical tools used to ensure the adequate protection of the data subjects’ interests and rights.” See: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.6. Note: *emphasis added*. Moreover, the excerpt underscores that recourse to broad-ranging illustrations of a technology’s use, in conjunction with the umbrella hypotheses their analysis inevitably produce, is inherently problematic.

⁵¹³ WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.6

⁵¹⁴ See: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, pp.6-7

4.2 Appraising the function of consent in the relationship of IoT devices to the data subject

The principle of gaining informed consent from the data subject prior to engaging in data collection or data processing is a fundamental concept in framing the data protection safeguards stipulated in the European legal framework. The centrality of consent to protection of the individual is explicitly recognised in Article 8(2) of the EU Charter of Fundamental Rights, which states that personal data may be processed “on the basis of the consent of the person concerned or some other legitimate basis laid down by law”.⁵¹⁵ However, consent does not constitute the only legitimate basis for which the processing of personal data may be authorised (as is also the case in the Data Protection Directive the EU Charter of Fundamental Rights recognizes other legitimate grounds). According to Directive 95/46/EC, consent provides one of the grounds for the lawfulness of the processing of personal data, though the obtention of an individual’s consent does not allow for the circumvention of other provisions within the framework of legal instruments that safeguard his rights to privacy and data protection.

In only in a narrow range of circumstances may a person’s consent allow for legitimate data processing where they would in other respects be proscribed; this being the case, for example, in respect of Article 8(2)(a), whereby the processing of certain special categories of data is permitted in instances only where explicit consent is given by the data subject and it is not prohibited by the laws of the Member State in the jurisdiction concerned.⁵¹⁶ Furthermore, even where the consent of a data subject is obtained, the principles relating to data quality and with respect to the fairness, necessity and proportionality of data collection and processing still apply. A data subject’s consent cannot nullify Article 6’s provisions to allow, for example,

⁵¹⁵ EUCFR, Article 8(2)

⁵¹⁶ Article 8

Directive 95/46/EC, Article 8:

“The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent.”

collection of location data that would be excessive in relation to a specified purpose.⁵¹⁷

Thus a close reading of the provisions relating to Directive 95/46/EC is necessary if we are to properly establish how we frame the concept of consent in respect of the operation of IoT devices and services.⁵¹⁸ In essence, for a data subject's consent to meet the threshold established under Directive 95/46/EC it must be given freely and on an informed basis,⁵¹⁹ however, one needs to consider the interdependency of the entirety of provisions and how they relate to one another in determining the scope of applicability. This concern is pertinent where a data subject may not be made aware of the collection or processing of location data by devices, and where the relationship

⁵¹⁷ The WP29 has affirmed that a data subject's consent may legitimise data processing activities in only very limited circumstances, stating: "As a principle, consent should not be seen as an exemption from the other data protection principles, but as a safeguard. It is primarily a ground for lawfulness, and it does not waive the application of other principles." *See*: WP29, Opinion 15/2011 on the definition of consent, 01197/11/EN WP187, 13 July 2011, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf, p.7

Directive 95/46/EC, Article 6:

1. Member States shall provide that personal data must be: (a) processed fairly and lawfully;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

⁵¹⁸ Directive 95/46/EC, Recital (30): "Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies;"

[]

Recital (33) "Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;"

⁵¹⁹ Directive 95/46/EC, Article 2: Definitions

For the purposes of this Directive:

- (h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

between the object and individual proves indistinct, such that determining whether data processing is legitimate on the basis that consent is given remains problematic.⁵²⁰

A critical consideration in this regard is the extent to which the user can comprehend the means by which the data processing renders them a data subject, where the provision of relevant information and instruction to the individual is either minimal or, feasibly, entirely lacking. A parallel might thus be drawn between the emerging issues stemming from the emergence of IoT technologies with those the Commission identified earlier with the advent of the use of enhanced capabilities in video surveillance by operators; with the latter development the Commission noted that a number of legal and practical issues resulted for both operator and the data subject in respect of the implementation of Directive 95/26/EC, particularly as regards the exercise of the individual of their fundamental right to data protection.⁵²¹ In such cases, then, it remains questionable whether consent can be relied upon as a legal basis for the corresponding data processing under the existing framework of EU law for many of the operations performed by IoT devices. In this context it should be noted that the WP29 has made the general assertion that it considers consent cannot be purposefully attained where a “lack of information constitutes a significant barrier to demonstrating valid consent under EU law.”⁵²²

The difficulty in achieving a conceptual clarification of consent is rendered more complex still where it is surmised that a workable approach must allow for the

⁵²⁰ Directive 95/46/EC, Article 7: Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

[]

(d) processing is necessary in order to protect the vital interests of the data subject;

⁵²¹ An immediate example for comparative purposes would be the uncertainties that arise in respect of the applicable definitions within Article 2 of Directive 95/46/EC and the operation of IoT devices, and the earlier issues raised in relation to whether isolated images or fingerprints were to be considered personal data in those cases where the data controller is unable or extremely unlikely to identify an individual, or whether simple monitoring would constitute a processing operation. The analogy reflects in particular the similitude between the data collected by devices that monitor the ambient surroundings of a space (thereby allowing for the collection and processing of data relating to persons, who may or may not be identifiable). The two aforementioned issues underscore how each new development in technology presents challenges to interpretation, and that in this respect IoT may not be so dramatically different. *See*: EU Commission, REPORT FROM THE COMMISSION, First report on the implementation of the Data Protection Directive (95/46/EC), 15 May 2003, COM(2003) 265 final, Available at: <http://eur-lex.europa.eu/LexUriServ>, pp.20-21.

⁵²² *See*: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.7

gradation of consent, such that it is qualified in relative terms (based upon the distinctions drawn, for example, between Article 7 (a) in “unambiguous consent” and “explicit consent” in Article 8 of Directive 95/46/EC.⁵²³ Whilst the notion that IoT raises concerns in relation to the data subject’s consent is relatively foreseeable, it should be noted however that, within the context of seeking to provide clarification as to the meaning of ‘consent’, the guidance given by interested parties, such as the EU Commission for example, has not always been especially explicit. This legacy of inexplicit instruction is of greater concern where advancements in IoT technologies herald more widespread use of personal location data in data processing. By way of illustration, in an explanation given as to how ‘consent’ is to be interpreted, it refers to Article 2(h) of Directive 95/46/EC in noting: “When informed consent is required, the current rules provide that the individual's consent for processing his or her personal data should be a ‘freely given specific and informed indication’ of his or her wishes by which the individual signifies his or her agreement to this data processing.”⁵²⁴

However, in distinguishing between different interpretations as to how these conditions are to be interpreted, the Commission errs in its attempt to differentiate between a requirement of *written consent* or an acceptance of *implicit consent*; that a distinction should be drawn such that the initial reference is to informed consent alone is highly suspect. The notion that “*informed consent is required*”, as opposed to, one might suggest, “*consent lacking an informed basis for decision-making*” is inopportune: for the purposes of the application of the provisions of Directive 95/46/EC valid consent can only ever be that which is given on an informed basis, as is stated in Article 2(h): “‘the data subject’s consent’ shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.” Therefore, to interpose

⁵²³ In this regard the Commission noted in its first report on the implementation of the Data Protection Directive that the ambiguity in respect of how these two concepts be interpreted relating to a data subject’s consent to accede to personal data collection and processing had rendered inconsistent enactment of the Directive. The Commission noted: “The notion of “unambiguous consent” (Article 7 (a)) in particular, as compared with the notion of “explicit consent” in Article 8, needs further clarification and more uniform interpretation. It is necessary that operators know what constitutes valid consent, in particular in on-line scenarios.” See: EU Commission, REPORT FROM THE COMMISSION, First report on the implementation of the Data Protection Directive (95/46/EC), 15 May 2003, COM(2003) 265 final, Available at: <http://eur-lex.europa.eu/LexUriServ>, p.17

⁵²⁴ Directive EC/46/EC Article 2(h)

‘consent’ alongside ‘informed consent’, where the two refer to a single legal concept is misleading.⁵²⁵

Whilst the Commission attempts to explain its position, it fails to adequately elucidate the vital notion that, for the purposes of personal data processing, a data subject’s consent is only valid where it is informed; as such, it needs articulate more resolutely that, absent an informed basis, the consent given by a data subject to processing would be invalid.⁵²⁶ Moreover, clarity on these key concepts is vital in the IoT environment, given that the intangibility and opacity of data collection and processing operations makes raising awareness of individuals as to their right to accept or decline such activity by giving informed consent a difficult task.

Appraising the quality of a user’s consent is made more complex too where IoT devices are being developed that incorporate embedded motion sensors that work in conjunction with established location tracking capabilities. Furthermore, simple, and in the past, straightforward distinctions between a user and a mere observer in connection with data collection and processing, which relate to the notion of agency and the means by which an action or activity engages the individual, are becoming more and more difficult to discern. Frequently complications arise where the progressive miniaturization of devices, coupled with the tendency to integrate location tracking into a wide range of objects that were previously incapable of capturing such information, presents the potential data subject with considerable difficulties in distinguishing how exactly they are to make themselves aware of the process by which data is being recorded and transferred.

⁵²⁵ It should be stated in this regard that two distinct notions corresponding to the qualities required of the provision of consent by the data subject appear to have been conflated: that of Article 7(a) of Directive EC/46/EC which refers to the data subject “unambiguously” giving consent; and the notion by which consent be an “informed indication”. Here ‘specific’ in Article 2(h) can be seen to closely correspond with term ‘unambiguously’ in Article 7 of the legislation.

⁵²⁶ It asserts: “Clarification concerning the conditions for the data subject’s consent should therefore be provided, in order to always guarantee informed consent and ensure that the individual is fully aware that he or she is consenting, and to what data processing, in line with Article 8 of the EU Charter of Fundamental Rights.” In this regard, ironically, a key clarification from the outset would be an affirmation that an informed basis is not merely imperative, but mandatory for consent to be valid. *See*: EU Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4 November 2010. Available at: <http://eur-lex.europa.eu/LexUriServ>, pp.8-9.

The particular question of agency is especially pertinent in this context, where the individual may be subject to processing operations in which the controller has not collected directly from the data subject. Whilst Recital 39 to the Preamble of Directive 95/46/EC indeed acknowledges this potentiality, IoT can be seen to constitute a genuinely transformative influence on the evolution of technologies, which creates distinct new challenges for the regulatory framework.⁵²⁷ Moreover, where the frequency in which citizens are likely to encounter such devices intensifies as their ubiquity proliferates, increasingly critical shall be how we are to determine the participatory component that consent necessarily inheres.

That the data subject “must be given accurate and full information, bearing in mind the circumstances of the collection”⁵²⁸ purposively connotes that consent is an active, participatory engagement reflecting individual choice based on decision making. In this sense it cannot be passive or involuntary; a data collector cannot in any event rely upon tacit agreement by the potential data subject, which would constitute an unworkable type of latent agreement for consent, which could be widely misapplied and abused to the detriment of an individual’s fundamental rights.

In this regard, it also needs be stated that the WP29 expert group’s comments vis-à-vis the particular application of the Directive’s provisions to consent and IoT are rather inauspicious. The choice of rather indistinct, obscure terminology to articulate the challenges inherent to gaining the consent of data subjects in the use of IoT is confusing where the publication of the expert group’s opinion is intended to be informative. Specifically, recourse by the WP29 to such terms as ‘classical mechanisms’, ‘low quality consent’ and ‘fine-tuned consent’ is especially unhelpful where its analysis should furnish more instructive, cogent form of guidance conducive to it being enacted by the parties concerned.⁵²⁹ The use of such terms is problematic

⁵²⁷ Directive 95/46/EC, Recital 39: “Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;”

⁵²⁸ See: Directive 95/46/EC, Recital 38

⁵²⁹ The WP29 Opinion of the Internet of Things states: “In addition, classical mechanisms used to obtain individuals’ consent may be difficult to apply in the IoT, resulting in a “low-quality” consent

in that in lacking any elucidation they further obfuscate rather than clarify the situation. Stakeholders in the IoT domain evidently require more clarity from the group's analysis, and indeed more coherent direction on the issues that have been highlighted as pertinent to their development in line with the existing legislative framework.

Recital 39 references the notion that processing may take place where the controller has not directly collected personal data from the data subject: this consideration is especially important in the context of IoT, where distinctions between the terms *direct* and *indirect* are ever more difficult to articulate in light of the proliferation of ambient sensing capabilities.⁵³⁰ Moreover, the phenomenon of ambient sensing risks further obfuscation of the link between the data subject, the data controller and the processor.

Essentially the problem is one of resolving how we distinguish between location data that relates solely to an object, and that which relates to both an object and an individual. The issue reflects a natural progression of the need to find an expedient rationalization of the parameters by which we differentiate categories of data. The problem stems in part from the persistent difficulties of identifying how an object relates specifically to an individual and, more specifically, how a device capable of sensing collects and processes personal data that that possibly also relates to the surrounding environment. Furthermore, in certain circumstances the data subject may not be the actual owner of the device, nor indeed even be aware of its existence (and, moreover, its data collection and processing functionality). In many cases for the data

based in a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals.” Thus, in stating that “new ways of obtaining the user’s valid consent should be considered by IoT stakeholders” the group might seek to more effectively articulate the foundation of its rationale, perhaps by providing clear examples of situations and scenarios to illustrate the challenges posed by IoT devices and services.

WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.7. Note: *emphasis added*.

⁵³⁰ Directive 95/46/EC, Recital 39: “Whereas certain processing operations involve data which the controller has not collected *directly* from the data subject;” Note: *emphasis added*. The central question here therefore is that of agency i.e. how exactly does the functioning of the device relates to an individual specifically in connection to the collection and processing of data; the issue as such recalls the a fundamental precept, namely one of the most fundamental of determinations vis-à-vis the principles of data protection, identifiability; *inter alia* Recital 26 of the preamble of Directive 95/46/EC states: “information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person;”.

subject it may prove unfeasible to comprehend how location is tracked, whether in respect of their movement relative to a fixed device or, as is more usual, where the device itself moves directly in conjunction with the individual as his position changes.⁵³¹ Moreover, as the ability to electronically monitor individuals' locations en masse is a relatively new phenomenon, our understanding as to the extent citizens perceive it inhibits the realization of their fundamental rights is limited. This impediment in turn also reinforces the premise that citizens themselves might not fully comprehend the scope of the tracking of their location, and thus are constrained in their ability to reason and make decisions, which constitutes the primary basis for informed consent.

5. Purpose limitation versus inferential determination

As has been illustrated thus far, IoT may generate a large volume of location data that, when processed using current data mining techniques or combined with other data furnished, can be utilised to develop new inferences relating to the data subject. These secondary uses may constitute a repurposing⁵³² of the personal data originally collected. With the generation of vast amounts of location data by certain IoT devices the propensity toward repurposing data is potentially very great.⁵³³ The processing of data relating to location and movement for secondary purposes is of particular significance where the use of discrete sensors such as accelerometers and gyroscopes (which are now almost ubiquitous in most modern smartphones, for example) allows for an unprecedented volume of supplementary information relating to the individual data subject to be inferred using data analytics.⁵³⁴ Furthermore, the phenomenon of

⁵³¹ As regards the former, technological developments now allow for parties to install fixed systems that can actively monitor an individual's movements prior to initiating any form of process pertaining to the accession of consent. *See*, for example: Bruno, R. and Delmastro F., Design and analysis of a Bluetooth-based indoor localisation system, Personal Wireless Communications Lecture Notes in Computer Science, Volume 2775, 2003, pp. 711-725

⁵³² *Note*: 'Data reuse' refers to the "taking of a data asset and using it more than once for the same purpose", whereas 'data repurposing' refers to the "taking of a data asset previously used for one (or more) specific purpose(s) and using that data set for a completely different purpose". *See*: 'Data Governance and Quality: Data Reuse vs. Data Repurposing' in David Loshin, The Practitioner's Guide to Data Quality Improvement, 2010, Morgan Kaufmann Series on Business Intelligence, p.349

⁵³³ *See, also*: Wenkart M., The Internet Of Things, 2014, p.45

⁵³⁴ The WP29 has highlighted the particular risks associated with combining data from various sensors, known as 'sensor fusion'. The expert group notes that whilst the approach aims at providing better and more precise information than would be possible when sources are working in isolation, nonetheless

‘sensor fusion’ dictates that the data collected by two disconnected devices can, when combined, be utilised to develop information and provide greater insight than would be possible with the data furnished by either device in isolation.⁵³⁵ The combination of data sources may reveal unexpected inferences; for example where location data is analyzed in conjunction with measurements of an individual’s heart rate and respiration, potentially yielding detailed information relating a person’s physical state vis-à-vis their locality and environment.⁵³⁶ As such, a sensor in a consumer device collecting location data (for example, a personal health monitor or vehicle ‘black box’ event recording device) can collect data that may be processed for many purposes beyond that particular sensor’s intended original use or context.⁵³⁷

Indeed, the challenges presented by the repurposing of data are amplified by the increased collection of data implicit to the IoT environment, as the use of data for purposes in addition to those originally specified is more serious a consideration where sensing and monitoring capabilities proliferate. Furthermore, repurposing of data may be contemplated prior even to the initial collection of data. The concern has been raised that public authorities, in particular law enforcement authorities, may seek access to data collected by other parties for specified purposes: a 2013 briefing paper to the EU Commission on IoT underscored how such activity might potentially

research to date has thus far identified that it carries substantial risks to data quality. *See*: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.7

⁵³⁵ Research conducted by computer scientists has evidenced how data provided by accelerometers and gyroscopes (sensors which can measure an individual’s simple movements) can be combined with location data to infer a person’s physical activity. A person’s psychological mood (such as agitation) may even be associated with a certain space or environment, based on the processing of this personal data. *See, for example*: David L. Hall & James Llinas, An Introduction to Multi-sensor Data Fusion, 85 PROC. IEEE 6, 6 (1997); Richard Beckwith, Designing for Ubiquity: The Perception Of Privacy, IEEE Pervasive Computing, Apr.–June 2003, pp.40,43; Kaivan Karimi, The Role Of Sensor Fusion And Remote Emotive Computing (Rec) In The Internet Of Things 6–7 (2013), Available at <http://perma.cc/FP82-HK55>.

⁵³⁶ Peppet S. R., Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Vol. 93 Texas Law Rev. 85, Available at: <http://www.texasrev.com/wp-content/uploads/Peppet-93-1.pdf>, p.93

⁵³⁷ It has been noted that IoT sensor data are so rich, accurate, and fine-grained that data from any given sensor context may be valuable in a wide variety of different information contexts. In this context, Peppet asserts: “The technical problem created by the Internet of Things is that sensor data tend to combine in unexpected ways, giving rise to powerful inferences from seemingly innocuous data sources... in a world of connected sensors, everything may reveal everything.” *See*: Peppet, S.R., 2014. Regulating the Internet of things: first steps toward managing discrimination, privacy, security and consent. Tex. L. Rev., 93, p.119

violate individuals rights to privacy and the protection of their personal data, and in addition impact more widely the public's social acceptance of such technologies.⁵³⁸

One of the difficulties though for stakeholders wishing to understand the appropriate application of the data protection legal framework is the confusion caused by the use of inappropriate terms. Key concepts in understanding the impact of IoT on the collection and processing of location data are rendered more opaque where experts such as the WP29 employ rather cryptic language to develop key concepts. For example, referring to location and movement data collected by IoT devices the WP29 suggests that data processing may “derive inferences from such ‘raw’ information”; and “rely on sophisticated algorithms to extract *sensible* information”. The WP29 opinion is unhelpful where it can be seen to conflate a number of critical terms, including ‘data’ and ‘information’.⁵³⁹ Furthermore, the idea of “sensible information” being provided by algorithmic processing appears equally misplaced. Finally, the distinction made between ‘levels of data’ (“whether raw, extracted or displayed data”) is perturbing; the separation made here between the three types requires clarification if the distinction is to be upheld.⁵⁴⁰

6. Discriminatory effects: ubiquitous location data collection and processing

The collection and processing of location data also risks revealing intrusive insights into patterns of an individual's behaviour that could be used in developing individual profiles; detailed and unique aspects of a person's habits, behaviours and preferences can be identified by processing the data made available by sensors, which in turn may

⁵³⁸ See: EU Commission, Factsheet on privacy, data protection and information security, March 2013, Available at: http://ec.europa.eu/information_society/newsroom, p.2

⁵³⁹ See: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, pp.7-8.

⁵⁴⁰ Fundamental principles relating to the sharing of information based on the acquisition of data are explored in more detail by Evans's analysis of communication, which describes how data constitutes the constituent component processed into information. Evans states: “This and other sources of information come together to form knowledge. In the simplest sense, knowledge is information of which someone is aware.” See: Dave Evans, Cisco Internet Business Solutions Group, *The Internet Of Things: How The Next Evolution Of The Internet Is Changing Everything*, (2011), Available at: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, p.6

foster significant profiling capabilities.⁵⁴¹ Such a trend could constitute a threat to individual freedom to act independently of their volition, and possibly also institute changes in citizens' behaviours.⁵⁴²

Apposite to our appraisal of the scope of any interference into Article 8 of the ECHR are the deliberations of the Court in the case *Smirnova v. Russia*, the judgment of which provides guidance as to the scope of protections afforded to private life. The Court appraised the notion that 'private life' maintains a broad ambit, and that this encompasses the protection of "the moral and *physical* integrity of the individual, including the right to *live privately, away from unwanted attention*. It also secures to the individual a *sphere within which he or she can freely pursue the development and fulfilment of his personality*."⁵⁴³ The Court's assessment underscores the premise that a constituent feature of the fundamental right to privacy is the requirement that uninvited and intrusive attention inhibits a person's capacity to form their own identity; this assertion would thus support the notion that the use of location data for the purposes of profiling a person's movements would likely constitute an interference in the private life of the individual concerned.

⁵⁴¹ The WP29 has warned of further risks the use of data analytics present in relation to data collection and processing by IoT, affirming: "information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behaviour patterns". See: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.8

⁵⁴² De Hert has asserted in this context that 'behaving normal' will be the eventual corollary of the implementation of pervasive monitoring, stating: "Both governments and private actors will monitor us and assess our behaviour continuously in order to fit us into new idem identities that we cannot control and that we are often not aware of." See: De Hert, P., 2008. A right to identity to face the Internet of Things? Available at: www.portal.unesco.org, p.5. An often-overlooked aspect of Bentham's invention of the Panopticon is the premise that the creation would engender behaviour change; those placed in the cells could be observed at any point in time. Bentham calculated that, even where observation at any one point might be down to chance, the prospect alone of being monitored could induce conformity, and thus instill obedience in the party subject to surveillance. See: Bentham J., 1787 (Verso 1995), Letter V, in *The Panopticon Writings*, p.43. In its Opinion on Geolocation services on smart mobile devices the WP29 noted that the profiling of behavioural patterns raised important privacy concerns, particularly as regards the data collected and processing by such devices could constitute special categories of data, subject to additional safeguards under existing data protection laws. The WP29 asserted: "A behavioural pattern may also include special categories of data, if it for example reveal visits to hospitals and religious places, presence at political demonstrations or presence at other specific locations revealing data about for example sex life. These profiles can be used to take decisions that significantly affect the owner." See: WP29, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN WP 185, 16 May 2011, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, p.7

⁵⁴³ *Smirnova v Russia* (Apps No 46133/99; 48183/99) ECHR 24 July 2003, §95. Note: *emphasis added*.

Interference with the right to privacy may prove a more serious concern where proximate devices (e.g. wearable units) are effectively able to perform monitoring of individuals in the most personal spheres of private life, such as within the home.⁵⁴⁴ In *Mikulić v. Croatia* the Strasbourg Court reiterated that Article 8 of the ECHR protects not only “family” but also “private” life. Private life, the Court held “includes a person’s physical and psychological integrity and can sometimes embrace aspects of an individual’s physical and social identity.”⁵⁴⁵ The Court’s affirmation as to the scope of the protection given a person’s private life, particularly as regards their psychological integrity needs contextualizing in respect of our consideration of the consequences that monitoring of a person’s movements might have. In this regard the Court’s reaffirmation that respect “for ‘private life’ must also comprise to a certain degree the right to establish relationships with other human beings” is also pertinent.⁵⁴⁶ Both points broadly inhere the notion that the formation and development of a human’s personal integrity requires that a degree of shelter be given one’s personal sphere from the pernicious effects of surveillance.

Furthermore, In *Moreno Gómez v. Spain* the Court expounded the meaning of Article 8 of the Convention in terms of the individual’s right to respect for his private and family life, his home and his correspondence. It asserted that, as regards a person’s home, the right to respect of the home is “not confined to concrete or physical breaches, such as unauthorised entry into a person’s home, but also include those that are *not concrete or physical*, such as noise, emissions, smells or *other forms of interference*.”⁵⁴⁷ In the light of this finding, then, one can reasonably assert too that other forms of non-physical interference, such as monitoring that could inhibit and constrain a person’s psychological integrity, will also impair the enjoyment of their

⁵⁴⁴ A significant concern is the assertion that monitoring of this nature could encourage individuals to adopt behaviours perceived as ‘more normal’ of citizens and refrain from abnormal or ‘non-usual’ behaviours so as to obfuscate or prevent detection of perceived anomalies in their activities and actions. Such an effect could prove highly intrusive to a person’s private life and severely inhibit intimacy and aspects of an individual’s identity linked to self-expression. Indeed, this risk was highlighted as especially grave a concern in the WP29’s most recent guidance on IoT, in which the advisory body asserts that the development of such a tendency should be “very closely monitored” so as to avert potential interferences in the fundamental rights of data subjects. *See*: WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.8

⁵⁴⁵ *Mikulić v. Croatia*, ECHR, No. 53176/99, 7 Feb. 2002, §52-5

⁵⁴⁶ *Mikulić v. Croatia*, ECHR, No. 53176/99, 7 Feb. 2002, §52

⁵⁴⁷ *Moreno Gómez v. Spain*, Application no. 4143/02, 16 November 2004, §53

private and family life where they reasonably expect that their conduct shall be free from outside interference.⁵⁴⁸

In the *Ryneš* case⁵⁴⁹ the ECJ reaffirmed its earlier articulations as to the interpretation of Directive 95/46/EC, stating that it is intended to ensure a *high level of protection* of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data, citing specifically the provisions contained within Article 1 of the Directive and recital 10. The Court further stated that the protection of the fundamental right to private life guaranteed under Article 7 of the Charter of Fundamental Rights requires that “derogations and limitations in relation to the protection of personal data must *apply only in so far as is strictly necessary*.”⁵⁵⁰

Of interest in our consideration of the use of IoT devices therefore is the question of how the household exemption might apply in the context of increasing use of embedded networked sensors in relation to data processing. In *Ryneš* the ECJ noted that the exception provided for by Article 3(2), whereby the “Directive shall not apply to the processing of personal data: by a natural person in the course of a purely personal or household activity”, must be narrowly construed.⁵⁵¹ However, the subsequent clarification of the aforementioned point made by the Court in the *Ryneš* judgment is rendered all the more interesting in terms of its choice of language employed. Specifically, the Court noted:

“The fact that Article 3(2) of Directive 95/46 falls to be narrowly construed has its basis also in the very wording of that provision, under which the directive does not cover the processing of data where the activity in the course of which that processing is carried out is a ‘purely’ personal or household activity, that is

⁵⁴⁸ See, also: *Alkaya v. Turkey*, judgment of 9 October 2012 (application no. 42811/06), §29, in which the Court further reiterated that Article 8 protected the individual’s right to respect for his or her home, meaning not just the right to the actual physical area, but also to the quiet enjoyment of that area. Accordingly, breaches of the right to respect of the home included those that were not concrete or physical.

⁵⁴⁹ Case C-212/13, *Ryneš* ECLI:EU:C:2014:2428

⁵⁵⁰ Case C-212/13, *Ryneš* ECLI:EU:C:2014:2428, §§27-28.

⁵⁵¹ Case C-212/13, *Ryneš* ECLI:EU:C:2014:2428, §29.

to say, not simply a personal or household activity.”⁵⁵²

As such we need consider the extent to which a multitude of different activities might be construed where the distinction is drawn between “purely” and “simply” personal or household activities. This differentiation would appear somewhat difficult to determine, where it is not immediately apparent upon what basis such activities might be delineated. The difficulty in transposing the reasoning of the ECJ in relation to the operation of video surveillance in the home, where it covers even partially a public space “and is accordingly directed outwards from the private setting of the person processing the data in that manner”, is that the inherent diversity and complexity of networked IoT systems may render such distinctions difficult to satisfactorily resolve. In essence, the notions of ‘public space’, ‘private setting’, and indeed surveillance which is “directed outwards” can become rather opaque; the question at hand again is one of agency, and reflects the fact that sensing technologies are evolving in such a manner that classifying a person’s activity on the basis of binary distinctions, inferring that one can categorize a ‘purely personal or household activity’ from a ‘simple personal or household activity’, will likely prove problematic.⁵⁵³

It must also be noted however that the ruling subsequently acknowledges that the application of Directive 95/46/EC allows for exemptions where appropriate; in this respect it could be argued that the operation of devices and networks could engage the provisions that allow for the protection of the legitimate interests of the data controller pertaining to, for example, his health and life of his family. The ECJ affirmed: “At the same time, the application of Directive 95/46 makes it possible, where appropriate, to take into account — in accordance, in particular, with Articles 7(f), 11(2), and 13(1)(d) and (g) of that directive — legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the case in the main proceedings.”⁵⁵⁴

Personal location data collection and processing by IoT requires further examination in respect of data as a proxy for information relating to different aspects of personal

⁵⁵² Case C-212/13, *Ryneš* ECLI:EU:C:2014:2428, §30.

⁵⁵³ Case C-212/13, *Ryneš* ECLI:EU:C:2014:2428, §35.

⁵⁵⁴ Case C-212/13, *Ryneš* ECLI:EU:C:2014:2428, §34.

behaviour, and whether this may facilitate discriminatory practices.⁵⁵⁵ Linked to this characteristic of location data is the issue of the possible concealment of illegitimate or unlawful discrimination behind proxies; bias may be embedded in complex algorithms or hidden within vast datasets, which make the detection of such discrimination extremely burdensome. Knowledge of positive correlations between factors, such as an individual's location and other attributes, may outwardly appear neutral, but can be exploited to mask the discriminatory outcomes of data processing. In this respect it may be especially difficult to determine whether a chosen factor is exploited for profiling on a legitimate basis, or whether it constitutes a pretense for unlawful discriminatory treatment of individuals or groups.⁵⁵⁶ Considered together, information pertaining to physical location, mobility and micro-scale movements of the data subject can provide the observer with considerable insight into the habits and exploits of the individual.

It is imperative therefore to analyze how specifically the collection and processing of location data may constitute a decisive component in developing the capability to create and access a highly nuanced, personalized profile of the individual data subject.⁵⁵⁷ The widespread deployment of sensing devices permits data collection allowing for further processing that enables profiling of citizens on a level heretofore unimagined, reflecting the comprehensiveness of the detail comprised by the data. What may initially appear relatively benign differentiation, based on the use of

⁵⁵⁵ Dwork and Mulligan's research has highlighted the role of algorithms in linking disparate personal data, proxies and developing value judgments through data analytics; their studies underscore how the impact of the ascription of data points to actions influences processes in data analysis, and subsequently the determination of value judgments by such activities. Their research has highlighted how the selection of algorithms influences the formation of value judgments in profiling, and may lead to discrimination or the marginalization of specific populations, and the potential to divide and sort the population through narrowcasting such that it undermines the shared public sphere. *See*: Cynthia Dwork & Deirdre Mulligan, *Aligning Classification Systems with Social Values through Design*, 2012, Available at: <http://privacylaw.berkeleylawblogs.org/2013/05/23/cynthia-dwork-deirdre-k-mulligan-aligning-classification-systems-with-social-values-through-design/>

⁵⁵⁶ *See*: Tene, Omer and Polonetsky, Jules, *Judged by the Tin Man: Individual Rights in the Age of Big Data* (August 15, 2013), *Journal of Telecommunications and High Technology Law*, Forthcoming. Available at: <http://ssrn.com/abstract=2311040>, p.7

⁵⁵⁷ Research has shown for example that existing sensors in mobile devices can be used to infer a user's exercise levels and types of physical activity or movement. *See*: Shoaib, M.; Scholten, H.; Havinga, P.J.M., "Towards Physical Activity Recognition Using Smartphone Sensors," *Ubiquitous Intelligence and Computing*, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), pp.80-87; Anjum, A.; Ilyas, M.U., "Activity recognition using smartphone sensors," *Consumer Communications and Networking Conference (CCNC)*, 2013 IEEE, pp.914-919; Dernbach, Stefan; Das, B.; Krishnan, Narayanan C.; Thomas, B.L.; Cook, D.J., "Simple and Complex Activity Recognition through Smart Phones," *Intelligent Environments (IE)*, 2012 8th International Conference, pp.214-221.

location data in conjunction with individuals' other types of personal data, may constitute an intrusive form of individual profiling in which new and invidious types of discrimination may challenge existing safeguards to citizens' fundamental rights.

However, from the outset one needs recognize too that constructive discrimination can occur in a value-neutral sense, based on detailed appraisal of distinctions made on the bias of an almost infinite number of differences that exist in individuals' characteristics, preferences and activities.⁵⁵⁸ Notwithstanding this concession, differentiations based on the analysis of personal data will prove problematic where there exists no coherent means by which automated processing can algorithmically distinguish between lawful and non-lawful discrimination. Furthermore, it is important to recognize that discrimination may be either direct or indirect. In data analysis direct discrimination can occur when decisions are made in connection to sensitive attributes (whether the prejudice or bias is acknowledged or not), whilst indirect discrimination occurs when decisions are made based on non-sensitive attributes that are strongly correlated with biased sensitive ones.⁵⁵⁹

The processing of personal data in connection with the identification of an individual's location could result in unlawful discrimination on the basis of grounds such as gender, race, colour and religion.⁵⁶⁰ In connection with the particular

⁵⁵⁸ The Oxford Dictionary takes discrimination in this sense to mean "the recognition and understanding of the difference between one thing and another." In contrast, discrimination may also constitute prejudicial treatment which involves denying opportunities to members of one group in favour of other groups." *See*: Oxford Dictionaries online, Available at: <http://www.oxforddictionaries.com/>. In this context Tene and Polonetsky have highlighted how the meaning of the term "discrimination" has become highly charged; the data mining of personal data collected by IoT sensors could be legitimate, where we may overlook the fact that entirely reasonable distinctions that differentiate and discriminate between persons may be justifiable, noting: "In our daily life, we draw distinctions (i.e., discriminate) all the time. A person sitting next to us on a plane is tall or short, agitated or relaxed, attractive or unattractive, young or old – there is an endless list of such adjectives; and our attitudes and actions towards that person will vary accordingly." *See*: Tene, Omer and Polonetsky, Jules, *Judged by the Tin Man: Individual Rights in the Age of Big Data* (August 15, 2013), *Journal of Telecommunications and High Technology Law*, Forthcoming. Available at: <http://ssrn.com/abstract=2311040>, p.4

⁵⁵⁹ Indeed, in this regard efforts to determine whether and how statistical analysis may allow patterns of discrimination to be discovered in datasets is only at an early stage of research. *See*, for example: P. Priya & Dr. J. C. Pamila, *Discrimination in Data Mining*, Available at: <http://www.europment.org/library/2014/venice/bypaper/OLA/OLA-19.pdf>, pp.1-7; Salvatore Ruggieri, Dino Pedreschi & Franco Turini, *Data Mining for Discrimination Discovery*, May 2010, 4(2) *ACM Transactions On Knowledge Discovery From Data*, Article 9.

⁵⁶⁰ *See*: Peppet S. R., *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, Vol. 93 *Texas Law Rev.* 85, Available at: <http://www.texasrev.com/wp-content/uploads/Peppet-93-1.pdf>, p.117

contribution location data may perform in respect of generating enhanced profiles, analysts have underscored the considerable risks associated with monitoring and surveillance that IoT may represent.⁵⁶¹ In its 2014 Opinion on the Recent Developments on the Internet of Things, the WP29 expert group highlighted the need to consider its review in conjunction with earlier findings on the application of the concepts of necessity and proportionality and data protection in law enforcement (WP211) and on surveillance (WP 215).⁵⁶² Where it has been suggested by specialists that these technological advancements may risk being further developed in an uncontrolled manner, absent the safeguards necessary to protect fundamental rights, we need consider whether the existing legal framework is indeed apt to ensure the requisite level of protection to individuals.⁵⁶³

7. Conclusions

The challenges inherent to applying existing safeguards to fundamental rights to the development of IoT were acknowledged from the outset.⁵⁶⁴ Currently, IoT consists of

⁵⁶¹ The reflections provided by the WP29 on IoT are especially apposite in that agencies such as the EDPS asserted at the early stages of development of IoT that the expert group's interpretation and guidance on the application of existing laws and principles would constitute a requisite for sustaining a coherent approach. *See*: EDPS, Internet of things: ubiquitous monitoring in space and time, European Privacy and Data Protection Commissioners' Conference Prague, Czech Republic, 29 April 2010, Available at:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Internet_Things_EN.pdf, p.7

⁵⁶² *See*: WP29, Opinion 01/2014 on the "Application of necessity and proportionality concepts and data protection within the law enforcement sector", 536/14/EN WP 211, 27 February 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf; WP29, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN WP 215, 10 April 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

⁵⁶³ For example, the WP29 has warned that the fundamental rights of citizens of the EU are at stake; it contends that the development of IoT raises "new and significant personal data protection and privacy challenges" that "could go as far as develop a form of surveillance of individuals that might be considered as unlawful under EU law." The WP29 further cautions that IOT raises important security concerns, where security breaches could entail significant privacy risks for the individuals whose data are processed in such contexts." WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p.4

⁵⁶⁴ In this context the EDPS, for example, affirmed that the combination of technological developments with "new global realities" rendered applying the existing legal principles pertaining to data protection particularly challenging, principally on the basis that Directive, it believed, had not accounted for such eventualities. Indeed, in this respect, rather curiously it asserted that such challenges might only partially "be solved by interpretation and flexibility." *See*: EDPS, Internet of things: ubiquitous monitoring in space and time, European Privacy and Data Protection Commissioners' Conference

a loose connection of disparate networks, though in time this will evolve such that greater organisation will allow far more powerful analytics and data-mining capabilities: in effect, a ‘network of networks’.⁵⁶⁵ A fundamental difficulty this ubiquity generates is that with data processing so pervasive, based on this proliferation of sensing capabilities into the most trivial of appliances and every day practices, it becomes ever more difficult to discern both where and how each individual’s personal activities are subject to data processing. As such the need to comprehend the challenges this presents to the protection of citizens’ fundamental rights to privacy and personal data protection remains critical.⁵⁶⁶ At the heart of the concept of IoT is the notion that ‘embedded intelligence’ in individual items detects and processes data relating to changes in their physical state.⁵⁶⁷ It is this ambient, pervasive perceptivity that distinguishes IoT in its capacity to perform surveillance of individuals on an unprecedented level, particularly as concerns its ability to monitor responses to environmental factors.⁵⁶⁸

With IoT the current inability for the data subject to gauge data quality has clearly been identified as problematic. This rudimentary shortfall in capability is significant considering claims being made of location-tracking technologies and their potential to provide complex renderings of human mobility. Guarantees of ever improving acuity

Prague, Czech Republic, 29 April 2010, Available at:
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Internet_Things_EN.pdf, p.6

⁵⁶⁵ See: Dave Evans, Cisco Internet Business Solutions Group, *The Internet Of Things: How The Next Evolution Of The Internet Is Changing Everything*, (2011), Available at:
http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, p.4

⁵⁶⁶ Indeed, the former EU Commissioner for the Digital Agenda Neelie Kroes has asserted that the Internet of Things “is surrounded by a value system: as it comes so close to the heart of everyday life, social relations and daily services, it needs a broad societal consensus to fulfill its potential”, thus reaffirming the concern that the collection and processing of personal data relating to highly intimate aspects of citizens lives could portend enormous impacts on the rights to privacy and data protection. See: *The 2nd Annual Conference Internet of Things Europe 2010 Conference Report, A Roadmap for Europe*, Held on 1st and 2nd of June 2010, Brussels, p. 2.

⁵⁶⁷ FTC, #484: FTC Seeks Input on Privacy and Security Implications of the Internet of Things, Available at: <http://www.ftc.gov/policy/public-comments/initiative-484>, p.13

⁵⁶⁸ The EDPS highlighted at an early juncture in the evolution of IoT the inherent challenges to privacy and data protection presented by an environment in which every single action of objects and individuals can be monitored from a spatial and temporal perspective, reflecting what the agency foresaw as a “lack of ‘natural’ limits which were preserving the privacy of the data subject so far.” As such, the issue arises as to how effective limits may in fact be set in order that the availability of this powerful monitoring capability may be regulated effectively. See: EDPS, *Internet of things: ubiquitous monitoring in space and time*, European Privacy and Data Protection Commissioners’ Conference Prague, Czech Republic, 29 April 2010, Available at:
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Internet_Things_EN.pdf, p.3

in detection and monitoring, coupled with assurances as to the increasing reliability of progressively more detailed deductions made on the basis of the analysis of location data, should be treated with caution. This technical deficiency is important where we consider the reliability of inferences drawn from the analysis of location data vis-à-vis the acuity of such deductions; assertions need acknowledge the reliability of assumptions based on the potentially inaccurate algorithmic determinations made in the processing of location data. This point is particularly pertinent where developers of IoT rarely discuss publicly such deficiencies in data quality pertaining to both collection and processing.

It should be recalled that IoT devices and services are still very much in the early stages of maturation, and that the viability of its advantages for society remains open to debate. It is crucial therefore that we take sufficient care to examine how the existing scope of protective safeguards is best applied based on an objective elucidation of the functionality inherent to the technologies. In this respect, the guidance of the WP29 at times unfortunately rarely reflects such an approach: rather its assessments explaining the application of the current legal framework are conspicuous for the confusing non-sequiturs that frequently appear.⁵⁶⁹ We must avoid unwittingly jumping to conclusions based upon ‘worse case’ type scenarios in which the most probable use of technologies in given scenarios, based upon emerging trends, is disregarded in favour of plotting speculative projections that promise more

⁵⁶⁹ An example being where WP29 explains that pervasive services *need* to be provided in an unobtrusive manner, such that this should require inevitably as a result data processing being conducted by a third-party: “As a *result* of the *need to provide pervasive services* in an unobtrusive manner, users *might in practice find themselves under third-party monitoring*. This may result in situations where the user *can lose all control* on the *dissemination* of his/her data, *depending on whether or not* the collection and processing of this data will be made in a *transparent manner or not*.”⁵⁶⁹ Furthermore, the use of the term “dissemination” so as to refer to both data collection and processing is, in respect of the terminology chosen, a rather disingenuous choice in this particular context. Thus consideration of the terminology employed in the definitions outlined by the Data Protection Directive is especially pertinent. Directive 95/46/EC Article 2(b) notes in respect of the definition of processing that dissemination should constitute but a part of processing as a whole: “processing of personal data’ (‘processing’) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;”.

hazardous, but relatively improbable, developments of IoT. The next chapter thus considers the implications of the application of IoT sensing capabilities in respect of the collection and processing of location data for the purposes of creating behavioristic profiles.

Chapter 6: Establishing and Developing Biometrics using Location Data

1. Introduction

As has been shown in the preceding chapters of this review, location data can be processed in such a way that it provides information relating to the data subject other than that which relates purely to temporal-spatial aspects of their behaviour or identity. Biometric data is a sphere of development pertinent to this phenomenon. This chapter explores how location data is increasingly being utilised in the creation of biometric identifiers that allow for the distinction between individuals based on different criteria linked to human movement.

Biometrics increasingly play a role in the implementation of new and emerging surveillance technologies aimed to improve security in face of threats to our society, and its use in this context is already established in many European countries.⁵⁷⁰ Growing attention is now being given to the implications of these developments.⁵⁷¹ Indeed, the concerns of the expert group WP29 were at an early juncture significantly high for it to assert that the use of personal data in this way inhaled specific challenges to the protection of fundamental rights, based on what it stated was its ‘special nature’, noting: “[Biometric] data is of a special nature, as it relates to the

⁵⁷⁰ The Practis FP7 project concluded in its final forward-looking report in 2011 that biometrics would play a greater role in surveillance of citizens, posing challenges in respect of the separation of private and public ‘spaces’: “In the coming years, this trend is expected to grow and the technologies will be used almost in all public environments, and in the far future, even in the private / personal space. It is quite obvious that large scale implementation of Biometric surveillance technologies is very problematic from the privacy point of view and should be dealt with.” *See*: Practis FP7, Privacy – Appraising Challenges to Technologies and Ethics, Deliverable D2.2: Final Horizon Scanning Report, July 2011, Available at: http://www.practis.org/docs/PRACTIS%20D2%20_130711final.pdf, p.22

⁵⁷¹ The WP29 noted in its first Opinion on biometric data that: “The rapid progress of biometric technologies and their expanded application in recent years necessitates careful scrutiny from a data protection perspective.” WP29, Working document on biometrics, 12168/02/EN WP 80, 1 August 2003, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/>, p.2.

behavioural and physiological characteristics of an individual and may allow his or her unique identification.⁵⁷²

The majority of research in the biometrics field has to date focused upon studying well-established physical biometrics such as iris scans and fingerprints. However, the increased sensitivity of embedded sensors, in conjunction with their greater ubiquity, have made integration of biometric technologies that collect location data into computing devices an attractive sphere for further innovation and development.⁵⁷³ The new systems being developed exploit physiological traits to allow for categorization and identification of individuals and the remote collection of personal location data upon which behavioural attributes may be modeled.⁵⁷⁴ The modelling of these attributes has been termed ‘behaviometrics’.⁵⁷⁵ *Mobile Behaviometrics*, a designation which stems from the terms “*mobile behaviour*” and “*biometrics*”, uses algorithms and models to measure and quantify the unique human behavioural patterns and natural rhythms that each user has when operating and interacting with their mobile device.⁵⁷⁶ The use of personal location data is particularly promising in

⁵⁷² See: WP29, Working document on biometrics, 12168/02/EN WP 80, 1 August 2003, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/>, p.2. Note: In its Opinion 4/2007 (WP136) the WP29 stated that biometric data may be defined as: “Special reference should be made here to biometric data These data may be defined as biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability.” See: WP29, Opinion 4/2007 on the concept of personal data, WP136, 20 June 2007, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/>, p.8

⁵⁷³ Indeed, technologists have cited that a distinct advantage for parties employing behavioural biometrics technologies is its cost effectiveness, based on the relative ease with which data collection and processing can be facilitated using networked devices with embedded sensors. See: Yampolskiy, R.V. and Govindaraju, V. (2008) ‘Behavioural biometrics: a survey and classification’, Int. J. Biometrics, Vol. 1, No. 1, pp.81-113. Available at: <http://cecs.louisville.edu/ry/Behavioral.pdf>, p.83

⁵⁷⁴ Behavioural-based techniques measure the behaviour of a person; methods thus far developed include those of keystroke analysis, gait analysis, way of walking or moving, and patterns that indicate aspects of an individual’s subconscious thought (e.g. lie detection). See: WP29, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, 27 April 2012, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/>, p.4

⁵⁷⁵ BehavioSec defines behaviometrics thus: “A human behavioural pattern consists of a variety of different unique “semi-behaviours”; all mixed together into a larger an utterly unique profile. Since every person’s unique behaviometric pattern is formed not only by biometric features, like the way you move your hand, but is also influenced by more social and psychological means, like if you are native in the language you write, it is just about impossible to copy or imitate somebody else’s behaviour...” See: BehavioSec, White Paper BehavioMetrics - A Paradigm Shift in Computer Security, February 2016, Available at: <https://www.behaviosec.com>, p.2.

⁵⁷⁶ See: Zhu, Jiang, “Mobile Behaviometrics: Behavior Modeling from Heterogeneous Sensor Time-Series” (2014). Dissertations. Paper 388. Available at: <http://repository.cmu.edu/dissertations/388>, p.3

the field of behaviometrics as strong, predictable patterns in individuals' mobility patterns make location data very useful as a passive factor for authentication.⁵⁷⁷

2. Biometric profiles conceptualized

Behavioural biometrics intend to quantify the behavioural traits an individual exhibits, which may then be used to verify identity or draw inferences from an analysis based on the profiling of others' measured behaviours.⁵⁷⁸ These new biometric technologies are now being extended for use from their original sphere of application, identification and authentication, to behaviour analysis - this is particularly the case in respect of surveillance and monitoring of populations.⁵⁷⁹ The personal data of citizens may be collected for the purposes of profiling and conducting remote surveillance.⁵⁸⁰

The development of novel forms of biometric identifiers based upon our movement patterns reflects a growing tendency in enhancing capabilities to examine, appraise and model personal behaviours that can be used to evaluate extremely intimate details of our personal identities.⁵⁸¹ Biometric technologies that allow for the identification and verification of individuals identities and behaviours based on the processing of precise personal location data constitute an experimental sphere of developing

⁵⁷⁷ See: Hayashi, E., Das, S., Amini, S., Hong, J. and Oakley, I., 2013, July. Casa: context-aware scalable authentication. In Proceedings of the Ninth Symposium on Usable Privacy and Security (p. 3). ACM, p.2

⁵⁷⁸ Brömme, A. (2003) 'A classification of biometric signatures', International Conference on Multimedia and Expo (ICME '03), p.1

⁵⁷⁹ See: WP29, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, 27 April 2012, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/>, p.16

⁵⁸⁰ The WP29 notes in this regard the role of the ongoing development of digital sensing capabilities that allow for the collection of personal data pertaining to newly recognised physiological characteristics that can be measured with increasing precision, and new methods to process traditional biometrics based on the enhanced computing and algorithmic capabilities being developed. See: WP29, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, 27 April 2012, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/>, pp.16-17.

⁵⁸¹ Van der Ploeg has highlighted concerns arising from the role the human body is increasingly playing in relation to the develop of information technology as a whole, asserting: "Rather than IT rendering the body irrelevant to identity – a mistaken idea to begin with – the coupling of biometrics with IT unequivocally puts the body center stage. The questions to be raised about biometrics are *how* bodies will become related to identity, and what the normative and political ramifications of this coupling will be. Unlike the body rendered *knowable* in the biomedical sciences, biometrics generates a *readable* body: it transforms the body's surfaces and characteristics into digital codes and ciphers to be 'read' by a machine." See: Van der Ploeg, I., The illegal body: 'Eurodac' and the politics of biometric identification, Ethics and Information Technology 1: 295–302, 1999. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.200.9254&rep=rep1&type=pdf>, p.295

information technology that raises key normative questions in respect of the relationship between the body and identity, and indeed how we conceptualize the notion of bodily integrity and the physical and mental dimensions of our right to privacy.⁵⁸² Therefore, of interest are the resultant effects for the protection of the individual's psychological integrity.⁵⁸³ In this respect, Reidenberg has argued that the treatment of personal information is an element of basic human dignity, asserting that: "Fair treatment of personal information accords respect to an individual's personality."⁵⁸⁴

A perceived advantage of behavioural biometrics in particular is that they may offer a number of distinct advantages over traditional biometric technologies; data can be collected less obtrusively and often without any additional special hardware.⁵⁸⁵ However, an immediate challenge presented by the 'non-obtrusiveness' that the use of

⁵⁸² It should be noted however that while spatial analysis utilizing geospatial technologies is increasingly being employed in forensics, thereby attesting to the technique's apparent utility, at present there exists a relative lack of published research qualifying its effectiveness. *See*: Elmes G.A., Roedl G. and Conley J. 'Concepts, principles and definitions' in Elmes G.A., Roedl G. and Conley J. (eds.) *Forensic GIS - The Role of Geospatial Technologies for Investigating Crime and Providing Evidence* (2014), Springer Publishing, London, p. 4

⁵⁸³ Interestingly, Sloot's scholarship has argued that we need appreciate the dimension of personality in respect of the harm interferences in the right to privacy may constitute, arguing that the protection of dignity and personal development as underlying rationales for the safeguard of privacy is rendered especially complex by the notion that these are "subjective rights due to their vague and unenforceable nature". *See*: Sloot, B.V.D., 2015. Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data'. *Utrecht Journal of International and European Law*, 31(80), p.28. *See also* Reiman's discussion of privacy as conceived as a right of an individual to control access to their person, including aspects of their expression of identity: Reiman, J.H., 1995. Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara Computer & High Tech. LJ*, 11, p.32. Levi and Wall assert in this context that there exists a risk of "data doubling" occurring, and of the resultant effect on a person's concept of their own identity, whereby "the organic body and its behaviour is abstracted by surveillant technological processes into a series of discrete data flows from the physical world." *See*: Michael Levi & David Wall, 'Crime and Security in the Aftermath of September 11: Security, Privacy and Law Enforcement issues relating to emerging information communication technologies' in 'Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)', July 2003, DG JRC, Available at: <http://www.jrc.es>, p.176. *See also*: De Mul, Jos. 2008. "Digitally mediated (dis)embodiment. Plessner's concept of excentric positionality explained for cyborgs." *Information, Communication & Society* 6: pp. 247-266.

⁵⁸⁴ Reidenberg, J.R., 1994. Setting standards for fair information practice in the US private sector. *Iowa L. Rev.*, 80, p.497. Similarly, De Hert's scholarship has also underscored the importance of understanding the risk posed by interferences to citizens' identities. In this context De Hert asserts: "Upholding identity is not only an issue of shielding persons against intrusions by governments and other actors, but also an issue of making identity formation possible." De Hert, P., 2008. A right to identity to face the Internet of Things? Available at: portal.unesco.org, p.13

⁵⁸⁵ *See, for example*: Cappelli, R., Maio, D., Maltoni, D., Wayman, J.L., and Jain, A.K. (2006) 'Performance evaluation of fingerprint verification systems', *IEEE Transactions on Pattern Analysis Machine Intelligence*, Vol. 28, pp.3-18; *See also*: Jain, A.K., Ross, A. and Prabhakar, S. (2004) 'An introduction to biometric recognition' *IEEE Trans. Circuits Systems Video Technologies*

behavioural biometrics frequently inheres is the possibility that personal data may be collected without the knowledge of the individual data subject.⁵⁸⁶ In *Biriuk v. Lithuania* the European Court of Human Rights emphasized the intrinsic value of the protection of a person's private life in allowing for their personal development, noting that its scope also encompassed a social dimension:

“As to respect for the individual's private life, the Court reiterates the fundamental importance of its protection in order to ensure the development of every human being's personality. That protection extends beyond the private family circle to include a social dimension.”⁵⁸⁷

In *Rotaru v. Romania* the Court reiterated its finding from earlier cases concerning surveillance of populations that citizens could legitimately claim that an interference in their Article 8 rights to privacy and family life had occurred even where they were unable to substantiate whether indeed they had been subject to a form of monitoring.⁵⁸⁸ In this respect, then, we might infer from established precedent that the mere existence of a register established by a public authority, such as a law enforcement agency, containing profiles based on biometric identifiers for crime prevention and investigation purposes could constitute an interference, regardless of whether or not it could be shown that an individual was a data subject.

In *Haramlambie v. Romania* the European Court of Human Rights also reaffirmed the precedent established in its jurisprudence that data of a notionally public nature may reveal aspects of a person's private life where it is systematically collected stored and in files held by a public authority, and that this applies even more so when such information concerns a person's distant past. The Court also reiterated the vital interest of the individual subjects of personal files held by public authorities to be

⁵⁸⁶ Yampolskiy, R.V. and Govindaraju, V. (2008) 'Behavioural biometrics: a survey and classification', *Int. J. Biometrics*, Vol. 1, No. 1, pp.81-113. Available at: <http://cecs.louisville.edu/ry/Behavioral.pdf>, p.82

⁵⁸⁷ *Biriuk v. Lithuania*, No. 23373/03, 25 November 2008, §38

⁵⁸⁸ The Court affirmed: "...as to the concept of victim, that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him (see the *Klass and Others v. Germany* judgment of 6 September 1978, Series A no. 28, pp. 18-19, § 34)." See: *Rotaru v Romania* (App No 28341/95), §35.

granted access, and further emphasized that the authorities had an obligation to provide an effective procedure for obtaining access to such information.⁵⁸⁹

In this context, therefore, the notion of bodily integrity is of foremost importance in our consideration of the possible interferences in the fundamental rights of individuals that such developments might constitute.⁵⁹⁰ Conceptually, bodily integrity inheres the idea that one's own distinctive selfhood, constituted by the unique characteristics that distinguish us from others, is innate and fundamental to our being. New technologies that exploit biometric capabilities intend to institute in digital form, through the collection and processing of performative elements of our behaviour, component of this identity that represent specific characteristics of the individual.⁵⁹¹ The performative nature of this method, its reliance open creating a distinctive temporospatial record of our presence and locomotion through space, is perhaps what renders this form of biometric identifier especially difficult for the layperson to conceive and appreciate its capabilities.⁵⁹²

⁵⁸⁹ See: *Haralambie v. Romania*, No. 21737/03, 27 October 2009, §77, §86. The Court earlier noted in the case *McGinley and Egan v. the United Kingdom* that under Article 8 of the Convention respect for private and family life “requires that an effective and accessible procedure be established which enables such persons to seek all relevant and appropriate information.” The Court further noted that given the applicants’ interest in obtaining access to the material in question and the apparent absence of any countervailing public interest in retaining it, the Court considers that a positive obligation under Article 8 arose.” See: *McGinley and Egan v. the United Kingdom*, (10/1997/794/995-996), 9 June 1998, §31.

⁵⁹⁰ The analysis of trends in wearable healthcare devices by Paredes et al indeed outlined significant concerns as to the invasiveness of these technologies, noting that: “Recent advancement in sensors and wireless technologies and related computational techniques have accelerated the push towards wearable healthcare devices capable of providing ambulatory monitoring of a variety of vital signs... Many of these vital signs are strongly linked with physiological changes induced by emotional arousal.” The risks inherent to these technological developments, and the concerns of citizens in possibly being subject to their use, have indeed been further acknowledged: “In spite of their growing availability, friction continues to exist in public adoption due to the intrusive nature of body periphery sensing.” See: Pablo Paredes, David Sun, John Canny, *Sensor-less Sensing for Affective Computing and Stress Management Technology*, December 2013, Available at: <http://bid.berkeley.edu/stressmanagement/wp-content/uploads/2013/12/sensorless-sensing.pdf>, p.2.

⁵⁹¹ The move toward ever-greater use of embedded sensors in everyday devices to conduct monitoring has prompted the observation by developers of behavioural health analytics that the technologies leverage such devices as: “automated diaries containing valuable insight into the mental well-being of people with mental illnesses.” The report highlighted that smartphones “produce significant behavioral data - such as location, calling and texting records, and app usage that map out a user’s daily patterns.” See: Matheson R., *Mental-health monitoring goes mobile*, MIT News, 16 July 2014, Available at: <http://newsoffice.mit.edu/2014/mental-health-monitoring-goes-mobile-0716>

⁵⁹² In this respect observers have noted an augmentation in sensing capabilities to discern in greater detail ever more intimate aspects of citizens’ lives, noting: “Exterior capta that render people’s lives transparent to outside organisations are now partially being complemented by interior capta, personal documentation of lives as they unfold, an internally self-produced autobiographical sousveillance.” See: Martin Dodge, Rob Kitchin, *CASA Working Paper 92, The ethics of forgetting in an age of*

3. Privacy and personal data protection challenges presented by biometric identifiers

Regarding the use of location data for the purposes of developing biometric identifiers that enables the distinguishing of different data subjects from one another and the creation of individual profiles, it is appropriate to reflect upon the basic founding principles that underpin the concept of personal data protection. In this context it should be noted that Recital 2 of Directive 95/46/EC is significant where it reaffirms the notion that a simple premise underpins the function of data processing, namely it operate in a favourable means whilst respecting fundamental rights: “data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress...”⁵⁹³

Regarding recent developments in the use of location data, in addition to the provisions made in Article 8 of the ECHR and Article 7 of the EUCFR with respect to the protection of the right to privacy, and Article 8 of the EUCFR in respect of the protection of personal data, we need also consider the safeguards established for the protection of citizens fundamental rights in the Data Protection Directive 95/46/EC and in Directive 2002/58/EC on privacy and electronic communications. Furthermore, we need also consider how perhaps less immediately discernible aspects of the individual’s right to private life and to personal data protection are engaged. In this context, therefore, discussion of the applicable provisions contained within the existing legal framework concerning sensitive health data need also be consulted. As such, in addition to the relevant stipulations made within Council of Europe Convention 108, the guidance given by Council of Europe Recommendation No. R(97) 5 on the protection of medical data also proves pertinent.⁵⁹⁴

pervasive computing, 1 March 2005, Available at:
<http://www.bartlett.ucl.ac.uk/casa/publications/working-paper-92>, p.6

⁵⁹³ Recital 2, Directive 95/46/EC

⁵⁹⁴ Council of Europe Recommendation No. R(97) 5 on the protection of medical data, 13 February 1997, Available at: <https://wcd.coe.int/>

3.1 Applying the principle of purpose specification

Observance of the requirement stipulated by Article 6 (a) of Directive 95/46/EC that personal data must be processed fairly and lawfully requires that the data collection itself should be achieved in a manner that is fair. As such, systems that collect data absent the knowledge of the data subject are unlikely to meet with this requirement.⁵⁹⁵ Article 6(b) of Directive 95/46/EC asserts that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.⁵⁹⁶ The European Union Charter of Fundamental Rights also clearly establishes the principle of purpose limitation, specifying that personal data must be processed “fairly for specified purposes”.⁵⁹⁷ Purpose specification and compatible use are however being subject to increasing scrutiny as regards their adaptability in the light of evolving technologies and the expansion of data processing activity.⁵⁹⁸ As the development of biometric identifiers based on the processing of personal location data is an emergent field, it thus proves challenging to draw upon precedents pertaining to established technologies. However, certain

⁵⁹⁵ Article 6(1)(a), Directive 95/46/EC:

1. Member States shall provide that personal data must be: (a) processed fairly and lawfully;

⁵⁹⁶ Article 6(1)(b)

1. Member States shall provide that personal data must be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

In this context the explanation provided by WP29 as to the degree of detail in which a purpose need be specified is somewhat oblique, where it affirmed this: “depends on the particular context in which the data are collected and the personal data involved.” See: WP29, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy/>, p.16.

Furthermore, in its Opinion on purpose limitation the WP29 noted with regard to a purpose being legitimate that this notion could be construed expansively, noting: “Legitimacy is a broad requirement, which goes beyond a simple cross-reference to one of the legal grounds for the processing referred to under Article 7 of the Directive. It also extends to other areas of law and must be interpreted within the context of the processing.” See: WP29, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy/>, p.39.

⁵⁹⁷ European Union Charter of Fundamental Rights, Article 8(2), Protection of personal data: “Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”

⁵⁹⁸ Indeed, in this context the expert group WP29 has alluded to this trend in its recent Opinion on purpose limitation, in which it noted: “However, even if the principle of purpose limitation itself seems stable, its precise meaning, including any exceptions to it, is now subject to discussion. The fact that purpose specification and legitimacy are two different and cumulative requirements, which is confirmed explicitly by Article 8 of the Charter, is challenged in the proposed Data Protection Regulation.” See: WP29, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy/>, p.11.

determinations in respect of the prior implementation of data processing of location data readily constitute a reasonable basis for our appraisal.⁵⁹⁹

WP29 noted in its Opinion on the use of location data with a view to providing value-added services that as “location data always relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in Directive 95/46/EC of 24 October 1995.” Furthermore, the expert group also noted that as the processing of such data is:

“A particularly sensitive matter involving the *key issue of the freedom to come and go anonymously*, the European legislature, taking into account the considerations of the European data protection authorities, has adopted specific rules requiring that the consent of users or subscribers be obtained before location data needed for supplying a value-added service are processed, and that users or subscribers be informed about the terms of such processing.”⁶⁰⁰

The WP29 also noted the application of the provisions within Article 9 of Directive 2002/58/EC of 12 July 2002. It would appear reasonable, therefore, to deduce from this statement that, should location data inhere autonomous movement, one might also reasonably deduce that data processing of location data to develop biometric identifiers also engages this provision.⁶⁰¹ Indeed, in respect of the service providers

⁵⁹⁹ The findings of WP29 in relation to the examination of the legal framework in the implementation of location-based services proves particularly apposite where we consider the broader principle of purpose specification and purpose limitation in particular. Indeed, the expert group provided an especially erudite and succinct elucidation of the intrinsic value of this principle to the protection of individuals’ fundamental rights in its published Opinion on the purpose limitation, in which it affirmed: “Specification of the purpose is a pre-requisite for applying other data quality requirements, including the adequacy, relevance, proportionality and accuracy of the data collected and the requirements regarding the period of data retention... When we share personal data with others, we usually have an expectation about the purposes for which the data will be used. There is a value in honoring these expectations and preserving trust and legal certainty, which is why purpose limitation is such an important safeguard, a cornerstone of data protection. Indeed, the principle of purpose limitation inhibits ‘mission creep’, which could otherwise give rise to the usage of the available personal data beyond the purposes for which they were initially collected.” See: WP29, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy/>, p.4.

⁶⁰⁰ See: Working Party 29, Opinion on the use of location data with a view to providing value-added services, 2130/05/EN WP 115, November 2005, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf, p.3.

⁶⁰¹ See: Working Party 29, Opinion on the use of location data with a view to providing value-added services, 2130/05/EN WP 115, November 2005, Available at:

providing value-added services, the WP29 later affirmed in its published Opinion document that: “In view of the very sensitive nature of the processing of location data, the Working Party would draw the attention of service providers to the need to provide clear, complete and comprehensive information on the features of the service proposed.”⁶⁰² Clearly, then, the expert group is in no doubt as to the importance of ensuring data subjects are adequately informed as to the scope of the processing to which their location data will be subject. Whilst the pronouncement is directed at service providers in this context, it can be inferred that the importance of providing safeguards to the protection of data subject’s personal location data for additional processing operations more widely is acknowledged. Taking these considerations into account, an assessment as to whether the collection and processing of biometric data meets with these requirements will facilitate the determination as to whether these principles have indeed been met. Moreover, this assessment should include a review of the risks such activity presents the safeguard of the fundamental rights of individuals, and whether as such the intended purpose might be achieved by a form of collection and processing that would prove less intrusive to the data subject, reflecting the need to evaluate the proportionality of such measures.⁶⁰³

The provisions pertaining to the data protection principle of legitimate purpose contained within Article 7 of Directive 95/46/EC are pertinent to our review of the development of soft biometrics based on processing of individuals’ location data. Of particular concern is the notion that the assessment of a person’s emotional state could become a primary objective of the systems being developed for deployment in public spaces; in this respect Article 7(f) of Directive 95/46/EC provides the necessary guidance as to the legitimacy of the purpose of processing this data, stating:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf, p.3. Note: *emphasis added*.

⁶⁰² See: Working Party 29, Opinion on the use of location data with a view to providing value-added services, 2130/05/EN WP 115, November 2005, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf, p.3.

⁶⁰³ Furthermore, an additional issue requiring examination is whether developing identifying profiles of individuals in this manner would constitute an ‘identifier of general application’ in accordance with Article 8(7) of Directive 95/46/EC. The development of biometric identifiers achieved by means of the data collection and processing of location data from electronic service providers, such as telecommunications network operators, would engage the provisions articulated within Article 8(7) of Directive 95/46/EC, according to the 2012 Opinion on developments in biometric technologies authored by WP29. See: WP29, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, 27 April 2012, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/>, p.9

“Member States shall provide that personal data may be processed only if: ‘processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).’”⁶⁰⁴

In *Mitkus v. Latvia* the Court noted that:

“...although the object of Article 8 of the Convention is essentially that of protecting the individual against arbitrary interference by public authorities, it does not merely compel the State to abstain from such interference. In addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life.”⁶⁰⁵

Moreover, in *K.H. and Others v. Slovakia* the Court held that the positive obligations of the State concerning the protection of personal data extended to the “making available to the data subject of copies of his or her data files.” The Court made a further additional important declaration in elucidating its position on data subject access rights, noting it: “does not consider that data subjects should be obliged to specifically justify a request to be provided with a copy of their personal data files. It is rather for the authorities to show that there are compelling reasons for refusing this facility.”⁶⁰⁶ In this regard, therefore, it is reasonable to suggest that the scope of positive obligations might extend to the State providing sufficient safeguards in its oversight of data controllers and processors to ensure that data subjects are afforded sufficient protection where biometric identifiers are developed using an individual’s personal data.⁶⁰⁷

⁶⁰⁴ Article 7(f), Directive 95/46/EC. Thus in this context we need also note that Article 1(1) affirms: “...Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.” Article 1(1), Directive 95/46/EC.

⁶⁰⁵ *Mitkus v. Latvia*, judgment of 2 October 2012 (no. 7259/03), §125.

⁶⁰⁶ *K.H. and Others v. Slovakia*, No. 32881/04, 28 April 2009, §§47-48.

⁶⁰⁷ *Mitkus v. Latvia*, judgment of 2 October 2012 (no. 7259/03), §125. The Court, citing its earlier judgment in *Appleby and Others v. the United Kingdom*, no. 44306/98, § 41, ECHR 2003-VI, noted

4. The challenge of repurposing location data

With regard to repurposing of data, the WP29 has noted the applicability of Article 6(b) in the context of biometric data in respect of the requirement that personal data collected must be: “specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.” The WP29 provides as an example an instance where biometric data are processed for access control purposes, and that the use of such data to assess the emotional state of the data subject or for surveillance in the workplace would not be compatible with the original purpose of collection. As such, it asserts: “all measures must be taken to prevent such incompatible re-use.”⁶⁰⁸ The concern therefore is one of the proportionality of the data collection and processing taking place, taking into consideration the requirement that personal data must be: “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.”⁶⁰⁹ More recently, in the *Google Spain* case heard at the ECJ⁶¹⁰, the court again affirmed the need for deliberation so as to consider how data processing may evolve in the course of time, and how processes might be interpreted in the light of the legal instruments’ provisions with respect to the processing of personal data, noting: “It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light

that: “What this means is that the Court will need to determine whether the respondent State failed to protect the applicant’s Article 8 rights from interference by other individuals.” Providing further elucidation, the Court however reiterated that the States maintain a wide margin of appreciation in determining the steps to be taken to ensure compliance with the Convention, noting: “such positive obligations, the notion of “respect” for private life is not clear-cut. In view of the diversity of the practices followed and the situations obtaining in the Contracting States, the notion’s requirements will vary considerably from case to case.” See: *Mitkus v. Latvia*, judgment of 2 October 2012 (no. 7259/03), §127.

⁶⁰⁸ See: WP29, Working document on biometrics, 12168/02/EN WP 80, 1 August 2003, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/>, p.7. A further concern in respect of the repurposing of data has also been expressed in that the storage of biometric data may increase the risk of data mining, whereby different databases, both in the public and in the private sector, are interconnected and exploited with the objective of creating detailed profiles of an individual's habits. See: WP29, Working document on biometrics, 12168/02/EN WP 80, 1 August 2003, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/>, p.7.

⁶⁰⁹ Article 6(c), Directive 95/46/EC

⁶¹⁰ *Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014

of the purposes for which they were collected or processed.”⁶¹¹

The principal difficulty therefore is that of determining how to appropriately ascertain the scope of such conceptions as ‘relevant’ and ‘not excessive’ as they apply to the context of evolving biometrics indicators, particularly in respect of the rather intangible notion of ‘soft biometrics’, which to an extent may prove even more complex to determine.⁶¹² The generation of biometric identifiers using personal data inheres the potentiality to expose sensitive information pertaining to the individual. Researchers have established connections between biometric identifiers and information pertinent to health, ethnicity and heredity.⁶¹³ Whilst these correlations are not determinative (i.e. the correlations do not *per se* afford scope to predict an attribute; rather, correlations between different factors may prove indicative of traits that can be observed in patterns), which therefore still allows scope to discriminate based on selected criteria. As such, this capability presents challenges to the protection of the fundamental rights, where the correlation between ancillary or supplemental human attributes correlating to selected biometric identifiers could be subject to misuse. These additional traits, which complement personal information related to primary biometric identifiers used principally to distinguish different persons from one another by way of biometric recognition, have been termed “soft biometrics”.⁶¹⁴ ‘Soft biometrics’ determined from location and movement data relating to a person’s individual patterns of mobility may include, for example, body characteristics that reflect age, physical impairments or disabilities (e.g. visual or locomotive conditions), and body weight.⁶¹⁵ Increases in both the precision and quantity of location data collected will guide the transformative power of soft

⁶¹¹ Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014, para. 93

⁶¹² Read et al define soft biometrics as: “traits can be typically described using human understandable labels and measurements, allowing for retrieval and recognition solely based on verbal descriptions. Unlike many primary biometric traits, soft biometrics can be obtained at a distance without subject cooperation and from low quality video footage, making them ideal for use in surveillance applications.” D. A. Reid et al, *Soft Biometrics for Surveillance: An Overview*, 2013, Available at: <http://core.ac.uk/download/pdf/9642804.pdf>, pp.1-3

⁶¹³ HIDE FP7 Project, D3.3a Ethical Brief on Embedded Technology, 1 Feb 2008, Available at: <http://www.hideproject.org/documents/documents.html>, p.9

⁶¹⁴ See, for example: Anil K. Jain, Sarat C. Dass, and Karthik Nandakumar (2004) *Soft Biometric Traits for Personal Recognition Systems*, Proceedings of International Conference on Biometric Authentication, LNCS 3072, Hong Kong, July 2004, pp. 731-738

⁶¹⁵ HIDE FP7 Project, D3.3a Ethical Brief on Embedded Technology, 1 Feb 2008, Available at: <http://www.hideproject.org/documents/documents.html>, p.9

biometrics to render more detailed personal information relating to data subjects; augmented capabilities in the analysis of large datasets incorporating soft biometrics derived from personal data will eventually allow for the type of indexing and filtering currently performed on other types of sensitive personal data. The inherent risk of this development is that soft biometrics could be used in conjunction with other personal data to facilitate the discrimination between data subjects based on the processing of personal data revealing, for example, racial or ethnic origin, religious beliefs, or the processing of data concerning health or sex life.⁶¹⁶

A further consideration pertains to the collection of data for “specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”.⁶¹⁷ The requirement of this principle relating to data quality engages the value-laden question of how one is to discern ‘purpose’, and to what degree this might be specified. Difficulties arise here in that the development of networked sensors is ever-increasing in its intrinsic complexity and, as such, problems arise in terms of determining at any given moment the level of specificity required to appropriately inform the potential data subject of the scope of the data collection they may be subject to. Furthermore, data collection in itself is but the initial concern; more important still is the subsequent extent of the data processing thereafter. Of importance in this context is the discrete collection of highly nuanced personal data relating to a person’s movements, the processing of which may constitute a grave interference in the individual’s right to privacy. At risk is the data subject’s right to bodily integrity, by which an individual is afforded the freedom from non-consensual interference in their physical and mental self-determination. Bodily integrity is critical

⁶¹⁶ Anil K. Jain, Sarat C. Dass, and Karthik Nandakumar (2004) Soft Biometric Traits for Personal Recognition Systems, Proceedings of International Conference on Biometric Authentication, LNCS 3072, Hong Kong, July 2004, p.738. Of note too is that Wood and Graham’s research has underscored the potential for discrimination, warning that designers, builders and programmers of systems are able to embody their prejudices and desires in the architecture of sensing networks even while such systems “are promoted as infallible, logical and free of human prejudice.” See: David Wood and Stephen Graham, Permeable Boundaries in the Software-sorted Society: Surveillance and the Differentiation of Mobility, Paper for ‘Alternative Mobility Futures’ Lancaster University, 9-11 January 2004. Available at: http://www.academia.edu/1069340/Permeable_Boundaries_in_the_Software-sorted_Society_Surveillance_and_Differentiations_of_Mobility

⁶¹⁷ Directive 95/46/EC, Article 6:

1. Member States shall provide that personal data must be:
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

to the individual in maintaining his or her own personal autonomy.⁶¹⁸ The conceptualization of bodily integrity relates to processes and procedures that capture and record information for the purposes of the identification of individuals from one another. The use of fingerprinting and, more recently DNA testing, are well-established forms of biometrics that constitute a form of bodily ‘search’.⁶¹⁹ However, the use of new forms of biometric identifiers, such as those that allow for data capture at a distance whilst precluding that the data subject be informed, or allow for the provision of their consent, prove highly problematic in terms of the safeguard of bodily integrity.

In the *S. and Marper* case it was noted that Lord Steyn, who had provided the lead judgment in the final domestic appeal in the United Kingdom, had outlined five principal factors leading to the conclusion that the interference was proportionate to the aim in respect of the retention of fingerprints and DNA samples; these prove relevant to our consideration of how new biometric identifiers might be appraised vis-à-vis their permissibility.⁶²⁰ In the case of *S. and Marper*, the contention made before the Strasbourg court by the United Kingdom government was that retention “had nothing to do with the past”, rather that the purpose for preserving records reflected their utility in assisting in “the investigation of offences in the future.”⁶²¹ As with DNA samples, certain premises pertaining to the collection and retention of data may be applied more broadly to newly developed biometric identifiers, such as those that

⁶¹⁸ Van der Ploeg affirms that the process of re-evaluating our notion of the physical, anatomical body and its relationship to the concept of ‘bodily integrity’ is ongoing, asserting moreover that the evolution of information technology has had a corresponding effect on our understanding of the normative implications of the growth in the generation and processing of “body data”. This, Van der Ploeg contends, has led to parties attempting to “draw lines, and separate legitimate use from misuse... concepts and values are invoked and applied in contexts and discursive spaces they are not invented for.” See: Van der Ploeg, I., ‘Biometrics and the body as information - Normative issues of the socio-technical coding of the body’, in Lyon, David. *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge, 2003, p.66

⁶¹⁹ See, for example: Mark A. Rothstein & Meghan K. Talbot, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy?* *The Journal of Law, Medicine & Ethics*, Volume 34, Issue 2, Summer 2006. pp. 153–164.

⁶²⁰ The *Marper* judgment states at paragraph 21: “Lord Steyn saw five factors which led to the conclusion that the interference was proportionate to the aim: (i) the fingerprints and samples were kept only for the limited purpose of the detection, investigation and prosecution of crime; (ii) the fingerprints and samples were not of any use without a comparator fingerprint or sample from the crime scene; (iii) the fingerprints would not be made public; (iv) a person was not identifiable from the retained material to the untutored eye, and (v) the resultant expansion of the database by the retention conferred enormous advantages in the fight against serious crime.” *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, §21, 4 December 2008.

⁶²¹ *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, §21, 4 December 2008.

correlate to a person's movements, for example: a person would not be identifiable from the retained material to the untutored eye; or that the material would not be made public.⁶²²

Whilst it may be contended that the link between precedents established with regard to biometric identifiers such as fingerprints and DNA samples appear with those relating to the metrics of an individual's mobility is obscure, in actuality the record of the *S. and Marper* judgment provides clear indications of the parallels that could emerge once these new identifiers become more widely used. For instance, biometric identifiers (referred to as "bioinformation" by the Court in the *S. and Marper* case) constituted by precise location and mobility data of individuals may also in turn be used for familial searching.⁶²³ Indeed, as was alluded to by the Court, in the case of the implementation of searches using new biometric identifiers based on mobility, it is not infeasible that such inspections might reveal "previously unknown or concealed genetic relationships". Whilst this contention might initially appear somewhat implausible, the likelihood of such an eventuality is distinctly probable where even patterns of mobility determined from the analysis of much less precise personal location data enables highly accurate discrimination between citizens, such has been evidenced in recent scientific research.⁶²⁴

⁶²² The judgment records that, in the appeal held before the House of Lords, Lord Steyn: "...saw five factors which led to the conclusion that the interference was proportionate to the aim: (i) the fingerprints and samples were kept only for the limited purpose of the detection, investigation and prosecution of crime; (ii) the fingerprints and samples were not of any use without a comparator fingerprint or sample from the crime scene; (iii) *the fingerprints would not be made public*; (iv) *a person was not identifiable from the retained material to the untutored eye*; (v) the resultant expansion of the national database by the retention conferred enormous advantages in the fight against serious crime." Note: *emphasis added. S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, §21, 4 December 2008.

⁶²³ For example, the recent research conducted by neurologists on genetically hereditary disorders including certain types of paraplegia, which are characterised by progressively disabling symptoms that affect an individual's gait, has provided evidence of the ability to detect genetic traits vis-à-vis mobility impairments. Gait analysis can thus be used as an object tool to quantify the impairment of a person's gait, and therefore their associated mobility, and analyze how this is manifested in family members. Thus this means of quantification and the collection of biometric identifiers can allow for the genetic relatives of persons to be distinguished where they exhibit similar patterns of movement symptomatic of the same genetic disorders. See: Klebe S. et al, Gait analysis of sporadic and hereditary spastic paraplegia, *Journal of Neurology*, May 2004; 251(5), pp.571-578. It also should be noted that in the *S. and Marper* case the Court referred to the conclusions drawn by the Nuffield Council on Bioethics as to the use of biometric databases for the purpose of searching for relatives as being particularly sensitive; see: *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, §39, 4 December 2008.

⁶²⁴ For example, the research by Montjoye et al examined a dataset of the locations of individuals and proved that just four spatio-temporal points were enough to uniquely identify 95% of the individuals. Montjoye et al noted that: "...the uniqueness of human mobility traces is high, thereby emphasizing the

In the *Marper* case the Court further cited the relevance of the protection given individuals with regard to automatic processing of personal data, noting that the Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data: “defines ‘personal data’ as any information relating to an identified or identifiable individual (‘data subject’)”.⁶²⁵ It should also be noted that in *Marper* the ECtHR referred to the applicability of Recommendation No. R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector.⁶²⁶ In a similar context, therefore, the processing of personal data by law enforcement of personal location data used to establish biometric indicators would also be subject to the same stipulations. In particular, Principle 2.1 of Recommendation No. R (87) 15 specifies *inter alia* that: “The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence.”⁶²⁷ Of further interest in this regard is the mention made by the Court in the *Marper* case with regard to data storage; the European Court of Human Rights referred to Principle 3 of

importance of the idiosyncrasy of human movements for individual privacy. Indeed, this uniqueness means that little outside information is needed to re-identify the trace of a targeted individual even in a sparse, large-scale, and coarse mobility dataset. Given the amount of information that can be inferred from mobility data, as well as the potentially large number of simply anonymized mobility datasets available, this is a growing concern... Together, these determine the uniqueness of human mobility traces given the traces’ resolution and the available outside information. These results should inform future thinking in the collection, use, and protection of mobility data. Going forward, the importance of location data will only increase and knowing the bounds of individual’s privacy will be crucial in the design of both future policies and information technologies.” See: Yves-Alexandre de Montjoye et al, Unique in the Crowd: The privacy bounds of human mobility, Nature.com - Scientific Reports 3, Article number: 1376, 25 March 2013, Available at:

<http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html>, p.4

⁶²⁵ The *Marper* judgment also cites the provisions of COE Convention 1981 in respect of the quality of data, which affirms that personal data undergoing automatic processing shall be:

- “... (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are stored;
- ...”

Accordingly, these provisions are relevant in our consideration of the automatic processing that the generation of biometric identifiers based on movement inheres. *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, §41, 4 December 2008.

⁶²⁶ *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, §42, 4 December 2008.

⁶²⁷ Council of Europe, Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector, 17 September 1987, Principle 2.1. Note: The explanatory memorandum to the Recommendation Rec (87) 15 notes that Principle 2.1 “excludes an open-ended, indiscriminate collection of data by the police. It expresses a qualitative and quantitative approach to Article 5.c of the Data Protection Convention which stipulates that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are stored.” See: Explanatory Memorandum to the Recommendation Rec (87) 15, 17 September 1987, Available at: <https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM>

Recommendation No. R (87) 15, which stipulates that: “As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law.”⁶²⁸

In *Marper v. United Kingdom* the Court also refers to the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters as relevant to the consideration of the processing of personal data by law enforcement, though of course the scope of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States. Whilst *Marper* was particularly concerned with data retention periods and hence focused in on Article 5’s provisions vis-à-vis the establishment of time limits for erasure and review of personal data, in the context of the possible recourse to biometric identifiers based on location data the provisions of Articles 6, 7 and 8 of Framework Decision 2008/977/JHA are all pertinent should such data be gathered or processed by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the processing of personal data transmitted or made available between Member States.

Article 6 of Framework Decision 2008/977/JHA pertaining to the processing of special categories of data is engaged where personal data concerns health, and permits processing only where it is strictly necessary and when the national law provides adequate safeguards.⁶²⁹ Article 7 of Framework Decision 2008/977/JHA needs also be taken into consideration in respect of the safeguards it provides for automated individual decisions, notably that when: “...automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject’s legitimate interests.” Moreover, the provisions therein need be taken into

⁶²⁸ *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, §42, 4 December 2008.

⁶²⁹ One must also note here that the stipulations regarding sensitive data made within Article 6 also apply in respect of personal data revealing categories such as political opinions, religious or philosophical beliefs and sex life; all of which may be inferred from the processing of precise location data. See: Article 6, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

consideration conjointly with an assessment as to the applicability of Article 8 of the Framework Decision, which stipulates that data quality be ensured such that personal data “which are inaccurate, incomplete or no longer up to date are not transmitted or made available.”⁶³⁰ When making measurements, resolution is imposed across the dimensions relevant to location data, including spatial and temporal attributes, in the form of discretisation. The effects on data quality that result from discretisation are critical to our consideration of the intrinsic utility, value and dependability of profiles and metrics drawn from the collection and processing of location data. In fact, the disregard of the effects of discretisation are likely to be more substantial in its impact than, conversely, the increasing appreciation of the effects errors of measurement yield. Whilst research on location data collection has tended to focus on measurement errors, the impact of discretisation may in many cases be more substantial in terms of its overall impact on the accuracy of determinations drawn from the processing and analysis of location data.⁶³¹

5. Reconciling covert data collection with the principle of informed consent

Ambient sensing using discrete sensors can foreseeably constitute covert monitoring. Moreover, the practice when combined with the processing of personal data in respect of determining behavioural and physiological biometrics evidently presents concerns. That capacities are predicted to shift towards more covert capabilities vis-à-vis data capture suggest the data subject may frequently be entirely unaware as to their being how data is being collecting. An accelerated transition toward discreet methods of

⁶³⁰ Article 7 & 8 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

⁶³¹ Discretisation is “an implicit measure of what is not known or what might be missing: overall reliability of a spatial representation is less influenced by the accuracy or precision of a measurement than by the number, density, or spacing interval of the measurements.” NCHRP, *Quality and Accuracy of Positional Data in Transportation*, 2003, Available at: http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_506.pdf: Forward to the NCHRP Project 20-47(01), p.16. *See also*: See: Chrisman, N., “The Role of Quality in Information in the Long Term Functioning of a Geographic Information System.” *Proceedings of Auto-Cartography*, Volume 6, 1983, pp. 303–312; *See also*: Sinton, D.F., “The Inherent Structure of Information as a Constraint to Analysis: Mapped Thematic Data as a Case Study.” *Harvard Papers on Geographic Information Systems*. Vol. 6, 1978, pp. 43–59. The NCHRP also notes: “The primary sources of error associated with positional data are acquisition or measurement, processing, transformation, and presentation or visualisation. Regardless of the measurement technique and referencing system, data will be observed with error.” NCHRP, *Quality and Accuracy of Positional Data in Transportation*, 2003, Available at: http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_506.pdf: Forward to the NCHRP Project 20-47(01), p.61

data collection in part reflects an inclination on the part of technology developers to institute a higher degree of user friendliness and convenience into the functionality of sensing capabilities, such that little or no conscious effort is required of the potential data subject in respect of their acquiescence.⁶³²

This progression unquestionably presents a significant challenge to the guarantees provided the data subject with regard to consent.⁶³³ Furthermore, one needs also consider the possible implications of the processing of personal data relating to biometrics where the criteria and procedure for interpreting the characteristics of individuals' behaviour is automated. In particular, an elevated risk arises where inferences are drawn that relate to a person's suspected intentions based on the analysis of location data identifying an individual's movements. The pitfalls inherent to interpreting such complex dynamics and, in particular, relying upon automated decision-making to detect and flag the correlation between suspect patterns of movement with malicious intent are well documented.⁶³⁴ A major concern therefore in the deployment of unobtrusive methods of data collection and processing for behavioural biometrics is the issue of consent and secondary use. Highly unobtrusive techniques offer the possibility of identifying people outside the scope of the original application, without any special equipment. A key question is, therefore, how to limit behavioural profiles to a specific context, and ascertain how to effectively implement

⁶³² See, for example: Wisman, T.H.A., "Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things", *European Journal of Law and Technology*, Vol. 4, No. 2, 2013, Available at: <http://ejlt.org/article/view/192/379>, p.10

⁶³³ See, for example: HUMABIO FP6, Human monitoring and Authentication using Biodynamic indicators and behavioural analysis, D1.2 Scenarios of use and system requirements, December 2006, Available at: http://www.humabio-eu.org/docs/HUMABIO-D1_2.pdf, pp.13-85. See also: HIDE FP7 Project, D3.3a Ethical Brief on Embedded Technology, 1 Feb 2008, Available at: <http://www.hideproject.org/documents/documents.html>, pp.5-7.

⁶³⁴ See, for example: National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment*, 2008, Available at: <http://www.nap.edu/catalog/12452.html>, pp. 138-140. See, also: Taylor R.B., (1997) 'Crime and place: what we know, what we can prevent, and what else we need to know,' Paper presented at the National Institute of Justice Annual Research Conference, Washington DC, 1997; Tompson L., Townsley M., (2010) Looking back to the future: using space-time patterns to better predict the location of street crime. *International Journal of Police Science Management* 12(1), pp.23-40; Roedl G., Elmes G.A., and Conley J. 'Spatial Technology Applications', in Elmes G.A., Roedl G. and Conley J. (eds.) *Forensic GIS - The Role of Geospatial Technologies for Investigating Crime and Providing Evidence* (2014), Springer Publishing, London; Leitner M. (ed.) (2013) *Crime modelling and mapping using geospatial technologies*. Springer, Heidelberg; Chainey S., Thompson L. (2008) *Crime mapping case studies: practice and research*. Wiley, Chichester.

data protection safeguards to prevent the unwarranted leak of personal data outside such a system.⁶³⁵

Articles 7 (a) and Article 26 (1) of Directive 95/46/EC affirm that every consent provided by a data subject must be given in an unambiguous manner; this requirement posits that there should be no reasonable doubt as to whether the individual concerned as the data subject allowed for the communication of his agreement to processing of their personal data. With regard to the processing of special categories of data, the provisions of Article 8(2) of Directive 95/46/EC apply as regards the distinctions to be drawn between explicit and non-explicit consent. In this respect the European Union Agency for Fundamental Rights (FRA) has drawn attention to the parameters for consent based upon the agreement of the data subject to be valid, noting that: “Deducing consent from mere inactivity is not capable of delivering unambiguous consent, for example.”⁶³⁶ Furthermore, with regard in particular to special categories of data, the FRA notes: “where data to be processed are sensitive, explicit consent is mandatory and must be unambiguous.”⁶³⁷ A further concern in the development of biometric identifiers based on location data is the issue of ensuring data quality, particularly as regards precision in the ascription of personal data to specific individuals. Indeed, this concern has been raised more widely in the context of the development of services relating to the processing of location data; the WP29, for example, has highlighted the need for providers of services to take appropriate measures when obtaining consent to ensure that the person to whom the location data relate is the same as the person who has given consent.⁶³⁸

⁶³⁵ ENISA posits that Directive 95/46/EC requires that every identification event involving behavioural biometrics should be processed with the informed consent of the data subject. For example, if a person’s keystroke signature is known they could be recognized on other systems with keystroke analysis software. See: *ENISA, ENISA Briefing: Behavioural Biometrics, 5 February 2010, Available at: <https://www.enisa.europa.eu/activities/risk-management/files/deliverables/behavioural-biometrics>, p.5*

⁶³⁶ European Union Agency for Fundamental Rights, Handbook on European data protection law, 2014, Available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf, p. 56

⁶³⁷ See: European Union Agency for Fundamental Rights, Handbook on European data protection law, 2014, Available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf, p. 56

⁶³⁸ See: Working Party 29, Opinion on the use of location data with a view to providing value-added services, 2130/05/EN WP 115, November 2005, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf, p.6.

6. The sensitivity of health data, and a data subject's right to self-determination

In its consideration of the practical application of Directive 95/46/EC in the light of developments in healthcare,⁶³⁹ the advisory group WP29 stated in an early opinion paper that personal data concerning health within the meaning of Article 8(1) of Directive 95/46/EC should be broadly interpreted.⁶⁴⁰ Indeed, WP29 affirmed that the definition applies to an individual's personal data concerning health when such data "has a *clear* and *close* link with the description of the health status of a person."⁶⁴¹ Thus the question arises as to how malleable the terms 'clear' and 'close' might be in respect of their application to any appraisal as to whether such data *describes* the health *status*.⁶⁴² Personal location data will in future be processed more widely in

⁶³⁹ See, for example: Shokri, R. and Shmatikov, V., 2015, October. Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM, p.1310; W. Scheirer and T. Boulton. Biometrics: Practical issues in privacy and security. Technical report, Securics, Inc. and the University of Colorado, Colorado Springs, 2011. Tutorial at International Joint Conference on Biometrics.

⁶⁴⁰ In addition to Article 8(1) of Directive 95/46/EC, Article 6 of Convention 108 also outlines a general prohibition of the processing of personal data concerning health. It should be noted that the special provision pertaining to sensitive data needs be considered in conjunction with the application of the additional safeguards aimed at ensuring the protection of personal data, in particular the provisions relating to data quality in Article 6 of Directive 95/46/EC and the applicable criteria for legitimate data processing contained within Article 7 of the Directive. Furthermore, it should be noted with regard to the term 'health data' that this could include those records of persons that may be considered entirely healthy. See, for example: Recital 6, Explanatory Memorandum, Recommendation No.R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, (Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies), Available at: www.coe.int/, p.2, which notes inter alia, that: "Health records may also be established outside the context of the doctor-patient relationship and may include data concerning perfectly healthy persons." Also relevant here is the concern that the use of biometric systems rarely produce error-free results; inaccuracy may stem from a variety of data acquisition issues pertaining to both environment conditions and also in connection with the different types of equipment used. Data processing errors may also occur in the operation of systems. See: WP29, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, 27 April 2012, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/>, p.6

⁶⁴¹ WP29, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP131, 15 February 2007, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf, p.7

⁶⁴² The WP29 expressed the view in a 2007 Working Document that a broad interpretation of the notion "personal data on health" led to the conclusion that all such personal data was subject to the special data protection rules on the processing of sensitive information contained in Article 8 of Directive 95/46/EC. See: WP29, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, 15 February 2007, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf, p.7 The opinion of expert group WP29 is based partially upon the ECJ's deliberations in the *Lindqvist* case, in which the Court confirmed: "In the light of the purpose of the directive, the expression 'data concerning health' used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual." European Court of Justice, Judgment of 6 November 2003, Case C-101/01 - Bodil Lindqvist, §50.

connection with health research.⁶⁴³ Indeed, Geographic Information Systems (GIS) have already been used by public health researchers to link individual health data to the physical space and social community within which a person lives.⁶⁴⁴

It has been suggested that the linkage of spatial data to demographic attributes, however, proves a concern where there runs a risk of misclassifications of data. It has been suggested by Edelman that the evolution of GIS technologies will allow ever more detailed research of health issues where descriptive attribute data is projected onto spatial data to visualize relationships, for example, in respect of injury rates and the physical environment (such as the location of stairways, elevators, etc.).⁶⁴⁵

The WP29 has called attention to the need to ensure that adequate safeguards are put in place to ensure the guarantee of the data protection rights of citizens and their right to privacy, noting that an essential consideration with regard to the development of systems that make use of sensitive health data is the principle of respecting a person's right to self-determination; the WP29 asserted in this context that: "the patient's self determination concerning when and how his data are used should have a significant role as a major safeguard." It should be noted with regard to the automatic processing of medical data, the Council of Europe Recommendation No.R(97)5 also affirms the importance of the safeguard of the fundamental rights of the individual, stating:

⁶⁴³ Camp et al argue in this context that movement, habit, and location data-related information (e.g. observation of the movements of a person with Alzheimer's disease is not strictly medical data) are not protected as health data. *See further:* Camp, L.J. and Connelly, K., 2008. Beyond consent: privacy in ubiquitous computing (UbiComp). *Digital privacy: Theory, technologies, and practices*, pp.327-343, p.338. *See also:* Glenn T, Monteith S. New measures of mental state and behavior based on data collected from sensors, smartphones, and the Internet. *Current Psychiatry Report*. 2014 doi:10.1007/s11920-014-0523-3.

⁶⁴⁴ *See:* E. K. Cromley & S. L. McLafferty, GIS and Public Health, The Guilford Press, 2002. Furthermore, Edelman has also underscored the essential value of location data to developing 'epidemiological surveillance data' that links health-related events in individuals to spatial areas: modelling may then allow for data processing that analyses and assesses the relative contribution of identified characteristics in individuals and population groups. *See:* Linda S. Edelman, Using Geographic Information Systems in Injury Research, *Journal of Nursing Scholarship*, 2007, Vol. 9(4), Available at: <http://www.ncbi.nlm.nih.gov/pubmed/18021129>, p.310. *See also:* Boulos M.N., Towards evidence-based, GIS-driven national spatial health information infrastructure and surveillance services in the United Kingdom, *International Journal of Health Geographics*, 2004 Jan 28;3(1):1, Available at: <http://www.ncbi.nlm.nih.gov/pubmed/14748927>. *See also:* Neff G, Fiore-Silfvast B. Pictures of health: Does the future of wellness need us? *Theorizing the Web*, NYC 2013. Available at: <http://thesocietypages.org/cyborgology/2013/02/26/ttw13-preview-gina-neff-and-brittany-fiore-silfvast-pictures-of-health-does-the-future-of-wellness-need-us/>

⁶⁴⁵ *See:* Linda S. Edelman, Using Geographic Information Systems in Injury Research, *Journal of Nursing Scholarship*, 2007, Vol. 9(4), Available at: <http://www.ncbi.nlm.nih.gov/pubmed/18021129>, p.306.

“3.1. The respect of rights and fundamental freedoms, and in particular of the right to privacy, shall be guaranteed during the collection and processing of medical data.

3.2. Medical data may only be collected and processed if in accordance with appropriate safeguards which must be provided by domestic law.”

Moreover, Recommendation No.R(97)5 elucidates the principle that medical data⁶⁴⁶ should only be collected and processed by health-care professionals, or by individuals or bodies working on behalf of health-care professionals. The Recommendation further clarifies this point in acknowledging that non-healthcare professionals indeed may be required to collect and process medical data, but that the following requirements be respected:

“Controllers of files who are not health-care professionals should only collect and process medical data subject either to rules of confidentiality comparable to those incumbent upon a health-care professional or subject to equally effective safeguards provided for by domestic law.”⁶⁴⁷

Recommendation No.R(97)5 on the protection of medical data also provides additional guidance as to the collection and processing of medical data and the scope

⁶⁴⁶It should be noted that, with regard to the terms “medical data” and “personal health data” that in the general comments on the recommendation including in the ‘Explanatory memorandum to Recommendation No.R(97) 5 on the protection of medical data the two terms are employed interchangeably. *See:* Explanatory Memorandum, Recommendation No.R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, (Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies), Available at: www.coe.int/, pp.1-2. However, WP29 noted in its recent paper on mHealth that: “...health data (or *all data pertaining to the health status of a data subject*) is a much broader term than the term 'medical'.” Indeed, particularly relevant to our consideration of the interrelationship between different types of sensitive data, including location data, is the particularly comprehensive list provided by WP29, whereby it states: “Based on the current Data Protection Directive, national legislators, judges and DPA's have concluded that information such as the fact that a woman has broken her leg (Lindqvist), that a person is wearing glasses or contact lenses, data about a person's intellectual and emotional capacity (such as IQ), information about smoking and drinking habits, data on allergies disclosed to private entities (such as airlines) or to public bodies (such as schools); data on health conditions to be used in an emergency (for example information that a child taking part in a summer camp or similar event suffers from asthma); membership of an individual in a patient support group (e.g. cancer support group), Weight Watchers, Alcoholics Anonymous or other self-help and support groups with a health-related objective...”. *See:* WP29, Paper on health data in apps and devices, 9 February 2015, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation>, p.2

⁶⁴⁷*See:* Recital 3, Recommendation No.R(97) 5 on the protection of medical data (13 February 1997), Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp.

of specific permissible purposes for which fair and lawful processing shall be allowed. Recital 4 of Recommendation No.R(97)5 affirms:

“4. Collection and processing of medical data

4.1. Medical data shall be collected and processed fairly and lawfully and only for specified purposes.

4.2. Medical data shall in principle be obtained from the data subject. They may only be obtained from other sources if in accordance with Principles 4, 6 and 7 of this recommendation and if this is necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data.”⁶⁴⁸

The above-mentioned provisions therefore need be taken in consideration in examining the permissibility of the use of location data that inheres the characteristics of medical data based upon data processing for the purposes of developing biometric identifiers. Additionally, due regard need be given to the provision contained with Recital 5 of the Recommendation No.R(97)5 on the protection of medical data insofar as it stipulates that the data subject shall be informed as to “the existence of a file containing his/her medical data and the type of data collected or to be collected”. Recital 5 of Recommendation No.R(97)5 on the protection of medical data also specifies further relevant provisions that require consideration in the current context, notably: “The purpose or purposes for which they are or will be processed; where applicable, the individuals or bodies from whom they are or will be collected; the persons or bodies to whom and the purposes for which they may be communicated;”.⁶⁴⁹ The obligation of States to develop adequate safeguards for the protection of special categories of data, such as health data, provided for in domestic legislation was reaffirmed in the case *K.H. and Others v. Slovakia*, where the Court again reiterated that: “communication or disclosure of personal health data that may be inconsistent with the guarantees in Article 8 of the Convention can be prevented by means such as incorporation in domestic law of appropriate safeguards with a view to strictly limiting the circumstances under which such data can be disclosed and the

⁶⁴⁸ Recital 4, Recommendation No.R(97) 5 on the protection of medical data (13 February 1997), Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp.

⁶⁴⁹ See: Recital 5(a)(b)(c)(d), Recommendation No.R(97) 5 on the protection of medical data (13 February 1997), Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp.

scope of persons entitled to accede to the files.”⁶⁵⁰

In the case of sensitive personal data explicit consent from the data subject is required. In addition, the requirement of explicit consent is that it must be specific to a particular processing operation; for a declaration of intent to be valid, in this context the explicitness of the consent should reflect the sensitivity of the personal data concerned.⁶⁵¹ Furthermore, it should be noted that personal data relating to health varies in the nature of its characteristics and its inherent capacity to disclose sensitive detail as to the individual’s health status, as was recognised in the Working Document on the processing of personal data relating to health in electronic health records, which stated: “In view of the varying damage potential of different types of health information, categories of use cases should be discerned with different degrees of the possibility to exercise self determination.”⁶⁵² In this context then the *Marper* case is relevant for the emphasis the Court placed on Article 6 of COE Convention 1981 in respect of special categories of data, where personal data concerning the individual’s health may not be processed unless domestic law provides appropriate safeguards. Furthermore, in *Biriuk* case the Court reaffirmed that the protection of a personal health data was especially important insofar as the safeguard proved integral to the respect of private and family life, stating:

⁶⁵⁰ See: *K.H. and Others v. Slovakia*, No. 32881/04, 28 April 2009, §56. See, also: *Z v. Finland*, judgment of 25 February 1997, *Reports* 1997-I, §§ 95-96).

⁶⁵¹ In this respect WP29 noted that: “Consent must be specific: ‘Specific’ consent must relate to a well-defined, concrete situation in which the processing of medical data is envisaged.” See: WP29, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, 15 February 2007, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf, p.7

⁶⁵² See: WP29, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, 15 February 2007, Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf, p.13. Moreover, this capability is evolving further still to develop yet more detailed aspects of physiological and psychological conditions pertaining to the data subject (especially where personal data is consolidated with that of the ambient environment, allowing for an individual’s response to external conditions to be gauged, such as temperature, stress levels, anxiety, etc.) The evolution of such a concept of identity based upon the biometrics of our personal movements and the biometrics of mobility is only nascent. We need thus acknowledge that the challenges posed for fundamental rights are only just beginning to be made apparent and appraised. See: Bowker G C, 2003, “The past and the Internet” *SSRC Items and Issues* 4(4), Available at:

http://www.ssrc.org/programs/publications_editors/publications/items/online4-4/bowker-past.pdf, p.30. See, also: Andronikou V., Demetis D.S., Varvarigou T., *Biometric Implementations and the Implications for Security and Privacy*, 2007, Available at: http://journal.fidis-project.eu/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_Implications_for_Security_and_Privacy.pdf, pp.11-17

“More specifically, the Court has previously held that the protection of personal data, not least medical data, is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention.”⁶⁵³

Furthermore, reinforcing this notion is the finding of the ECJ in the *Lindqvist* case, in which it held that existing jurisprudence affirmed the requirement that personal data concerning health within the meaning of Article 8(1) of Directive 95/46 should be broadly interpreted, noting thereby: “In the light of the purpose of the directive, the expression ‘data concerning health’ used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual.”⁶⁵⁴

Indeed, we need also consider how developing technologies are reshaping our notion of health monitoring and, therefore, challenging traditional conceptualisations as to what we consider ‘health status’ represents. Whilst earlier in the discussion here it was noted that biometric data has indeed been described various plausible and explicit definitions, the application of the term itself in connection to the designation of ‘special categories of data’ and the ascription of the notion that it constitutes ‘sensitive data’ remains somewhat contentious. In this context it must be noted that the position of experts has wavered, and changed over time. For example, the earlier approach adopted by the WP29 was such that biometric data was not necessarily considered sensitive: namely, it noted in its early 2003 Opinion on biometric data that the processing of biometric data does not *per se* constitute a processing of sensitive data: it determined that whether data processing contains sensitive is dependent upon an appreciation of the specific biometric characteristic used and the biometric application itself.⁶⁵⁵

⁶⁵³ *Biriuk v. Lithuania*, No. 23373/03, 25 November 2008, §39

⁶⁵⁴ Case C-101/01 *Lindqvist* [2003] ECR I-12971, §50

⁶⁵⁵ See: WP29, Working document on biometrics, 12168/02/EN WP 80, 1 August 2003, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/>, p.10. While the expert group WP29 identified concerns that the use of biometrics could “impact significantly on the dignity, privacy and the right to data protection of vulnerable people such as young children, elderly people and persons physically unable to complete the enrolment process successfully”, it failed

With regard to the privacy of health data as sensitive data, and especially pertinent to our appraisal of the challenges presented by the collection and processing of personal location data, is the jurisprudence of the European Court of Human Rights. In *I. v. Finland* the Court referred to the “sense of privacy of a patient”; interestingly, the use of embedded sensing devices portends an era where distinctions between persons receiving or registered to receive medical treatment, i.e. the patient, and the layperson not requiring such care shall become increasingly indistinct.⁶⁵⁶ Further complicating this evolution is the notion that the wide distribution of health-related monitoring capabilities is required, researchers claim, so as to facilitate the determination of health concerns and discern symptoms of ailments at the earliest possible juncture, and therefore enable early medical interventions.⁶⁵⁷ With specific regard to the principle of data quality, Recommendation No.R(97)5 on the protection of medical data provides further elucidation on the importance of this principle in respect of personal information pertaining to an individual’s health, notably: “The quality and integrity of information is extremely important in matters of health. At a time of increasing personal mobility, the exchange of accurate and relevant information is necessary for the individual's safety.”⁶⁵⁸

Health data may inhere a particularly high value to certain parties based on the sensitivity of the information it contains, such that the risk for the potential of misuse of such data may be significant. One requirement in relation to safeguarding personal data from inappropriate processing and misuse is the necessity of creating sufficient

to acknowledge in this regard other aspects of concern (particularly in connection with health and medical-related conditions) relating to the possible stigmatisation of individuals based on the collection of such sensitive data. *See*: WP29, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, 27 April 2012, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/>, p.9

⁶⁵⁶ In its more recent Opinion on health data in apps, the WP29 indeed remarked upon the complexity of discerning what personal data constitutes health data where there is a “wide range of personal data that may fall into the category of health data, this category represents one of the most complex areas of sensitive data and one where the Member States display a great deal of diversity and legal uncertainty.” *See*: WP29, Paper on health data in apps and devices, 9 February 2015, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation>

⁶⁵⁷ This is especially the case in the field of psychiatry and mental health. *See*, for example: Blum J., Prof. Evan Magill, M-Psychiatry: Sensor Networks for Psychiatric Health Monitoring, 28 August 2008, Available at: <http://www.cms.livjm.ac.uk/pgnet2008/Proceedings/Papers/2008028.pdf>, pp.1-5

⁶⁵⁸ Recital 7, Explanatory Memorandum, Recommendation No.R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, (Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies), Available at: www.coe.int/, p.2

transparency so that citizens place trust in the systems applying the processing; and this requires comprehension on the part of the data subject as to the nature of the data processing that occurs.⁶⁵⁹ However, a further challenge lies in the fact that giving meaning to the complexity contained in much of the personal data that can now be collected entails subjective decision-making based on value judgments; in essence, reliance is placed on algorithms to determine patterns, label themes and develop modes of categorization.⁶⁶⁰ This concern therefore needs to be taken into consideration as concerns the process of providing the necessary transparency to data subjects. In the *I. v. Finland* case the European Court of Human Rights reiterated its position on the necessity of safeguards within each jurisdiction's domestic legislation to protect personal health data from inappropriate disclosure or communication: this concern, then, is especially valid where the pervasiveness of sensing capabilities and dissemination may challenge the protection afforded individuals in their right to the protection of personal data.⁶⁶¹

6.1 The application of public interest exemptions to the processing of sensitive data and developing movement-based biometrics

It should however be noted that Article 8 of Directive 95/46/EC relating to special categories of data does contain a provision allowing Member States to derogate further from the prohibition on processing of sensitive data, where it may be demonstrated that the appropriate balance between a data subject's rights and the legitimate interests of the data controller and other their parties in establishing a permissible public interest exemption. With regard to the provision made in Article

⁶⁵⁹ See: WP29, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, 15 February 2007, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf, p.20.

⁶⁶⁰ See: Herrera M. R., Barreda D. S., 'The SDIK Police Model: How to Make the Invisible Visible' in Elmes G.A., Roedl G. and Conley J. (eds.) *Forensic GIS - The Role of Geospatial Technologies for Investigating Crime and Providing Evidence* (2014), Springer Publishing, London, p.147.

⁶⁶¹ The Court stated: "Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (see *Z v. Finland*, judgment of 25 February 1997, *Reports of Judgments and Decisions* 1997-I, §§ 95-96)." See: *I. v. Finland*, No. 20511/03, 17 July 2008, §38

8(4)⁶⁶² we need also consider the declaration that precedes it in Recital 34 of Directive 95/46/EC, pertaining to permissible derogations based on the public interest.⁶⁶³ Whilst Recital 34 of Directive 95/46/EC indeed provides examples of activities that may inhere ‘substantial public interest’ cases, one must however reflect on the observation that the application of Directive 95/46/EC does not however apply in the domestic setting to data processing in the area of police and judicial cooperation in criminal matters may be exempted from its provisions.⁶⁶⁴

In this context Recommendation No. R(87)15 provides useful guidance in terms of the safeguards that need be considered where data processing by police authorities may have a significant impact on the individual data subjects concerned. Whilst the rights of data subjects were made subject to restrictions by Article 9(2) of Convention 108, where Member States may derogate from the Convention's basic data protection principles in the interests of, *inter alia*, “the suppression of criminal offences”, the drafting of Recommendation (87) 15 was intended to identify problems that had arisen by the use of personal data in the police sector and to formulate concrete proposals for their solution.⁶⁶⁵ Significantly, the EU Fundamental Rights Agency has highlighted the importance of taking into consideration the guidance the Recommendation provides in noting that it addresses in detail how data should be collected for police work, how data files in this sphere need be maintained, how access to the data in question should be controlled (including the conditions for which

⁶⁶² Article 8(4), Directive 95/46/EC

“Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.”

⁶⁶³ Recital 34, Directive 95/46/EC

“Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;”

⁶⁶⁴ Council Framework Decision 2008/977/JHA in part attempts to address certain lacunae in respect of the existing legal framework for data protection in the EU, and provides for the protection of personal data that is processed in the framework of police and judicial cooperation in order to prevent, investigate, detect or prosecute a criminal offence or execute a criminal penalty. The Framework Decision has limited effect in respect of the domestic setting in the sense that where data originates and is processed within a Member State its provisions do not apply.

⁶⁶⁵ See: Explanatory Memorandum to CoE, Committee of Ministers (1987), Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector, 17 September 1987, at §5.

the transfer of data to foreign police forces may be authorised), and how data subjects should be empowered to exercise their data protection rights.⁶⁶⁶ Moreover, the EU Fundamental Rights Agency has further drawn specific attention to the necessary limitation on the processing of special categories of data, asserting: “Processing of sensitive data should be limited to that which is absolute necessity in the context of a particular inquiry. Where personal data are collected without the knowledge of the data subject, the data subject ought to be informed of the data collection as soon as such disclosure no longer inhibits investigations. The collection of data by technical surveillance or other automated means should also be based on specific legal provisions.”⁶⁶⁷

Recommendation No.R(87)15 also articulates several stipulations that are especially relevant in the context of the permissibility of the possible use by law enforcement of personal data for the purpose of developing profiles using biometric identifiers. Principle 2.3 of Recommendation No. R(87)15 states that the “collection of data by technical surveillance or other automated means should be provided for in specific provisions.”⁶⁶⁸ Another important safeguard pertaining to the requirement that States provide legislative provisions protecting the rights of data subjects in connection with data collection and processing in the police sector is Principle 5.6, which outlines the requirement that conditions be placed on the interconnection of files and on-line access to files.⁶⁶⁹

⁶⁶⁶ See: European Union Agency for Fundamental Rights, Handbook on European data protection law, 2014, Available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf, p.146

⁶⁶⁷ See: European Union Agency for Fundamental Rights, Handbook on European data protection law, 2014, Available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf, p.147.

⁶⁶⁸ CoE, Committee of Ministers (1987), Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector, 17 September 1987, Principle 2.3.

⁶⁶⁹ Principle 5.6, CoE Committee of Ministers (1987), Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector, 17 September 1987:

Principle 5.6.

“Interconnection of files and on-line access to files

The interconnection of files with files held for different purposes is subject to either of the following conditions:

- a. the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or
- b. in compliance with a clear legal provision.”

In assessing the use of sensitive data in by public authorities in the type of processing activity being considered here, reference to the caselaw of both the ECHR and the ECJ provides scope for determination of its permissibility. The ECJ noted in the Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert*, that Article 8(1) of the Charter states that: “everyone has the right to the protection of personal data concerning him or her” and that this fundamental right “is closely connected with the right to respect of private life expressed in Article 7 of the Charter.” However, it reiterated that these protections are not absolute, noting: “the right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society.”⁶⁷⁰

According to the provisions articulated in Article 8(2) of the European Convention on Human Rights and the established jurisprudence of the Court, for an interference in the right to private and family life to be legitimate it must be ‘in accordance with the law’ and be ‘necessary in a democratic society’. Furthermore, it need also be appraised as to whether the processing is necessary in the light of the legitimate aim pursued, and whether the measures taken in the data processing operation are in fact proportionate. As such, it is imperative that the responsible party for the data processing assesses whether in fact other less infringing measures for conducting the monitoring activity might be available, and thus constitute a more appropriate means when implemented to achieve the desired objective.

In *Bykov v. Russia* the Strasbourg Court reiterated its declaration as to the necessary scope of provisions required by domestic legislation, citing its earlier ruling in *Khan v. the United Kingdom*, whereby it affirmed that:

“the phrase “in accordance with the law” not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of covert surveillance by public authorities, domestic law must provide protection against arbitrary interference with an individual's right under Article 8. Moreover, the law must be sufficiently clear in its terms to give individuals an adequate indication as

⁶⁷⁰ Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, §§47-48. See, also: Case C-112/00 *Schmidberger* [2003] ECR I-5659, §80 and the caselaw cited).

to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures.”⁶⁷¹

The aforementioned citation further indicates the importance of the notion of foreseeability, in that whilst the detail of specific measures may necessarily be withheld in the interests of the preservation of their operational efficacy, which may require a degree of secrecy, nonetheless citizens require to be sufficiently informed of the significance of such operations.

Moreover, the ECtHR has ruled that the principles concerning the accessibility and clarity of the laws governing both interception and more general programmes of surveillance (referred to under the moniker “strategic monitoring” in the *Weber and Saravia* case, at §18) should be no different. In *Malone v United Kingdom* the ECtHR stated that the requirement of foreseeability is clearly bounded.

“In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee *when* the authorities are likely to intercept his communications so that he can adapt his conduct accordinglylaw must be sufficiently clear in its terms to give citizens an adequate indication as to the *circumstances* in which and the *conditions* on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.”⁶⁷²

The ECtHR’s judgment is particularly valuable for its articulation of the criteria by which the notion of foreseeability is to be construed; the enablement of foreseeability being dependent primarily upon provision of an adequate indication as to the circumstances and conditions under which monitoring may be lawfully employed. Notably, the Court’s statement does not address other tangible considerations such as the capabilities of the measure deployed: a question that technological advancements in techniques inevitably raise i.e. can a citizen comprehend the possibility of an

⁶⁷¹ *Bykov v. Russia* [GC], No. 4378/02, 10 March 2009, §76. See, also: *Khan v. the United Kingdom*, no. 35394/97, § 26, ECHR 2000-V.

⁶⁷² *Malone v. United Kingdom*, (1984) Series A, No 82, §67 Note: emphasis added

interference in her rights where she is wholly unaware as to the means at the disposal of public authorities?

6.2 In accordance with the law

The case of *Cemalettin Canli v. Turkey*⁶⁷³ provides guidance in respect of the use made by public authorities of information records and, in particular, the Court's observations vis-à-vis data quality. The *Cemalettin Canli* case concerned false claims made within a police report that the applicant contended had had adverse effects on his private life within the meaning of Article 8 of the Convention, particularly insofar as the information had been circulated more widely by the media. Of importance in our consideration of the handling and procedural safeguards given to personal records is that the judgment noted that the report: "...included the applicant's fingerprints, address and birth registry details, had been drawn up in accordance with Article 12 of the Police Regulations on Fingerprinting, which empowered the police to keep such details on persons accused or convicted of certain offences."⁶⁷⁴ The Court noted that the Council of Europe had examined questions regarding data protection and cited provisions within the Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, the purpose of which it noted was: "to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined in Article 2 as "any information relating to an identified or identifiable individual".⁶⁷⁵

The Court subsequently noted that the inaccurate nature of the information contained in the police report was not disputed, and that the referral to the applicant as a "member" of the organisation in question in the police report had been potentially damaging to his reputation. Of particular relevance then to our assessment is the Court's subsequent referral to *Pfeifer v. Austria*, where it reiterates that a person's right to the protection of his or her reputation as being encompassed by Article 8 as

⁶⁷³ *Cemalettin Canli v. Turkey*, No. 22427/04, 18 November 2008

⁶⁷⁴ *Cemalettin Canli v. Turkey*, No. 22427/04, 18 November 2008, §10.

⁶⁷⁵ *Cemalettin Canli v. Turkey*, No. 22427/04, 18 November 2008, §17.

being part of the right to respect for private life.⁶⁷⁶ The Government had defended the actions of its public authorities, namely the police force, in that whilst the drafting of the report was to be regarded as an interference with the applicant's rights under Article 8 of the Convention, it had been in accordance with the domestic legislation in force at the time and, furthermore, it had "been necessary in a democratic society in the interests of public safety and the prevention of disorder." However, in the opinion of the Court the authorities had failed to implement procedural safeguards provided for by domestic law for the protection of the individual's rights under Article 8. Thus the Court held that the drafting of the report had not been "in accordance with the law".⁶⁷⁷

The ruling of the Court therefore is especially pertinent to our review of the use of records by public authorities and the possible implications of the further development of novel forms of biometric identifiers in that, where in domestic legislation legal safeguards exist for the protection of the fundamental rights of privacy and personal data protection, these need closely be observed and adhered to. Clearly it is not merely sufficient that the necessary protections exist under law, but that the laws are followed such that the safeguards are meaningfully adhered to and implemented. Compliance with the protective safeguards within Article 8 of the ECHR also inheres an obligation of public authorities to ensure the accuracy of such personal records, particularly as a person's right to the protection of his or her reputation is encompassed by Article 8 as being part of the right to respect for private life. It can be contended that the scope for possible interferences in this right in connection with reputation may be even more widely engaged where the processing of an individual's location data in conjunction with other forms of personal data might indeed allow for the development of very detailed, complex profiles of the private life of the person concerned.

⁶⁷⁶ *Cemalettin Canli v. Turkey*, No. 22427/04, 18 November 2008, §36; *See, also: Pfeifer v. Austria*, no. 12556/03, § 35, ECHR 2007, and the cases cited therein.

⁶⁷⁷ *Cemalettin Canli v. Turkey*, No. 22427/04, 18 November 2008, §§38, 43.

6.3 Necessary in a democratic society

In *Z v. Finland*⁶⁷⁸ the Strasbourg Court, in discussing the respective arguments of the parties concerned, reviewed whether applicant's right to respect for her private and family life under Article 8 had been interfered with in a manner that could not be said to have been 'necessary in a democratic society'. Relevant here in the context of understanding the possible challenges presented should a public authority avail itself of sensitive health-related data was the Court's disquiet in having observed that "there was no indication that the police had exercised their discretion to protect at least some of the information emanating from the applicant's medical records, notably by excluding certain material from the investigation file."⁶⁷⁹

This pronouncement therefore provides clear guidance as to the need for public authorities to exercise the relevant degree of discretion and a responsibility of care in respect of their handling of sensitive personal data. In *Z. v. Finland* the Court also gave particular attention to the appraisal of the importance of the protection of personal medical data as part of its review as to whether, in the light of the case as a whole, the reasons adduced to justify the impugned measures were relevant and sufficient and, furthermore, whether the measures were proportionate to the legitimate aims pursued. The Court asserted that the protection of medical data is vital not only to "respect the sense of privacy of a *patient*, but also to preserve his or her confidence in the *medical profession* and in the *health services in general*."⁶⁸⁰ The aforementioned citation from the *Z. v. Finland* case thus illustrates a salient point as regards the principle of the special status afforded medical data due to its sensitivity; the Court referred to the principle of patient confidentiality in the wider context of preserving trust in the "medical profession" and "health services" *in general*. In this respect a principal issue therefore is how the established notions pertaining to the sensitivity of medical data are to be transcribed in the inception of novel forms of health data that include biometric identifiers based on individual's movements. A pertinent question in this context might be whether the trust of the individual need be

⁶⁷⁸ *Z v. Finland*, judgment of 25 February 1997, *Reports of Judgments and Decisions* 1997-I

⁶⁷⁹ *Z v. Finland*, judgment of 25 February 1997, *Reports of Judgments and Decisions* 1997-I, §83

⁶⁸⁰ *Z v. Finland*, judgment of 25 February 1997, *Reports of Judgments and Decisions* 1997-I, §95.

Note: *emphasis added*.

considered with regard to other parties privy to such information. Thus, the Court rightly noted that the broader issue of trust in the safeguard of personal data observably concerns the notion that, without such protection, “those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary...”⁶⁸¹ This concern is especially important where we consider that the very essence and nature of health data is now potentially subject to a substantial transformation, whereby a person’s simple everyday movements are subject to a process of transcription and interpretation through data collection and processing. The problem, therefore, being that in itself the opacity of such a process may further dissuade citizens from revealing such information, in turn also possibly endangering others in the community.

We may also consider the Court’s pronouncement as regards data controllers and the risks of inappropriate disclosure or data processing where personal data pertains to a person’s health status; the ECtHR having noted that in certain cases (corresponding to medical conditions, namely HIV infection, to which a certain stigma had been attached) disclosure of such data “...may dramatically affect his or her private and family life, as well as social and employment situation, by exposing him or her to opprobrium and the risk of ostracism.”⁶⁸² It is not over-imaginative nor unrealistic to foresee the possibility that other medical conditions to which certain stigmas are still attached, and for which diagnosis utilizing forms of mobility-related location data and associated biometric identifiers may prove attainable, could in the future similarly be disclosed. For instance, a number of research papers have already indicated the viability of embedded sensors in networked IoT devices and wearables to facilitate the diagnosis of neurological disorders and medical conditions such as Alzheimer’s and Parkinson’s disease.⁶⁸³ In *Z. v. Finland* the Court elucidated its position on the

⁶⁸¹ *Z v. Finland*, judgment of 25 February 1997, *Reports of Judgments and Decisions* 1997-I, §95.

⁶⁸² *Z v. Finland*, judgment of 25 February 1997, *Reports of Judgments and Decisions* 1997-I, §96.

⁶⁸³ *See, for example:* Donghee Son et al, Multifunctional wearable devices for diagnosis and therapy of movement disorders, *Nature Nanotechnology* 9, pp. 397–404 (2014) Available at: <http://www.nature.com/nnano/journal/v9/n5/abs/nnano.2014.38.html>; D. Campbell Dewey et al, Automated gait and balance parameters diagnose and correlate with severity in Parkinson disease, 15 October 2014, *Journal of the Neurological Sciences*, Volume 345, Issues 1-2, Pages 131–138, Available at: <http://dx.doi.org/10.1016/j.jns.2014.07.026>; Walter Maetzler et al, Quantitative wearable sensors for objective assessment of Parkinson's disease, October 2013, *Movement Disorders*, Volume 28, Issue 12, pages 1628–1637, Available at: <http://10.1002/mds.25628>. Moreover, recent research has also identified the viability of discerning cognitive impairments and issues pertaining to the mental health of an individual; these research findings in particular herald concerns with respect to the

factors it considered in assessing the proportionality of measures in respect of the legitimate aims pursued, in particular as regards the interests of protecting the confidentiality of information: this assessment proving germane to an evaluation as to the permissibility of actions pertaining to the possible use of personal location data by which biometric identifiers and health-related inferences may be drawn. The Court affirmed:

“The interests in protecting the confidentiality of such information will therefore weigh heavily in the balance in determining whether the interference was proportionate to the legitimate aim pursued. Such interference cannot be compatible with Article 8 of the Convention (art. 8) unless it is justified by an overriding requirement in the public interest.”⁶⁸⁴

In determining the proportionality of any interference, therefore, we need consider that the use of location data in relation to monitoring an individual’s movement can provide substantiation of many intimate and sensitive health-related conditions. Any proportionality assessment would need to consider the capacity of the individual affected to comprehend the nature of the data processing and analysis conducted, which may prove especially complex where, for the layperson with little technical knowledge, their discerning exactly how attributes of their physiology are subject to such measurements proves unfeasible. The Court did however note that this requirement would at the same time be balanced by the needs of the individual concerned and the wider good of the community, particularly as regards “the confidentiality of medical data may be outweighed by the interest in investigation and prosecution of crime and in the publicity of court proceedings.”⁶⁸⁵

protection of personal data and the safeguard of a person’s right to privacy. In addition, the possibility of indirectly detecting and monitoring changes in the individual’s mental state has also been observed where mental health metrics are recorded. *See*: Pablo Paredes, David Sun, John Canny, Sensor-less Sensing for Affective Computing and Stress Management Technology, December 2013, Available at: <http://bid.berkeley.edu/stressmanagement/wp-content/uploads/2013/12/sensorless-sensing.pdf>, pp.1-2.

⁶⁸⁴ *Z v. Finland*, judgment of 25 February 1997, *Reports of Judgments and Decisions* 1997-I, §96

⁶⁸⁵ *See*: *Z v. Finland*, judgment of 25 February 1997, *Reports of Judgments and Decisions* 1997-I, §§96-97.

7. Location data as a biometric identifier: determining the way forward

The capabilities of behavioural biometrics vis-à-vis identification of individuals have developed considerably. The notion that they are insufficiently precise to identify persons with a high degree of accuracy is no longer tenable; currently, the potential to discriminate between individuals based on behavioural observations and analysis is now extremely well developed.⁶⁸⁶ Nonetheless, trepidation toward biometric systems remains, with some citizens fearing their implementation may erode their individual rights to privacy and personal data protection. Understanding the development of new forms of biometric identifiers based upon location data relating to an individual's movement is of vital importance. Enhancements in discrete sensing devices are leading to the institution of ever more elaborate and precise monitoring capabilities that effectively digitize the human body as a subject of monitoring. This process has both a physiological and a psychological dimension, embracing the interconnection of an individual's body to networked devices that monitor actions and activities. This collection and processing of personal data could foreseeably yield information that influences automated decision-making that facilitates profiling and the categorization of individuals' traits and proclivities according to differentiated categories of risk.⁶⁸⁷

The development in behavioural biometrics that utilizes data collected in relation to an individual's movement constitutes an example of the merging of the digital and non-digital spheres. In this regard, institutions charged with the oversight of the implementation of data protection safeguards in the European sphere such as the

⁶⁸⁶ For example, ENISA has highlighted that the use of behavioural biometrics relating to movement and mobility can allow for the collection of personal data from which can be derived incidentally particularly sensitive information relating to the individual. ENISA has affirmed that: "gait features may reveal emotional features such as depression." This issue is important therefore as there may be a correlation between the biometric measurement based on the collection of personal data and other more sensitive features of an individual's particular profile that relate to their state of health, including their psychological condition. ENISA, ENISA Briefing: Behavioural Biometrics, 5 February 2010, Available at: <https://www.enisa.europa.eu/activities/risk-management/files/deliverables/behavioural-biometrics>, p.4 "gait features may reveal emotional features such as depression." ENISA, ENISA Briefing: Behavioural Biometrics, 5 February 2010, Available at: <https://www.enisa.europa.eu/activities/risk-management/files/deliverables/behavioural-biometrics>, p.4. See also: Yves-Alexandre de Montjoye et al, Unique in the Crowd: The privacy bounds of human mobility, Nature.com - Scientific Reports 3, Article number: 1376, 25 March 2013, Available at: <http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html>, pp.1-5

⁶⁸⁷ See: Van der Ploeg, I., 'Biometrics and the body as information - Normative issues of the socio-technical coding of the body', in Lyon, David. Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination. London: Routledge, 2003, p.62

EDPS have highlighted the challenges of this convergence, outlining that such a transformation infers a development of parallel domains, comprised of the ‘real’ and ‘digitized worlds’.⁶⁸⁸ The boundaries between these two environments are becoming increasingly indistinct, thereby creating a seamless space in which each individual moves and establishes distinctly personal traces of their mobility.

This phenomenon of convergence possibly heralds significant complications for regulation and governance, and underscores the necessity of determining how to coherently apply the existing legal frameworks for privacy and data protection so as to avoid creating legal uncertainties, or undermining the confidence of citizens that their fundamental rights are to be protected. The transformation in traditional distinctions made between seemingly quite distinct types of data, such as location data and health data, renders previous concrete and distinct categorizations indeterminate and complex to resolve. Taking these developments into consideration, it is not difficult to foresee possible challenges that such activity might present to the protection of privacy and personal data. As an example, the Opinion of the Advocate General in the *Digital Rights Ireland* case draws attention to the difficulties of construing intelligibly the essential characteristics that personal data inheres, particularly as regards differentiation as to the sensitivity of the data in question. Interestingly, the effort is characterised by its rather unwieldy articulation and abstruseness; it struggles to coherently articulate how distinctions can be delineated, absent applying rather subjective criteria to any such assessment. The Advocate General’s Opinion states:

“There are data that are personal as such, that is to say, in that they individually identify a person, such as data which, in the past, could *appear* on a safe-conduct, by way of example. Such data frequently have a certain permanence and are *frequently somewhat neutral* too. They are personal but no more than that and, in general, *it could be said* that they are those for which the structure

⁶⁸⁸ The EDPS affirms that the fundamental challenge in this respect is the need to reconcile the online and offline environments such that there be “a single harmonised umbrella or at least to provide an enhanced interoperability between them”. See: EDPS, Internet of things: ubiquitous monitoring in space and time, European Privacy and Data Protection Commissioners’ Conference Prague, Czech Republic, 29 April 2010, Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Internet_Things_EN.pdf, p.3

and guarantees of Article 8 of the Charter are best suited.

There are, however, data which are *in a sense* more than personal. These are data which, qualitatively, relate essentially to private life, to the confidentiality of private life, including intimacy. In such cases, the issue raised by personal data commences, *so to speak, further 'upstream'*. The issue which arises in such cases is not yet that of the guarantees relating to data processing but, at an earlier stage, that of the data as such, that is to say, the fact that it has been possible to record the circumstances of a person's private life in the form of data, data which can consequently be *subject to information processing*.⁶⁸⁹

The opinion proceeds rather awkwardly in affirming that “in a sense” it is “possible to argue that” the aforementioned distinctions might be applied so as to appropriately determine the correct application of the rights safeguards afforded by Articles 7 and 8 of the EUCFR.

“It is in that sense that *it is possible to argue that*, when such data are involved, they raise an issue which essentially precedes that of their processing, relating primarily to the privacy guaranteed by Article 7 of the Charter and only secondarily to the guarantees concerning the processing of personal data referred to in Article 8 of the Charter.”⁶⁹⁰

The language employed in this line of reasoning does little therefore to clarify and resolve how we effectively distinguish the scope of the rights concerned. The primary issue with the above-cited contention is that the declaration creates a certain opacity in distinguishing between the following data types: personal data; special categories of personal data, and data which falls into the former, but may become the latter should it be subject to processing that reveals for sensitive aspects of a data subject's private life. The premise constitutes a very problematic principle in terms of its

⁶⁸⁹ Note: *emphasis added*. OPINION OF ADVOCATE GENERAL CRUZ VILLALÓN - JOINED CASES C-293/12 AND C-594/12 DIGITAL RIGHTS IRELAND AND OTHERS - ECLI:EU:C:2013:845, 12 December 2013, Available at: <http://curia.europa.eu/juris>, paras. 64 & 65

⁶⁹⁰ Note: *emphasis added*. OPINION OF ADVOCATE GENERAL CRUZ VILLALÓN - JOINED CASES C-293/12 AND C-594/12 DIGITAL RIGHTS IRELAND AND OTHERS - ECLI:EU:C:2013:845, 12 December 2013, Available at: <http://curia.europa.eu/juris>, para.66

capacity to guarantee the necessary legal certainty and foreseeability required for parties to exercise the necessary judgment as to the lawfulness of any envisaged data collection or processing activities.⁶⁹¹ A more definitive line of argumentation is required to furnish an apposite conceptualisation of the underlying distinctions. As such, the opinion is categorically deficient, based on its inordinate degree of vacillation. The ubiquitous collection of personal data pertaining to an individual's location and physical condition for the purposes of establishing profiles based on behavioural biometrics reflects an augmentation in the pervasive monitoring capabilities of individuals in both public and private spaces.⁶⁹²

Where monitoring, data collection and processing pertaining to an individual's behavioural biometrics may be achieved in a discrete manner the convenience and lack of perceptible intrusion and obtrusiveness may obscure the concealment of highly intrusive surveillance of a person's movements. In terms of the level of interference such intrusions constitute in respect of the individual's right to privacy, freedom of movement, and right to the protection of their personal data, the configuration, implementation and actual use of the technology will constitute critical aspects as to examining and assessing the impact of its operation. The utilization of behavioural biometrics engages very real concerns as to the effect its use might have on the development of individual identities based on interferences in bodily integrity,

⁶⁹¹ Scholars such as Morel and Prins have offered a pessimistic assessment of the future in this regard, despite the changes heralded with the ongoing reform of the EU's data protection framework; they contend that the strengthening of the information and consent requirements will neither improve the position of data subjects nor give them more control over data processing. Rather, they believe that the underlying logic of data-processing operations and the purposes for which they are used have become so invariably complex that the average citizen cannot comprehend them. *See further*: Moerel, Lokke & Prins, Corien, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things* (May 25, 2016). Available at: <https://ssrn.com/abstract=2784123>, p.9

⁶⁹² In particular, the pervasiveness of devices capable of capturing such data has raised concern. The Federal Trade Commission in the United States has underscored the challenge this collection and processing of personal data relating to our behaviours represents, noting that in the near future: "many, if not most, aspects of our everyday lives will leave a digital trail. That data trove will contain a wealth of revealing information that, when patched together, will present a deeply personal and startlingly complete picture of each of us". *See*: FTC, *Opening Remarks of FTC Chairwoman Edith Ramirez Privacy and the IoT: Navigating Policy Issues, International Consumer Electronics Show Las Vegas, Nevada, 6 January 2015*, Available at: http://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf, p.3. Richards's scholarship too has noted that, as we increasingly use portable and wearable computers to capture data about others and ourselves, questions as to the appropriate limits on data collection in public will continue to arise. Richards, N. M., *Intellectual Privacy - Rethinking Civil Liberties in the Digital Age*, (2015), Oxford University Press, Oxford, p.71

even where this is achieved without immediate contact or consciousness i.e. covertly. Previous research on the use of embedded biometric sensing technologies in public spaces has identified significant concerns as regards the awareness of such systems, and their capabilities in establishing ‘anticipatory conformity’ whereby citizens attune themselves to pervasive monitoring of their movements and adopt patterns of behaviour they believe will make them less likely to be subject to harassment, discrimination or unwanted scrutiny by public authorities concerned with public security.

Implementation of behavioural biometrics in any surveillance of a population also inheres specific risks associated with categorization based on distinctions drawn from observed patterns of mobility.⁶⁹³ A primary concern is that of the extension of inferences from the monitoring of bodily parameters, relating patterns of movement in correlations with respect to certain emotional or mental states. In addition, the Opinion of Advocate General Cruz Villalón is also pertinent in this particular context where we consider the interrelationship between privacy and data protection and the normative delineation of the two. Indeed, especially enlightening is the notion articulated by the Advocate General as to the capacity of personal data to, in essence, morph between different states of sensitivity. Advocate General Cruz Villalón notes:

“The data in question, it must be emphasised once again, are not personal data in the *traditional sense of the term*, relating to specific information concerning the identity of individuals, but ‘*special*’ personal data, the use of which may make it possible to create a both faithful and exhaustive map of a large portion of a person’s conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity.”⁶⁹⁴

Moreover, an additional concern raised in respect of the more widespread deployment of monitoring using location data for the purposes of generating biometric identifiers is the notion of ‘function creep’. The greater technical capacities of future information

⁶⁹³ See: Byrne, J.M., (2008) ‘The best-laid plans: an assessment of the varied consequences of new technologies for crime and social control’. Fed. Probat. 72(3): pp.10-21

⁶⁹⁴ Note: *emphasis added*. OPINION OF ADVOCATE GENERAL CRUZ VILLALÓN - JOINED CASES C-293/12 AND C-594/12 DIGITAL RIGHTS IRELAND AND OTHERS - ECLI:EU:C:2013:845, 12 December 2013, Available at: <http://curia.europa.eu/juris>, para.74

technology systems may allow for the repurposing of sensitive data collected.⁶⁹⁵ In the realm of privacy protection, irreversibility is a decisive concern; in the context of new technological advancements risks are frequently uncertain. As such, if precautionary steps are not taken any loss or impediment incurred to existing safeguards might plausibly be characterised as irreversible.⁶⁹⁶

8. Conclusions

The application of location data processing to develop biometric data, including behaviometric quantification of individuals' physiologies, risks rendering a chilling effect on the data subject's enjoyment of their fundamental rights. More broadly, citizens' behaviour may be influenced by the knowledge of monitoring, such that the ability to function truly autonomously is seriously challenged. Furthermore, certain people might either consciously or subconsciously conform so as not to solicit unwelcome attention from other parties due to a behavioural pattern proving dissimilar from the anticipated norm, ostensibly generating cause for suspicion. Bauman and Lyon have noted that behaviometrics risk allowing for data from the body to be processed and analysed to form a 'data double' of the individual concerned, suggesting that the "...information that proxies for the person is made up of 'personal data' only in the sense that it originated with a person's body and may affect their life chances and choices. The piecemeal data double tends to be trusted more than the person."⁶⁹⁷ More broadly, we might reflect on the warnings tendered by those such as Erin Murphy, who has warned of the future difficulties the use of location-based technologies could present, asserting that "many of the characteristics that make second-generation sciences so appealing in fact places them at equal, if not greater, risk for error in the current regime... the technical complexity of second-generation techniques make close and continuous judicial scrutiny of their methodological soundness less likely." Moreover, Murphy forewarns that, despite the

⁶⁹⁵ See: WP29, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, 27 April 2012, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/>, p.17

⁶⁹⁶ See: Sunstein, Cass R., *Irreversibility* (July 12, 2008). Oxford University Press, Law, Probability and Risk, Forthcoming; Harvard Public Law Working Paper No. 08-25; Harvard Law School Program on Risk Regulation Research No. 08-1. Available at: <https://ssrn.com/abstract=1260323>, p.1

⁶⁹⁷ See: Bauman, Zygmunt, and David Lyon. *Liquid surveillance: A conversation*. John Wiley & Sons, 2013, p.113

heightened likelihood of error, courts may feel discouraged from delving too deeply into complicated and seemingly inaccessible science. Accordingly, Murphy suggests that those that believe cell phones and GPS satellites “generally work” in the world may be less inclined to question whether, when put to forensic purposes, the methodological underpinnings remain sound.⁶⁹⁸

A possible approach might embrace the precautionary principle, which determines that one avoids taking steps that would otherwise create a risk of harm.⁶⁹⁹ Where the protection of the rights to privacy and personal data are engaged, the safeguards to the individual embodied therein must be given relevance and applied in the context of behavioural biometrics.⁷⁰⁰ The importance of establishing the conditions that facilitate a sound and coherent framework for well-reasoned purpose specification is evidently linked to the connected concepts of transparency, predictability and the user exercising the requisite degree of control in relation to collection of their personal data.⁷⁰¹ In addition, the capacity of data subjects to comprehend the extent, context and detail of any data processing they are subject to has been highlighted as a particular concern. Defining stringent safeguards to protect data subjects from impermissible data processing activities stemming from the disregard of purpose limitation represents a critical measure in preserving an individual’s fundamental rights in terms of both data protection and privacy. The erosion of compliance with this principle would inhere an ensuing degradation of other related data quality principles. Furthermore, the risks in relation to profiling based upon automated

⁶⁹⁸ See: Murphy, E., 2007. The new forensics: Criminal justice, false certainty, and the second generation of scientific evidence. *California Law Review*, pp. 768-769

⁶⁹⁹ However, it should be noted that certain scholars, such as Sunstein, have warned that the application of the principle cannot always be defended: “... simply because risks are on all sides of social situations. Any effort to be universally precautionary will be paralyzing, forbidding every imaginable step, including no step at all.” See: Sunstein C. R., *Beyond The Precautionary Principle*, The Chicago Working Paper Series, January 2003, Available at: <http://www.law.uchicago.edu/Lawecon/index.html>, p.3; O’Riordan, T. and Cameron, J. (eds.), 1994. *The history and contemporary significance of the precautionary principle. Interpreting the precautionary principle*, Cameron May Ltd.

⁷⁰⁰ Interestingly, the Assistant European Data Protection Supervisor asserted in a 2010 address on the topic of IoT governance that, regarding privacy and security of personal information, “we need to *use our imagination* to find new ways to apply these principles in the new, evolving information and communication technologies scenario.” Note: *emphasis added*. See: EDPS, *Internet of Things: ubiquitous monitoring in space and time*, European Privacy and Data Protection Commissioners’ Conference Prague, Czech Republic, 29 April 2010, Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Internet_Things_EN.pdf, p.4

⁷⁰¹ WP29, *Opinion 03/2013 on purpose limitation*, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy/>, pp.13-14

processing and decision-making and the prediction of behaviours and preferences has also been raised.

Significant risks also arise from the repurposing of data and the possible use of biometric identifiers in revealing an individual's physical characteristics for the purposes of individual profiling and targeting. Should such activities emerge, they may well result in greater stigmatisation and discrimination of individuals stemming from possible biases introduced into the identification systems by the design of their data processing operations.⁷⁰² Also pertinent to this discussion regarding purpose limitation is the issue of the appropriacy of exerting that a data subject's consent is made on an informed basis where the nature of subsequent processing activities may be indeterminate, due in part to the complexity of articulating the type of analysis being performed on somewhat esoteric aspects of human mobility that relate to barely perceptible physiological attributes as discerned by the ordinary citizen. Increasingly anatomies, in conjunction with our particular physiologies, are becoming 'informatised'. Moreover, with the advancement of behaviometrics ever more discrete and often barely perceptible motions and gestures are being regarded as incontrovertible evidence as to both the identity and the persona of an individual. Scholars such as Van der Ploeg have raised concerns that this tendency risks the bodily integrity of citizens.⁷⁰³ Bauman and Lyon too have expressed concern that the implementation of behaviometrics is a reductive process; the scholars assert that: "in numerous surveillance situations, bodies are reduced to data... One cannot but conclude that information about that body is being treated as if it were conclusive in determining the identity of the person."⁷⁰⁴

The further development of the capability to create biometric identifiers that relate to the individual data subject based upon the collection and processing of personal data that includes location data requires more adequate resources be committed to identify how information regarding the scope of this activity is to be comprehensibly

⁷⁰² See: WP29, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, 27 April 2012, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/>, p.17

⁷⁰³ See: Van der Ploeg, Irma. *The Machine-readable Body: Essays of Biometrics and the Informatization of the Body*. Maastricht, Shaker Publishing, (2005), p.94

⁷⁰⁴ Bauman, Zygmunt, and David Lyon. *Liquid surveillance: A conversation*. John Wiley & Sons, 2013, p.113

communicated to the citizens concerned. Absent such a provision, choices exercised on the part of data subjects cannot be held to be made with informed consent; thus the data protection safeguards that would subsequently then apply become incidental, as there exists no primary basis for the data processing in the first instance. The WP29 have also recounted that meaningful purpose specification is reliant upon conditions that afford the data subject sufficient transparency in apprehending the scope of a data processing activity, and that they may also be reasonably able to predict the consequences that stem from their decision making in respect of the processing of their personal data.⁷⁰⁵ Furnishing sufficient clarity in terms of providing the necessary detail in purpose specification is therefore vital, whereby it in turn presents the requisite conditions for the foreseeability that enables citizens to make freely informed decisions, ensuring a guarantee of legal certainty as regards upholding the rights of data subjects. This understanding also reflects the importance of comprehending how recognition of the challenges presented by the use of location data in biometrics can also highlight broader concerns vis-à-vis data processing. In this respect the discussion heretofore may also prove illuminative and facilitate the development of further investigation where innovations herald novel and as yet undiscovered uses for location data in modelling and depicting human attributes for the purposes of distinguishing between different individuals.

⁷⁰⁵ See: WP29, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy/>, p.13.

Chapter 7: Conclusions

This research has shown that whilst the themes of locational privacy; perceptions of space and time, and their influences in respect of our identities are all at times seemingly esoteric and complex considerations to comprehend, they can however be conveyed in a manner such that the layperson may understand how these concerns affect their enjoyment of their fundamental rights. Whilst distinctions and precedent have been drawn in law whereby certain types of spaces have been categorised as constituting an area affording the protection of privacy, it is now the case that we apprehend the nature of the changing relationship that different geographic spheres occupy within the human conscience and, in consequence, the performative roles they enact. As has been asserted by scholars such as Lessig, the constitution and composition of the environment that we ourselves develop within as a society is not a product purely of the enactment of laws; rather the manner in which we conceive of an implement technological innovations also plays an essential role. As such, a critical task is that of creating a shared framework of complimentary legal and technical parameters and restraints that provide a cohesive and coherent regulatory architecture that provides operable safeguards for the citizen, whilst at the same time facilitating beneficial innovations in data collection and processing activities.⁷⁰⁶ The difficulties of coherently articulating the appropriate application of the existing legal framework to the use of location data for the purposes of developing identifiers, metrics and profiles relating to the individual must also appreciate the inescapable compromises inherent to the transposition of technical concepts into regulatory instruments. This problem is further compounded by the practical requirements of developing rules that are sufficiently accessible to those lacking a technical understanding.

The movement of individuals is increasingly mediated by all manner of technologies

⁷⁰⁶ See: Lessig, L., *Code: Version 2.0*. New York: Basic Books, 2006. See also: Leenes, Ronald E. and Koops, Bert-Jaap, 'Code' and Privacy - Or How Technology is Slowly Eroding Privacy. *Essays On The Normative Role Of Information Technology*, T.M.C. Asser Press, The Hague, Netherlands, 2005. Available at: <https://ssrn.com/abstract=661141>, p.164 See also: Reidenberg, J.R., 1997. *Lex informatica: The formulation of information policy rules through technology*. *Tex. L. Rev.*, 76, p.553.

that facilitate our navigation. Locational privacy is a specific type of privacy, and is necessary to protect broader aspects of our civil liberties that stem from our ability not just to move freely, but also to engage and interact with others, to exercise the freedom to search and discover that which is inherent to the development of our own thoughts — and which is hence an intrinsic element of an individual’s autonomy and identity. Locational privacy is pivotal in respect of facilitating interactions, associations and relational ties with others, rather than simply afford a degree of independence from people in other settings. A binary distinction that reflects the conceptualisation of the right to privacy as a negative right, with related concepts such as identity and personality formation as positive, are increasingly difficult to maintain.

It is important to appreciate that both our reflexes toward and interactions with technology are, on a human level, highly contextualized. Citizens’ reactions to the processing of information are inseparable from their interests, desires, resources, cognitive capacities and social contexts. As Heidegger has indeed observed, the essence of technology is by no means anything technological.⁷⁰⁷ Furthermore, social norms that would have once been considered inhibiting may well eventually be fully internalised and pursued unconsciously. Locational privacy may be construed therefore as a form of ‘expressive privacy’. DeCew has referred to ‘expressive privacy’ in the context of autonomy as a socially embedded notion, suggesting that this independence is a pre-requisite for self-expression that enables the individual to exercise control over engagement with others to form new and deeper relationships, shape one’s life and values.⁷⁰⁸ The intrinsic rationale of personality is in essence the creation of the self, on self-development and the realisation of one’s own potential. As such, personality reflects a positive state, whereby the individual is afforded scope within her surrounds to develop her own identity and create her persona. Macklem argues in this respect that the “isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is

⁷⁰⁷ Martin Heidegger: Basic Writings, ed. David Farrell Krell, trans. William Lovitt, New York: Harper & Row, 1977, p.287

⁷⁰⁸ Judith DeCew, In Pursuit Of Privacy: Law, Ethics And The Rise Of Technology 77 (1997), p.69

sponsor and guardian to the creative and the subversive.”⁷⁰⁹ Locational privacy is crucial in this respect as it shapes the conditions in which social interactions within a certain milieu can occur.

It is also possible that locational privacy may be progressively eroded as technologies develop and extend their influence on how we choose to enact our own choices concerning mobility. Particularly conspicuous is the evolution of information sharing more generally amongst the population, the manifest acceptance of which on the part of many citizens would suggest that attitudes toward interferences in privacy and data protection rights are subject to a process of sustained recalibration vis-à-vis developing social mores. The value of locational privacy extends beyond its more immediately understandable spatial criteria; its intrinsic worth is substantially broader insofar as it cultivates both cognitive and expressive processes through which citizens can nurture ideas for themselves. These activities are critical for self-development and require the liberty to contemplate and deliberate without deterrence or interference from other parties. Deprived of locational privacy one is less able to explore and test thoughts and opinions; it allows us therefore to assess and appraise ideas in comparative seclusion, thereby providing reassurance and a shield from a scrutiny that might otherwise inhibit and provoke anxiety.

At this point we are in a unique position where we can influence changes in the architecture of evolving information technology systems that will stand for decades. In this context we might also consider the Opinion provided by the Advocate General Cruz Villalón in the *Digital Rights Ireland* case,⁷¹⁰ which was notable for its commentary regarding the relationship between the respective rights to privacy and data protection and, particularly, with respect to the latter right being subject to “an autonomous regime”.⁷¹¹ Data protection legislation is not aimed at the protection of

⁷⁰⁹ Macklem T., *Independence of Mind* (2006), Oxford University Press, p.36. Similarly, Julie Cohen argues in a similar vein that privacy shelters dynamic, emergent subjectivity from actors to “render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops.” See: Cohen, Julie E., *What Privacy Is For* (November 5, 2012). Harvard Law Review, Vol. 126, 2013. Available at: <http://ssrn.com/abstract=2175406>, p.2

⁷¹⁰ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014.

⁷¹¹ Advocate General Cruz Villalón’s opinion states: “Article 8 of the Charter enshrines the right to the protection of personal data as a right which is distinct from the right to privacy. Although data protection seeks to ensure respect for privacy, it is, in particular, subject to an autonomous regime,

data *per se*, rather, as the formal title to the Directive 95/46/EC suggests (directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data) it concerns the protection of individuals. Furthermore, Article 1 of the aforementioned directive explicitly outlines the objective “to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.” This point is especially relevant to our contemplating the link between personal data, location and the individual. As Brandeis so presciently observed: “The logic of words should yield to the logic of realities.”⁷¹² In analyzing the historical distinctions drawn between content and metadata, one may appreciate how the basis for this differentiation was recognized and proved a coherent form of discrimination between fundamentally distinct types of data. However, recent technological advancements render this distinction obsolete. The distinction between content data and metadata is rapidly fading away in a modern network environment.

At this juncture we might also reflect on a parallel that exemplifies the necessity of a retaining a flexible approach to interpretation. Moreover, as was underscored in the *Google Spain* judgment at the CJEU, courts may increasingly prove willing to appraise the evolving capabilities of technologies as regards data processing by adopting relatively progressive procedures to interpreting the legal framework.⁷¹³ As a further illustration, the Opinion of Advocate General Bot in the *Schrems v. Data*

primarily determined by Directive 95/46, Directive 2002/58, Regulation No 45/2001 and Directive 2006/24 and, in the field of police and judicial cooperation in criminal matters, by Framework Decision 2008/977/JHA.” OPINION OF ADVOCATE GENERAL CRUZ VILLALÓN - JOINED CASES C-293/12 AND C-594/12 DIGITAL RIGHTS IRELAND AND OTHERS - ECLI:EU:C:2013:845, 12 December 2013, Available at: <http://curia.europa.eu/juris>, para. 55

⁷¹² Louis D. Brandeis. 273 U.S. 34, 47 S.Ct. 267, 71 L.Ed. 524, *Di Santo vs. Commonwealth of Pennsylvania*.

No. 288. Argued Oct. 27, 1926. Decided Jan. 3, 1927.

⁷¹³ The ECJ judgment asserted: “It must be pointed out at the outset that, as has been found in paragraphs 36 to 38 of the present judgment, processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual’s name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which *potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty* — and thereby to establish a more or less detailed profile of him.” Note: *emphasis added*. *Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014, para.80

*Protection Commissioner*⁷¹⁴ case at the CJEU is enlightening for its semantic deliberation of the framing of interpretative approaches to the relevant legal instruments pertaining to data protection. In particular, the opinion's contemplation of the appropriate application of the term "adequate" in the context of fundamental rights protection is revealing. Significantly, where the review elects to underscore the importance of recognising that in assessing the term "adequate" it is to be construed so as to infer a high level of protection of fundamental rights, it should be taken as a compelling indication that one must indeed invest sufficient effort to discern the nuances of the relevant instruments' formulations and nomenclature. The explanation given by the Attorney General, which furnishes an unusually expansive interpretation of so apparently banal a term as "*adequate*", highlights the necessity of appraising the possible impact engendered by each appellation and linguistic composition, however seemingly inconsequential the term may appear.⁷¹⁵

With the increased detail, usefulness and inherent privacy of information contained in communications metadata there is evidently a major qualitative difference today in the type of communications data as compared to that which was available even a decade ago. Thus the distinction that has established a greater intrinsic value in the content of communications versus that of communications metadata is growing ever more problematic. The differentiation is premised on the assumption that communications content is inherently more personal, of greater worth and more private than communications metadata. This proposition has become progressively more difficult to defend in the light of huge increases in the both the quantity of metadata collected and processing capacity capable of analysing personal information.

Rhetorical-legal constructions have shaped the construal of location data as a term and in its application, representing a development of the ontology of metadata. In

⁷¹⁴ Case C-362/14. Maximilian Schrems v Data Protection Commissioner

⁷¹⁵ See: the Opinion of Advocate General Bot in the Case C-362/14 Maximilian Schrems v Data Protection Commissioner, in which at paragraph 142 it is asserted: "Although the English word 'adequate' may be understood, from a linguistic viewpoint, as designating a level of protection that is just satisfactory or sufficient, and thus as having a different semantic scope from the French word 'adéquat' ('appropriate'), the only criterion that must guide the interpretation of that word is the objective of attaining a high level of protection of fundamental rights, as required by Directive 95/46.": OPINION OF ADVOCATE GENERAL BOT, Case C-362/14 Maximilian Schrems v Data Protection Commissioner, 23 September 2015, Available at: <http://curia.europa.eu/juris/>

relying on precedent in shaping regulatory instruments lawmakers frequently extend or devise new terms to reconcile gaps in existing conceptual approaches, especially where new technologies expose lacunae in the existing ontological framework.⁷¹⁶

The classification and terminology of technologies can illustrate how terms and legal metaphors are developed and applied so as to bridge gaps in applying existing context and precedent. Though the designation ‘location data’ once constituted a reasonable accommodation in nomenclature by furnishing a term that was once intelligible and easily comprehensible, even while constituting a significant oversimplification of the data it represented, technological advances have rendered the term increasingly problematic. This is all the more significant where, absent resolution of this concern, advances in technologies will further test the existing legal framework’s coherency as regards the collection and processing of personal data in the specific respect of location data. The term now reflects an antiquated perspective in respect of how the data concerned is subject to collection and processing. The term in the present-day may thus be conceived as more a metaphor than as an accurate description conveying a precise elucidation of the features of the data it is intended to represent. In the legal sphere, metaphors are more commonly used to convey concepts and notions figuratively, where new and complex advancements in technology defy simple elucidation; in the context of developing regulation to govern their use, figurative expression may thus allow lawmakers to convey in a more simple manner inherently impenetrable or abstract technologies.⁷¹⁷ The term ‘location data’ is too frequently construed in a very narrow sense, reflecting a misunderstanding as to the nature of the information contained therein.

⁷¹⁶ See also: Vee, A., 2012. Text, speech, machine: Metaphors for computer code in the law. *Computational Culture*, 2, p.1 Available at: <http://computationalculture.net/article/text-speech-machine-metaphors-for-computer-code-in-the-law>

⁷¹⁷ Vee asserts in this respect that “metaphors can illuminate the unstable identities for technologies when they are new”, noting: “Central metaphors for technologies can set the terms of legal discourse, initiating terms or defining them, therefore shaping the ways that subsequent subjects are treated under the law.” See: Vee, A., 2012. Text, speech, machine: Metaphors for computer code in the law. *Computational Culture*, 2, Available at: <http://computationalculture.net/article/text-speech-machine-metaphors-for-computer-code-in-the-law>, p.1. See also: Perelman, C. and Olbrechts-Tyteca, L., 1957. The new rhetoric. *Philosophy Today*, 1(1), pp.4-10, which provides a basis for understanding the use of narrative and metaphorical allusion in legal reasoning. See further: Bosmajian, H.A., 1992. *Metaphor and reason in judicial opinions*. SIU Press, regarding the judicial decisions presented through arguments developed by rational discourse and literal language. See also the discussion of rhetoric and law in: O'Rourke, Sean Patrick, Haig Bosmajian, Fredric G. Gale, Austin Sarat, and Thomas R. Kearns. "Metaphor and Reason in Judicial Opinions." (1995): pp.213-220.

Indeed, as early as the eighteenth century the importance of the distinction between temporal and spatial quantification was understood: prescient therefore is Kant's erudite observation that: "We can equally call both history and geography descriptions. The difference is the former is a description in terms of time; the latter in terms of space."⁷¹⁸ As has been elucidated heretofore within this review, the nomenclature of 'location data' has been shown to be deficient; the locution constitutes an insufficiently precise descriptor as regards the intrinsic information of the metadata to which it relates. It is erroneous to assume that the term 'location' adequately defines the wider scope of the data in question; the term is in essence an oversimplification. Whilst a cursory assessment might, in certain circumstances, appraise the close approximation that the term 'location data' constitutes to be sufficient, in actuality, while relatively straightforward for the layperson to comprehend, it is evidently too reductive. The term fails to connote a core dimension of the data inhered i.e. the temporal data. A more appropriate nomenclature would be that of 'spatio-temporal data'. The propensity to overlook the inherent value of the temporal data and, furthermore, the neglect of the utility the conjunction temporal and spatial elements represents, reflects a pervasive inability to apprehend the technical basis and intrinsic value of different data types. Such an approach is essentially poststructuralist, insofar as it questions whether we have adequately appraised the gaps and ambiguities in the structures of meanings and the ontological truths we perceive the data represents.

As regards the issue of data quality, a merit of the existing conceptual framework at the European level is that it remains technologically neutral; this approach must be preserved if their application is to continue in a logical and cogent manner. One needs appreciate that as citizens' comprehension of their association with their own mobility and interactions with others evolves, perspectives toward the worth of their personal data, particularly location data, may well transform too. To date we have observed but a partial shift; a far greater reevaluation of concerns linked to the monitoring of citizens' mobility will take considerable time. A significant re-examination and committed appraisal to the impact of the mass surveilling of citizens' patterns of

⁷¹⁸ Kant, I., 2004. *Kant: Metaphysical Foundations of Natural Science*. Cambridge University Press (first published 1786), p.448

movement is most probably only likely where the issues are given more prominence. Perhaps adjustments in attitudes and, indeed, an advance in consciousness of the right to freedom of movement, will occur only when more certainty is secured as to how its obstruction and curtailment inhibits our dignity and personal identity. Paradoxically, innovation can allow for location data collection and processing to foster and enhance a greater freedom of movement for citizens through a diverse range of enabling applications. Simultaneously, however, the persistence of obstacles to transparency and accessibility in respect of data quality and consent continue to compromise the value of potentially beneficial and efficacious location-based functionality and broader delivery of IT-enabled services. Even now, despite progress, there still remains plenty of scope for improvement as regards data quality with respect to spatial data. Understanding data quality in this context requires further disambiguation; in essence, all spatial data is inherently inaccurate to a degree, as it reflects only a conceptualization of the reality it tries to represent. The existing data protection legislation conceives of location data according to antiquated concepts of processing personal data and the feasibility of misuse; new methods of location data collection and analysis deliver markedly more insightful knowledge that harbours the capacity to penetrate deep into the privacy of an individual's dignity and identity.

A greater understanding of the utility of location data is certainly required. The hierarchy that delineates personal data from special categories of personal data, and provides for additional safeguards with respect to the latter, lacks the necessary flexibility to acknowledge the capacity for location data to act as a proxy for other sensitive data. The risk of identifying ever more intimate and nuanced detail of a citizen's life, behaviours and convictions through the analysis of their location data is clearly evident, and a cause for concern. A challenge therefore is the development of the regulatory framework that allows sufficient adaptability in this regard, thereby ensuring that protective measures that safeguard citizens' personal data are apt to acknowledge where certain types of content data, including location data, may act as proxies that inhere sensitive information.

The practice of modelling behaviours and generating profiles based on location data collection and processing is dependent upon the contention that an individual is reducible to the aggregation of their actions, activities and physical attributes as

manifested in their articulation of movement measured in a spatio-temporal setting; formulated summarily such that these traits prove compelling in forecasting other predictors of the individual. Whilst this hypothesis has a certain credibility insofar as much human behaviour on an individual level is repetitive, based primarily on reoccurring need, the manner in which we express our innate characteristics are not. Certain information that relates to the persona is intrinsically incapable of being measured or captured by sensing devices, or otherwise rendered subject to any form of data processing. Predictive determinations pertaining to one's future behaviour are far harder to dispute than determinations based upon the investigation of past behaviour. We need therefore recognise that elements of both the human psyche and our respective physiologies are conveyed only internally, and cannot therefore be meaningfully reproduced digitally for predicative purposes. The omnipresence of location data collection represents a real possibility in terms of instituting such changes. Should this happen, this prevalence may in time narrow our objectivity in respect of how we deliberate over the information the analysis of the data constructs, and how we subsequently frame our opinions and concerns. Society thus runs the risk of developing a dependence upon technology for solutions that the technical advances may themselves be largely responsible for, constituting a damaging self-referential feedback loop. Indeed, in this context we might well ponder Heidegger's reflection that technology may in certain circumstances inhere a decidedly inhibiting role in our self-appreciation, stating: "The essence of technology, as it shapes the ways in which we understand ourselves, our essence, is such to exclude other non-technological ways of understanding being."⁷¹⁹

Distinctions in terms of the constitution of our personal mobility, our patterns of movements and the manoeuvring between and in the online and offline worlds still remain opaque. Paradoxically, understanding how our mobility informs and influences our own identity still remains intrinsically complex to discern, despite the plethora of location data now being made available. Thus a relevant consideration in respect of our contemplating the harm of seemingly intangible interferences is the question of heuristics. In this respect, the public's demand for the protection of law will be greater where citizens' can perceive of the harm in question. If the harm is

⁷¹⁹ Heidegger, Martin. "The question concerning technology, and other essays." (1977), New York: Harper & Row, pp.287-317

otherwise complex to understand and appreciate, then it is very likely that the pressure for greater oversight and regulation will be diminished. It is therefore important that we duly consider the genuine palpability of interferences activities many precipitate. Hence, from a heuristic perspective the question therefore pertains to the familiarity of instances that would be recognisable as harmful by the individual concerned, or indeed by other parties. Should citizens be unable to contemplate cases in which a risk comes to fruition, unavailability bias may well then reflect an unjustified failure to appreciate the repercussions of a harmful practice implemented. Furthermore, rights have traditionally emphasised the individual's interests rather than that of groups or associations. However, the reality of new sensing technologies that can capture location data linking different persons' mobilities and interactions is that interferences and harm to welfare increasingly have a societal interest, and broader structural implications. Notwithstanding these concerns, as the uses of each individual's location data continue to evolve, innovations in location-based technologies may allow for the development of new knowledge that can ostensibly improve our quality of life. The commitment to protect locational privacy thus hinges upon a certain interpretation of a moral demand; namely the assertion that we should, as a society, protect individuals from interferences that risk harm to their personal autonomy and liberty. Furthermore, individual human mobility inheres an expressive capacity that aids the development of a person's identity. These capacities are characterised in indispensable and elemental aspects of the constitution of our selfhood and individuality. While recognising the benefits that the use of location data can provide in many spheres of modern life, we nevertheless need avoid a determinism shaped by evolving technologies to allow personal data collection and processing that compromises developing social norms and societal cohesion, as well as individuals' right to privacy and personal data protection.

Safeguarding an individual's enjoyment of their liberty and freedom from interference in accordance with the right to the protection of personal data is intrinsically of a different nature from that afforded by the right to privacy. Historically, the right to privacy has been subject to a prodigious degree of examination, interpretation and dispute. In part, the apparent intangibility of the notion itself has furnished ample opportunity for its conceptualisation to reflect wholly different elucidations influenced by a plethora of political, ethical and philosophical determinants. In

contrast, the capacity of the data protection framework to furnish effective measures to protect the individual is far more dependent on criteria premised upon substantive formulations that include of necessity established and inflexible definitions. In resolving to differentiate two distinctly separate rights, there exists a significant challenge insofar as human rights are in essence inter-dependent and indivisible. Indeed, more recently in the *Google Spain* case⁷²⁰ the CJEU again sought to highlight the interdependence of data protection as a right in relation to the safeguard of other fundamental rights, in particular the right to privacy.⁷²¹ Where data protection intersects with the right to privacy we see a persistent tension between the two, insofar as the two inhere distinctly different mechanisms to frame, appraise and adjudicate the gravity of the interference an action may represent to the individual concerned. As such, there persists an essential tension integral to the co-existence of rights conceived of as conceptually interconnected, yet of requirement, both substantively and normatively, formulated distinctively in specification and qualification.

This body of research examining the designation and use of location data has proven illustrative of the inherent difficulty of simplifying irreducible concepts to facilitate comprehensibility and afford scope to formulate accessible, cogent and conclusive normative terms. The points at issue extend beyond the narrow scope of those concerns raised in this research with regard to the collection and processing of location data. The restricted scope of this enquiry, with its designated focus being that of location data, ought not obscure the fact that other types of metadata intrinsically represent similar challenges for the further development of a coherent framework of protections and safeguards for citizens in an era of irrepressible technological innovation. This study has sought to illuminate and evaluate the pressing questions that arise from the evolution of practices involving the collection and processing of

⁷²⁰ *Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*

⁷²¹ It was noted in the judgment that: “The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter (see, in particular, Case C-274/99 P *Connolly v Commission* EU:C:2001:127, paragraph 37, and *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 68).” *Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014. para. 68

location data. In doing so, this study has illustrated the inadequacy of the present formulation of the term 'location data' itself. Moreover, in its analysis this review has further highlighted a more widespread tendency toward irresolution in respect of sustaining the application of a clear, workable normative framework to address the challenges presented by the paradigmatic shift that ubiquitous computing now represents.

Indisputably, for the purposes of comprehensibility and transparency, and in order to assure the necessity of foreseeability, there exists a certain need for the adoption of clearly defined terms within the regulatory framework so as to facilitate a lucid conceptualisation of broader normative precepts. While accepting this premise as reasonably founded, it is discernible however that in certain instances the effort to formulate a viable, defensible definition has fallen short. This is most evidently the case in respect of the designation 'location data'. As has been illustrated from the outset, the term does not accurately reflect the constitution of the metadata in question. In the opening section of this review the extent to which resources had been employed in researching the implications of more extensive and complex uses of location data in computer science was identified; moreover, one also noted the degree to which this level of engagement clearly reflected a far greater recognition amongst technologists that issues pertaining to location data in respect of privacy and data protection rights were already beginning to foster concern. Interestingly, in computer science, where the understanding that location data concomitantly comprises a composite of both temporal and spatial data is a given, research has continued apace into developing potential solutions to mitigate the interferences constituted by both incumbent and emerging data collection and processing activities.

In the legal sphere, however, the level of agitation and concern has been relatively less pronounced. True, a certain apprehension has finally been raised regarding the anxieties experienced by citizens in the light of revelations of pervasive sensing and monitoring of location, and how these capabilities are increasingly able to detect and scrutinize ever more sensitive aspects of personal activities and interactions. However, as has been outlined in the analysis conducted herein with respect to the rollout of IoT and the creation of a pervasive computing network by which knowledge of our whereabouts risks becoming entirely normalized, considering the potential

gravity of the changes afoot, and the possible impact on our society and democratic norms, the relatively little introspection evidenced and the corresponding indifference apparent on the part of civic society is worrying. The application of biometrics based on ever more granular measurements coupling an individual's movement to unique traits of their physiology represents perhaps an even greater risk. The analysis conducted heretofore in this review has highlighted the challenges movement-enabled biometrics present. This research study has highlighted just how abstruse and opaque the potentialities are that these nascent technologies harbour, and has underscored the obvious difficulty many will experience in trying to discern how their use affects them. The challenges presented are not unique to the development of functionality in collecting and processing personal location data; the problem more generally affects other processes and types of metadata too. As such, useful parallels can be drawn and the analysis conducted in this review can provide insight and serve to lay the foundation for examination of similar concerns relating to ICT development in other spheres of daily life.

In the opening chapter of this research study the author clearly articulated the rationale for limiting the scope of the enquiry conducted to the legislation in place at the time of the review, rather than speculate and attempt to hypothesize as to the nature of any provisions that may be agreed upon and made law as part of the EU's efforts to reform the legal framework pertaining to data protection. This approach has been rendered all the more apposite when one considers that, despite the adoption of the GDPR and complementary legislation pertaining to the police and criminal justice sector by way of Directive (EU) 2016/680, further revisions to the framework remain under way. This consideration is especially salient insofar as, even when this new legislation comes into force in May 2018, the single appropriate provision pertaining to the elucidation of the composition of the metadata termed as "location data" shall remain the existing definition furnished by the revised e-Privacy Directive 2009, i.e. "location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the *geographic position* of the terminal equipment of a user of a publicly available electronic communications service.⁷²² Dependence on this strikingly deficient definition constitutes a substantial

⁷²² Note: *emphasis added*. e-Privacy Directive 2009/136/EC, Article 2

concern. As this research has highlighted, particularly in respect of the examples of emerging technologies such as IoT and biometrics subject to detailed appraisal in the latter sections of this review, the temporal information inherent to the composition of the metadata in question is of commensurate value as that which pertains to the spatial characteristics the data represents. As has been underscored by the detailed analysis conducted herein, the spatial and temporal elements are intrinsically connected; as such, the two components constituent features of the information the metadata illustrates that are inter-dependent. Furthermore, while the proclivity to overlook the innate value of the temporal facet to location data has been identified and evaluated in the discussion here, there however appears little inclination on the part of those overseeing fundamental rights at the institutional and regulatory level to address the lacuna and discern its consequential impacts. The seriousness of this failure is rendered the more acute when one considers that data collection and processing of location data is subject to increasingly more powerful analytical capabilities. As discussed earlier in this review, research in the domain of computer science has established the inherent value of inferences that can be discerned from the examination exclusively of the temporal aspect of location data, granting novel insights into both an individual's patterns of behaviour linked to mobility and, at a more detailed level of resolution, elements of the person's physiological form.

The limitations of the existing instruments at the European level vis-à-vis the use of data protection law to regulate surveillance need be apprehended separately from those pertaining to the right to private life. It is important to recognise that the path by which data protection principles developed accounts for the distinct advantages they inhere in terms of their structured approach to detailed regulation of data collection and processing. However, despite the ongoing efforts concerning data protection reform at the EU level, development of a coherent normative framework and substantive legal principles for the regulation of data processing remains compromised; the onward march of innovation continues to test the applicability of

Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications)

2) Article 2 shall be amended as follows:

(a) point (c) shall be replaced by the following:

‘(c) “location data” means any data processed in an elec-tronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;’”

existing precedents established according to legal reasoning that appraised scenarios distinctly different from those we now encounter.

While the EU Commission acknowledges the important technological and economic developments that have taken place since the last revision of the ePrivacy Directive in 2009 and the procedure for the repeal of the e-Privacy Directive 2002/58/EC has commenced, the process is only in its early stages.⁷²³ Interestingly, the text of the proposal document that concerns the repealing of Directive 2002/58/EC underscores that, in respect of assuring consistency with existing policy provisions in the policy area, the “proposal is *lex specialis* to the GDPR and will particularize and complement it as regards electronic communications data that qualify as personal data.”⁷²⁴ In relation to its status as the *lex specialis* to the GPDR, the proposal’s preamble is particularly germane for its commentary on the broader significance of metadata vis-à-vis its potentially sensitive nature, noting in Recital (2):

“Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc.”⁷²⁵

⁷²³ See: EU Commission, Procedure 2017/0003/COD: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Available at: http://eur-lex.europa.eu/procedure/EN/2017_3

⁷²⁴ EU Commission, Procedure 2017/0003/COD: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Available at: http://eur-lex.europa.eu/procedure/EN/2017_3, p.2

⁷²⁵ EU Commission, Procedure 2017/0003/COD: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Available at: http://eur-lex.europa.eu/procedure/EN/2017_3, p.12. Indeed, in its discussion of the proposal for a regulation on high level of privacy rules for all electronic communications the EU Commission notes that a key point for consideration is that “metadata have a high privacy component”. See: EU Commission, Proposal for an ePrivacy Regulation, 19 January 2017, Available at: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>

Moreover, in Recital (14) the proposal also articulates the necessity of defining electronic communications data in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged:

“...including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation.”⁷²⁶

Taken in conjunction, the two above-cited proclamations are significant for the recognition they afford as to the importance of adopting a suitably objective and forward-thinking perspective to comprehending the intricacies associated with metadata and its potential exploitation. Reflecting on the content of these recitals, therefore, it is quite apparent that the language employed represents quite a divergent contrast from similar provisions within the GDPR. Notwithstanding the *lex specialis* nature of the proposal as a replacement to the e-Privacy Directive, the disparity between the degrees of specificity exhibited in the two instruments is marked.

In contrast to the above-mentioned excerpts of the proposal, the corresponding references in the GDPR are overly vague and indeterminate. In the context of Recital (71), which broadly concerns the processing of personal data in relation to profiling and analogous decision making procedures, the GDPR refers simply to “location or movements” in respect of analysis or prediction of aspects concerning the data subject.⁷²⁷ Again, later in the text of the instrument Recital (75) highlights the risk to

⁷²⁶ EU Commission, Procedure 2017/0003/COD: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Available at: http://eur-lex.europa.eu/procedure/EN/2017_3, p.14

⁷²⁷ General Data Protection Regulation (EU) 2016/679, Recital 71:
“[]...Such processing includes ‘profiling’ that consists of any form of automated processing of

rights and freedoms of persons by analysing or predicting aspects of their “location or movements”⁷²⁸.

References in the GDPR to “location or *movements*” clearly reflect an appreciation that the concept of *movement* i.e. locomotion, had not previously been given sufficient recognition in prior legal instruments, considering its importance. From a normative standpoint, it has proven critical to begin the process of revising the notion that, in the context of personal data processing, location is to be perceived as representing a static, single instance of position: such a conceptual approach is redundant. Further elucidation of the scope of these broadly conceived allusions pertaining to the processing of location data that relates to a data subject is noticeably absent. Whilst the definition for ‘personal data’ furnished within Article 4 of the GDPR references “location data”, no additional clarification is given as to the normative interpretation of the idiom itself. Similarly, no further explication of the rather oblique expression that is “location or movements” is provided. Absent any explicit elucidation, lacunae persist vis-à-vis the lucidity and coherency of the provisions articulated within the legal framework being developed.

As has been demonstrated comprehensibly in this review, the capacity for location data to act as an effective proxy for health data is manifest. Of interest, then, is the greater recognition given personal data concerning the health of the data subject.⁷²⁹ The commentary Recital (35) provides thus broaches the complex issue of classifying personal data. It might well reasonably be asked whether the enactment of new legislative measures such as the GDPR is proving an effective response to the need to

personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.”

⁷²⁸ General Data Protection Regulation (EU) 2016/679, Recital 75:

“[] ... where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.”

⁷²⁹ Refer to General Data Protection Regulation (EU) 2016/679, Recital (35), which states, *inter alia*, that: “Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject... information derived from the testing or examination of a body part... the physiological or biomedical state of the data subject independent of its source...”.

adequately resolve the effective categorisation of metadata; achieving this objective is a prerequisite condition to affording the data subject, data controllers and all other parties concerned the necessary intelligibility and foreseeability integral to an efficacious legal framework.

Indeed, the relevant provisions within the regulation pertaining to defining terms underscore the inherent complexity of classification; Article 4 of the GDPR furnishes descriptions⁷³⁰ with respect to both “biometric data” and “data concerning health” that could well be applied to specific instances pertaining to the collection and processing of location data, as has been outlined heretofore in this study. As such, further reflection regarding the broader issue of categorizing metadata, and location data in particular, again raises the additional and equally significant issue as to the distinction drawn between personal data as a whole, and special categories of data. We may recall that this study has also outlined the extent to which processes involving the collection and processing of location data may increasingly induce the generation of information relating to the data subject that may engage protective safeguards within the legal framework pertaining to sensitive data. Applying the relevant provisions of Recital (51) of the GDPR pertaining to the necessary safeguard of the fundamental rights and freedoms of the data subject in relation to the risks posed by sensitive data highlights the persistence of a key predicament that remains despite the new regulation; rendering perspicuous normative distinctions between metadata, notionally based upon functional differentiation distinguishing the type of information they confer, remains inherently problematic.⁷³¹

Moreover, it should be noted that this review has also called attention to the extent to

⁷³⁰ General Data Protection Regulation (EU) 2016/679, Article 4, (14) & (15)

Article 4:

(14) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physio- logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;”.

⁷³¹ Refer to General Data Protection Regulation (EU) 2016/679, Recital (51):

“Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms...”.

which location data may increasingly act as a surrogate for special categories of personal data that are particularly sensitive in relation to fundamental rights and freedoms. Article 9 of the GDPR is therefore especially germane in this context as the processing of location data may, depending upon the circumstances and the nature of the processes and analysis to which the personal data is subjected, engage multiple clauses of the conditions outlined.⁷³² This observation is especially pertinent where we consider the challenges anticipated in respect of the processing of location data in relation to both health and biometrics. Absent the requisite precision needed to articulate the specification of location data, efforts to subsequently examine and frame the relevance of its use in developing biometric and health indicators using personal data will become mired in inexactitudes. This predicament could have been avoided had greater forethought been given the pitfalls of applying an intrinsically circular approach to applying a normative framework prone to inconsistent interpretation when facing the inexorable advance of technological capabilities.

An occasion for the legal framework to elaborate a more cogent and practicable codification of location data has thus been passed up; as such, the lapse connotes a missed opportunity in terms of providing citizens more robust safeguards in respect of their privacy and data protection rights. A simple illustration of this point may be demonstrated in our considering the processing of location data collected by biometric sensors that monitor human gait. This example is especially apt as it can serve to exemplify precisely why temporal-spatial information is so intrinsically valuable, and why its manipulation potentially represents such a risk to the safeguard of citizens' enjoyment of their fundamental rights.

A data subject's physical comportment, her or his gait, subject to the measurement and computation of the spatial—temporal points it delineates, inheres the capacity to confer information revealing, *inter alia*, religious beliefs, biometric data and data concerning health. It is not beyond the bounds of feasibility that it may also furnish,

⁷³² See the specific clauses pertaining to special categories of sensitive data in General Data Protection Regulation (EU) 2016/679, Article 9(1):

“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health...”

depending upon the circumstances, data relating to a natural person's sex life or sexual orientation or, indeed, political opinion (think, for example, of a posture adopted during prayer at a specific location). Crucially, the importance of the temporal attributes of 'location data' are critical to our frame of reference; data that relates to timing allows the data processor to draw inferences in connection to events at a particular place, or in relation to a position or posture. Furthermore, the development of ever more sophisticated algorithms, coupled with machine learning advances and artificial intelligence, suggest that ever more nuanced inferences are likely to be drawn based upon the collection and processing of location data in conjunction with other forms of personal data. The author's view is that in having exposed these inauspicious deficiencies in the legal framework we need consider appropriate ways to move forward, so as to develop the required competences to best mitigate the resultant effects as expeditiously as possible.

Recommendations

Looking forward, it is clear that scope exists to develop responses in the light of the findings of the research conducted in this study. The extent of the challenges detected to more effectively secure citizens' right to privacy and data protection is certainly quite broad, whilst on the conceptual level the tackling of the more esoteric, abstract dimensions relating to the fundamental paradigmatic shifts we see with respect to locational privacy appear somewhat daunting. However, on a practical level the author believes that the findings of this study provide an opportunity to outline three basic recommendations that constitute a realistic starting point from which to develop a pragmatic response to improve the current situation.

Accordingly, the author suggests that in the short term future efforts may prove most efficacious where they focus upon addressing issues relating to three principal dimensions of the prevailing discourse: firstly, developing a more cogent and comprehensible framework towards a risk-based approach to data protection and privacy; second, the allocation of resources to conduct practical reviews that engage stakeholders to examine and evaluate how technologies are currently being utilised in respect of monitoring human mobility; and, finally, investing resources to develop a more expansive, comprehensive understanding, both in quantitative and qualitative

terms, of the scope of the challenges location data collection and processing represents for our society.

The first recommendation concerns the need in the longer term to establish a more consistent, coherent and transparent approach toward the role of a risk-based approach in the data protection legal framework at the European regional level. This objective represents a more over-arching goal with regards to developing a cogent normative framework in respect of protecting the rights of data subjects' sensitive personal data, including location data in the relevant instances. Whilst the inclusion of the risk-based approach has been supported by an analysis and interpretative guidance published by WP29,⁷³³ the pace of technical innovation is such that more up-to-date scrutiny and counsel is required. The risk-based approach is not a new concept, having been assimilated into and embodied in the approach of the current Directive 95/46/EC. Indeed, a primary example is that of the legal regime applicable to the processing of special categories of data (elucidated in Article 8 of Directive 95/46/EC), which reflects a mode of applying a risk-based assessment to determine whether more stringent obligations stem from any processing activity which might present risks to the safeguard of the rights of the data subject concerned. Risk assessment also needs to take into account the potential that datasets based in part on location data may contain inherent biases upon which data processing results in questionable inferences that undermine the protection of the data subjects' fundamental rights. Principally, the exigency here of framing and articulating risk in relation to the processing of location data is borne of the necessity to provide a clearer articulation of the application of the legal framework to this particular type of metadata, to explain and provide more nuanced understanding of its utility with resolute, practical direction and instruction.

The second recommendation is pragmatic in the sense that it calls for more research that aims at furnishing empirical insight into the existing state of affairs vis-à-vis technologies featuring location data collection or processing characteristics. This research needs focus on the practical application of location-aware capabilities and

⁷³³ See: WP29, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN WP 218, 30 May 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

deliver experiential insight into their effects. In turn, the findings of this research can help inform the debate regarding possible interference in fundamental rights based upon sound, factual evidence — as opposed to the current status quo, whereby far too often appraisals and criticism is based upon cursory observations that encourage speculative pronouncements. The gravity of the issues at stake, which bear upon the safeguard of rights that concern the innermost aspects of our personal identities, are such that the discourse ought to be informed with credible, accurate insight.

The final recommendation advances that initiatives be encouraged that work towards developing our understanding of the issues and questions posed by the relentless proliferation of sensing capabilities represented by IoT and ubiquitous computing. To date, primarily it has been computer scientists who have carried out the majority of research conducted in this domain. Geographers too have contributed to the body of knowledge examining the impact to society of a greater pervasiveness of monitoring of our patterns of movement. In the legal sphere, much of the research examining locational privacy has remained fastened to exploring established precepts such as the dichotomy of public and private space; in fact, very limited has been the evaluation of the cleavage forming in relation to the dearth of information to enlighten citizens of the impact of location-based monitoring on their fundamental rights: which stands in stark contrast to the mass of research and materials being generated to support the wider rollout of IT that exploits location data. The omnipresence of ‘smart cities’ as a topic of discussion across the media and academia is a very pertinent example of this worrying disconnect. Lawyers, policy makers and legislators need actively engage in bridging the gap in understanding, and promote research efforts that move beyond inherently speculative, sociological approaches to delivering more definitive, evidence-based assessments of the role of location data in real-world concerns. To date, a lack of meaningful research into citizens’ perception of the challenges they face has contributed to the knowledge gap.⁷³⁴ The author therefore recommends that a priority be made of dedicating the necessary resources to developing the means to

⁷³⁴ This lacuna is confirmed in the paucity of statistical data available to lawmakers at the European level, and displayed in the Commission’s 2016 report on public consultation on the e-Privacy Directive, which in actuality appears to suggest there exists little enthusiasm for such an analysis as to citizens’ perception of the safeguard and protection of their data protection and privacy rights. *See*: EU Commission, Full report on the public consultation on the ePrivacy Directive, December 2016, Available at: <https://ec.europa.eu/digital-single-market/news-redirect/37204>

engage with and consult citizens as to their concerns regarding the development of further utilities that process location data. Evidently, execution of this initiative might be rendered more straightforward through the co-opting of the existing framework for the promotion of infrastructure enhancement using location data-related services; this might allow for the development of a more holistic approach to planning that considers the fundamental rights concerns of individuals and communities.

These recommendations represent realizable objectives given their relatively broad scope. They are intended as guidance and as a first step in shaping further plans for research. Their attainment is to a large extent dependent upon both resolve and responsibility, as each asks for a commitment of resources for their being able to be pursued. It is hoped that all the interested parties therefore apply the necessary enterprise and ingenuity to ensure the next phases of research are duly conducted and delivered.

Further research

As has already been detailed by the author in the course of this review, the nature of the field of study in question is such that its purview is subject to constant revision. Indeed, one of the principal complications arises from examining innovation in technologies is the constant, perpetual shift that characterizes computing. IT is driven by the search for new methods and characterised by transformation. Law, on the other hand, is perhaps inevitably always relatively restrained in the extent to which it can prove dynamic and responsive to such developments. By its nature, the fundamental premises upon which the normative framework is structured cannot simply be rescripted each time a novel innovation threatens to upend established precedent. Manifestly, this contradistinction represents the crux of the quandary, and constitutes a logical position from which to consider the broader issues that pertain not just to location data, but also to metadata and data processing as a whole.

Viewed from a wider perspective, the concerns raised need to be placed in context, especially in the light of the progress being made in emergent applications of ambient intelligence (AI) and advancements in data mining. Moreover, it should be noted in addition that machine learning techniques may also be used to measure citizens'

expressed privacy preferences in their everyday use of information technologies to develop capabilities such as semi-automated privacy setting of configurations for individual users, thereby in theory rendering data protection and privacy-related decision making for the data subject an appreciably more manageable task. Undeniably, these spheres of innovation represent huge challenges for society and shall certainly present many predicaments for those charged with regulating their future uses whilst safeguarding the ability of citizens to enjoy the full scope of their fundamental rights. Research in these domains must therefore also include an examination as to what possible risks may arise from their implementation; further evaluation might then in turn shape the appropriate regulatory and legislative responses to ensure that the legal framework that safeguards citizens is preserved and, where appropriate, enhanced with effective protections to meet the challenge posed by nascent threats.

Today, just as a new technology or innovation can afford benefits and represent an opportunity to improve our quality of life and welfare, so too can our collective public response equally ensure that its deployment is managed successfully so as best to ensure the long term sustainable functioning of our society. We need contemplate the aforementioned point of principle particularly in regard of the potential changes afoot with developments in machine learning. Machine learning and AI promise to deliver ever greater insight based upon research into facets of our daily lives such as human mobility and the context of our spatial relationships with our surroundings and other people; these aspects of our behaviour until recently remained occluded and impenetrable due to their inherent complexity. Scientific progress would appear to have reached a major inflection point. We now find ourselves on the cusp of major transformations in the way we use personal data to unravel and explain our innermost, concealed and private traits. It is most important, then, that we continue to question the purpose of this pursuit and, moreover, that we carefully consider how, as a society, we forge the appropriate policy responses to protect ourselves from endangering the very liberties that we purport the furtherance of technology ostensibly enriches.

Considering the sizeable commitment in investment made to date in developing and implementing current ICTs, and indeed given by now our tangible reliance on them in

our everyday lives, we have already tacitly accepted a substantial change in how, on a personal and intimate level, we comprehend and realise our own fundamental rights in respect to personal mobility. This acquiescence in part reflects a certain inevitability of technological change. However, we need nonetheless prepare for further developments and establish how, from the standpoint of shaping future regulatory responses and instituting legislative reform, we are to adopt a more proactive approach that accepts the inevitability of rights being subject to an evolutionary, perpetual process of reformulation in the light of this process.

Therefore, in accepting that innovation in ICTs continues unabated we must as such acknowledge that a response to the challenges highlighted is imperative. Moreover, further engagement necessitates deploying greater resources to assess how most effectively to respond to the concerns that have been raised. In particular, there exists a pressing need to augment efforts to examine the potential impacts of developments in monitoring human mobility and understand the implications of the application of these technologies. To date, as has been highlighted, the vast majority of scholarship conducted on locality and its relationship to our environment and, in conjunction, the perception and expression of liberty in relation to movement, has been limited to research conducted primarily by geographers and computer scientists. The analysis of the paradigmatic shift toward pre-emptive, speculative approaches in surveillance now being applied to location tracking, and to the mapping of patterns of mobility, manifests the necessity of adopting a parallel approach in terms of scrutinizing the coherence of the legal framework. Critically, any future alignment of research in the legal sphere toward assessing nascent technologies' impacts on the fundamental rights of citizens must adopt the type of enterprising and forward-thinking approaches as those employed in the domains of IT and scientific innovation; absent recognition of this fundamental premise we risk ever more harmful deficits in our ability to safeguard the vital and innate role that mobility and free movement exercise in the expression of human dignity.

Appendix I: References

A) Books

- Altman, I., 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, California : Brooks/Cole Publishing Company.
- Amoore, L. & De Goede, M. eds., 2008. *Risk and the War on Terror*. Routledge.
- Arendt, H. (1958). *The Human Condition*. Garden City: Doubleday.
- Barabasi, A.L., *Linked: The New Science of Networks*, Perseus Group, 2002, and Carrington, P.J., Scott, J. Wasserman, *Models and Methods in Social Network Analysis*, Cambridge University Press, New York, 2005
- Bauman Z. & Lyon D., *Liquid surveillance: A conversation*. John Wiley & Sons, 2013.
- Bennett, C.J., 1992. *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.
- Bentham J., Letter V, in *The Panopticon Writings* p.43 (Verso 1995) (1787).
- Bernasco, W., *Putting Crime in its Place: Units of Analysis in Geographic Criminology*, Dordrecht: Springer, 2008.
- Borgmann, A., 1999. *Holding on to Reality: The Nature of Information at the Turn of the Millennium*. University of Chicago Press
- Borgman C. L., (2015). *Big Data, Little Data, No Data*. MIT Press
- Bowker, G. and Leigh-Star, S. (1999) *Sorting Things Out*, Cambridge, MA: MIT Press
- Brin, David. *The transparent society: Will technology force us to choose between privacy and freedom?*. Basic Books, 1999.
- Bygrave, L.A., 2002. *Data protection law: approaching its rationale, logic and limits*. Kluwer Law Intl.
- Bygrave, L.A.: *Data Privacy Law*. Oxford University Press, Oxford (2014)
- Butts, C.T., *Social network analysis: A methodological introduction*, *Asian Journal of Social Psychology* (2008)

- Cresswell, T., 2006. *On the move: Mobility in the modern western world*. Taylor & Francis.
- Curry, M., 2008. *Digital places: Living with geographic information technologies*. Routledge.
- Custers, B., 2004. *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Nijmegen: Wolf Legal Publishers.
- DeCew, Judith Wagner. *In pursuit of privacy: Law, ethics, and the rise of technology*. Cornell University Press, 1997.
- Dodge, M., & Kitchin, R. (2011). *Code/space: software and everyday life*. Massachusetts: MIT Press.
- Douglas M., 'Risk and Justice' in *Risk and Blame: Essays in Cultural Theory*, Routledge, 1992
- Frits W. Hondius, *Emerging Data Protection in Europe*, (1975), Amsterdam; North-Holland Publishing Company.
- Flaherty, D.H., 1979. *Privacy and government data banks: An international perspective*. London : Mansell.
- Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Trans. Alan Sheridan. New York: Pantheon, 1977,
- Fung, Archon, Mary Graham, & David Weil. *Full Disclosure: The Perils and Promise of Transparency*. New York: Cambridge University Press, 2007
- N. Katherine Hayles, *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature and Mathematics*, Chicago: University of Chicago Press, 1998
- Foucault, M., *Discipline and Punish: The Birth of the Prison*, Vintage Books, (1979)
- Gandy, O.H., 2016. *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Routledge.
- Gentner, D. (Ed.). (2001). *Spatial Metaphors in Temporal Reasoning*. Cambridge: MIT Press.
- Gibbs, R. W., jr. (1994). *The poetics of mind: Figurative thought, language, and understanding*. Cambridge: Cambridge University Press.
- Goffman, E., *The Presentation of Self in Everyday Life*, New York: Doubleday, 1959
- Grosz E., *Architecture from the Outside: Essays on Virtual and Real Space* (Cambridge, MA: MIT Press, 2001)

- Hayden, Dolores (1995) *The Power of Place: Urban Landscapes as Public History*. MIT Press.
- Heidegger, Martin. "The question concerning technology, and other essays." (1977), New York: Harper & Row.
- Hildebrandt, M., 2015. *Smart technologies and the end (s) of law: Novel entanglements of law and technology*. Edward Elgar Publishing.
- Hillier, B. *Space is the Machine: a Configurational Theory of Architecture*. Cambridge University Press (1996).
- Hillier, B. & Hanson, J. *The Social Logic of Space*. Cambridge University Press (1989).
- Hobbes, T., *Leviathan or, The Matter, Form, and Power of a Commonwealth Ecclesiastical and Civil*. London: Andrew Crooke, (1651).
- Holland D., Lachicotte W., Skinner D., & Cain C., 2001. *Identity And Agency In Cultural Worlds*, Harvard University Press, Cambridge, MA.
- Jasanoff, Sheila. 2016. *The Ethics of Invention: Technology and the Human Future*. New York: W.W. Norton & Company.
- Jenkins, R., *Social Identity*, 2nd Ed. (New York: Routledge, 2004).
- Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011
- Kant, I., 2004. *Kant: Metaphysical Foundations of Natural Science*. Cambridge University Press (first published 1786)
- Karimi K., *The Role Of Sensor Fusion And Remote Emotive Computing (Rec) In The Internet Of Things 6–7* (2013)
- Rob Kitchin. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences*. Sage: London.
- Lakoff, G. and Johnson, M., 2008. *Metaphors we live by*. University of Chicago Press
- Lessig, L., *Code: Version 2.0*. New York: Basic Books, 2006
- Lewis, D. K., (1986). *On the Plurality of Worlds*. Blackwell Publishers.
- Locke, J. (1690). *An Essay Concerning Human Understanding*. London: T. Basset.
- Locke, J. (1772). *Two Treatises of Government*. New York: Kessinger Publishing, LLC.

Lukacs G., *History and Class Consciousness: Studies in Marxist Dialectics*, trans. R. Livingstone (Cambridge, 1971)

Lyon, D., *Surveillance, Power, and Everyday Life*, Oxford University Press, New York, 2007

Macklem T., *Independence of Mind* (2006), Oxford University Press.

Mayer-Schönberger V. & Cukier K., “Big data: A revolution that will transform how we live, work, and think.” *Houghton Mifflin Harcourt* (2013).

McAdam, D., Stearns L. & Uglow D., *The politics of privacy: Planning for personal data systems as powerful technologies*. (New York: Elsevier, 1980)

McCue, C., *Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis*, (Oxford: Elsevier), 2007

Miller, Arthur R., *The Assault on Privacy: Computers, Data Banks and Dossiers*. Ann Arbor 1971

Minton, A., 2006. *The privatisation of public space*. London: Royal Institute of Chartered Surveyors.

Nardi B A and O’Day V L 1999 *Information ecologies. Using technology with heart*. MIT Press, Cambridge, MA

Negroponte, Nicholas. *Being Digital*. New York: Alfred A. Knopf, 1995

Newman, M., (2010) *Networks: An Introduction*. Oxford University Press; Easley D, Kleinberg J (2010) *Networks, crowds, and markets: Reasoning about a highly connected world*. Cambridge University Press

Nilsson, N.J., 2009. *The quest for artificial intelligence*. Cambridge University Press.

O’Riordan, T. and Cameron, J. (eds.), 1994. *The history and contemporary significance of the precautionary principle. Interpreting the precautionary principle*, Cameron May Ltd.

Pentland, A. and Heibeck, T., 2010. *Honest signals: how they shape our world*. MIT press

Rose, N. (1999a) *Governing the soul: The shaping of the private self*, London: Free Association Books.

Schneier B., *Data and Goliath : the Hidden Battles to Collect Your Data and Control Your World*. New York, NY :W.W. Norton & Company, 2015

Schoeman F., *Philosophical Dimensions of Privacy*. Cambridge, UK: Cambridge University Press, 1984.

- Schoeman F., *Privacy And Social Freedom*, Cambridge University Press (1992)
- Sennett, R., 1996. *Flesh and stone: The body and the city in Western civilization*. WW Norton & Company.
- Shoshana Amielle Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity*, Durham, NC: Duke University Press, 2011, 224 pp.
- Sieghart P. (1976) 'Privacy and Computers' London:Latimer, 1976
- Song, H., Srinivasan, R., Jeschke, S. and Sookoor, T., 2017. *Smart Cities: Foundations, Principles and Applications*. John Wiley & Sons.
- Sunstein, C. R., & Thaler, R. H. (2009). *Nudge: improving decisions about health, wealth, and happiness*. London: Penguin.
- Townsend, A. (2013). *Smart cities: Big data, civic hackers, and the quest for a new utopia*. New York: W.W. Norton & Co.
- Ullman, Ellen. *Close to the Machine: Technophilia and its Discontents*. Macmillan, 2012.
- Van der Ploeg, I., *The Machine-readable Body: Essays of Biometrics and the Informatization of the Body*. Maastricht, Shaker Publishing, (2005)
- Webster F., *Theories of the Information Society*, 1995, Routledge New York, NY.
- Weisburd, D., Bernasco, W. and Bruinsma, G. eds., 2008. *Putting crime in its place*. Springer New York.
- Westin, A.F., *Privacy and Freedom*, 6th ed., New York 1970
- White, J.B., 1985. *The legal imagination*. University of Chicago Press.

B) Chapters in Books

- Acquisti, A., Gritzalis, S., Lambrinoudakis, C. and di Vimercati, S. eds., 2007. *Digital privacy: theory, technologies, and practices*. CRC Press.
- Bennett, C. J. 2001. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" pp. 99-125, in *Technology and Privacy: The New Landscape*, edited by P. E. Agre and G. Bramhall. Cambridge, Massachusetts: MIT.
- Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In J. Lane, V. Stodder, S. Bender & H. Nissenbaum (Eds.), *Privacy, Big Data and the Public Good* (pp. 44-75) New York: Cambridge University Press.

Bigo, D., 2006. 'Security, exception, ban and surveillance', in D Lyon (ed), *Theorizing surveillance: The panopticon and beyond*, pp.46-68.

Castelluccia, C., *Behavioural Tracking on the Internet: A Technical Perspective*, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Springer, 2012

Cohen, Julie E., *Between Truth and Power* (October 28, 2013). Mireille Hildebrandt & Bibi van den Berg, eds., *Freedom and Property of Information: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2014, Forthcoming. Available at: <https://ssrn.com/abstract=2346459>

Danezis G. & Clayton R., *Introducing Traffic Analysis*, in Acquisti, A., Gritzalis, S., Lambrinouidakis, C. and di Vimercati, S. eds., 2007. *Digital privacy: theory, technologies, and practices*. CRC Press.

Duckham, M. and Kulik, L., *Location privacy and location-aware computing*. In Drummond, J., Billen, R., and Joao, E., Eds., *Dynamic and Mobile GIS: Investigating Change in Space and Time*, Taylor & Francis, Boca Raton, FL, 2007.

Elias, P., 2014. A European Perspective. *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, pp.171-187

Elmes G.A., Roedl G. and Conley J. 'Concepts, principles and definitions' in Elmes G.A., Roedl G. and Conley J. (eds.) *Forensic GIS - The Role of Geospatial Technologies for Investigating Crime and Providing Evidence* (2014), Springer Publishing, London.

Foucault, M. 1981. 'Omnes et singulatim: towards a criticism of "political reason"', pp. 223–54 in S.M. McMurrin (ed.), *The Tanner Lectures on Human Values*. Salt Lake City, UT: University of Utah Press.

Foucault, M. (1991). *The Foucault effect: studies in governmentality* (Eds. G. Burchell, C. Gordon & P.Miller). Chicago: University of Chicago Press.

Foucault, M. (2007). *Security, territory, population: lectures at the collège de France 1977–1978* (Ed. M.Senellart). New York: Picador.

Goerge, R.M., 2014. 7 Data for the Public Good: Challenges and Barriers in the Context of Cities. *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, pp.153-171

Giannotti, F. & Pedreschi, D., *Mobility, Data Mining and Privacy: A Vision of Convergence*, in *Mobility, Data Mining and Privacy* (2008) F. Giannotti and D. Pedreschi (eds.), pp. 1-11, Available at: <http://www.mendeley.com/research/privacy-in-data-mining>

Greenfield, A. (2017). *A Sociology of the Smartphone*, in 'Radical Technologies: The Design of Everyday Life'. Verso Books. Available at: <https://longreads.com/2017/06/13/a-sociology-of-the-smartphone/>

Herrera M. R., Barreda D. S., 'The SDIK Police Model: How to Make the Invisible Visible' in Elmes G.A., Roedl G. and Conley J. (eds.) *Forensic GIS - The Role of Geospatial Technologies for Investigating Crime and Providing Evidence* (2014), Springer Publishing, London

Kluitenberg, E., *The Network of Waves: Living and Acting in a Hybrid Space*, in *Open 11: Hybrid Space. How wireless media are mobilizing public space*, NAI Publishers, (2006); pp. 6-16, Available at: <http://www.skor.nl/eng/publications/item/open-11-hybrid-space-how-wireless-media-are-mobilizing-public-space?single=1>

Koonin, S.E. and Holland, M., 2014. The value of big data for urban science. In J. Lane, V. Stodder, S. Bender & H. Nissenbaum (Eds.), *Privacy, Big Data and the Public Good* (pp. 137-158) New York: Cambridge University Press

Lupton, Deborah, *You Are Your Data: Self-Tracking Practices and Concepts of Data* (December 4, 2014). *Lifelogging: Theoretical Approaches and Case Studies about Self-tracking*, edited by Stefan Selke, Springer, Forthcoming. Available at: <http://ssrn.com/abstract=2534211>

Millar, J., *Core privacy - A Problem for Predictive Data Mining* (March, 2009), *Lessons From The Identity Trail: Anonymity, Privacy And Identity, in A Networked Society*, New York: Oxford University Press, 2009; pp.103-119, Available at: idtrail.org/content/view/799

Rachels, J., *Why Privacy Is Important*, in *Philosophical Dimensions of Privacy: An Anthology*, Ferdinand D. Schoeman, ed., Cambridge: Cambridge University Press, (1984)

Rosenberg, Richard. *The Social Impact of Computing*, Ch. 9: *Privacy and Freedom of Information*, Academic Press, Boston, MA., 1992

Rouvroy, A.; Poullet, Y. (2009), "The Right to Informational Self-Determination and the Value of Self- Development: Reassessing the Importance of Privacy for Democracy," in: *Reinventing Data Protection*, S. Gutwirth et al. (eds.).

Strandburg, K., "Surveillance of Emergent Associations: Freedom of Association in a Network Society," in *Digital Privacy: Theory, Technologies, and Practices* (Alessandro

Strandburg, K.J., 2014. Monitoring, datafication, and consent: Legal approaches to privacy in the Big Data Context." *Privacy, big data and the public good* (eds Lane J, Stodden V, Bender S, Nissenbaum H), pp.5-43.

Turkle S., "Always-on/Always-on-you: The Tethered Self." In *Handbook of Mobile Communication Studies*, James E. Katz (ed.). Cambridge, MA: MIT Press, 2008. pp.121-139

Uteck, A., *Ubiquitous Computing And Spatial Privacy* (March, 2009), p.89, *Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society*, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/799

Waelbroeck P. An Economist's Thoughts on the Future of Privacy, in *The Futures of Privacy* (Editor -Carine Dartiguepeyrou), Fondation Télécom, Institut Mines-Télécom, February 2014

S Watt, M Lea, & R Spears, "How Social is Internet Communication? A Reappraisal of Bandwidth and Anonymity effects" in S Woolgar (ed.) *Virtual Society?: Technology, Cyberbole, Reality* (2002)

C) Articles in Journals

Acquisti, A. and Grossklags, J., 2007. What can behavioral economics teach us about privacy? *Digital Privacy: Theory, Technologies and Practices*, 18, pp.363-37

Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. *IEEE Security & Privacy* (January/February 2005) 24–30

Aharony, N., Wei Pan, C., Inas Khayal, I., and Pentland, A., Social fMRI, Investigating and Shaping Social Mechanisms in the Real World, *Pervasive and Mobile Computing*, Vol. 7, 2011, pp. 643-659

Alarie, Benjamin and Niblett, Anthony and Yoon, Albert, Regulation by Machine (December 1, 2016). Available at: <https://ssrn.com/abstract=2878950> or <http://dx.doi.org/10.2139/ssrn.2878950>

Althoff T., Sosič R., Hicks J.L., King A.C., Delp S.L., Leskovec J., Large-scale physical activity data reveal worldwide activity inequality. *Nature*, 2017; DOI: 10.1038/nature23018

Ambrose, M.L. & Ausloos, J., The Right to Be Forgotten Across the Pond (September 21, 2012). 2012 TRPC, *Journal of Information Policy*, Volume 3 (2013), pp. 1-23. Available at: <https://ssrn.com/abstract=2032325> or <http://dx.doi.org/10.2139/ssrn.2032325>

Andersen, C.U. and Pold, S.B., 2012, November. Occupation of the 'open city'. In *Proceedings of the 4th Media Architecture Biennale Conference: Participation* (pp. 1-4). ACM.

Ardagna, C.A., Cremonini, M., Damiani, E., di Vimercati, S.D.C. and Samarati, P., 2007. Privacy-enhanced location services information. *Digital Privacy: Theory, Technologies and Practices*, pp.307-326

Bakhshandeh, Reza, et al. "Degrees of separation in social networks." Fourth Annual Symposium on Combinatorial Search, May 2011, p.18, Available at: <http://www.aaai.org/ocs/index.php/SOCS/SOCS11/paper/viewFile/4031/4352>

Balkin, Jack M., *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 2 (2008)

Balkin, Jack M. & Levinson, Sanford V., (2006) *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*. Fordham Law Review, Vol. 75, No. 2, 2006; Yale Law School, Public Law Working Paper No. 120. Available at: <http://ssrn.com/abstract=930514>

Baran, P., 1967. The future computer utility. *The Public Interest*, (8), p.75.

Barnett, I. and Onnela, J.P., 2016. Inferring Mobility Measures from GPS Traces with Missing Data. Available at: <https://arxiv.org/abs/1606.06328>

Barnett, I., Khanna, T. and Onnela, J.P., 2016. Social and Spatial Clustering of People at Humanity's Largest Gathering. *PloS one*, 11(6), p.e0156794. Available at: <http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0156794>

Barocas, Solon and Selbst, Andrew D., *Big Data's Disparate Impact* (2016). 104 California Law Review 671 (2016). Available at: <https://ssrn.com/abstract=2477899>

Baruh, L., Secinti, E. and Cemalcilar, Z., 2017. Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, 67(1), pp.26-53.

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., et al. (2012). Smart cities of the future. *European Physical Journal Special Topics*, 214(1), pp.481–518.

Beckwith, R., *Designing for Ubiquity: The Perception of Privacy, Pervasive Computing*, IEEE (Volume: 2, Issue: 2), 11 June 2003, pp.40-46, Available at: <http://ieeexplore.ieee.org>

Bellovin, Steven M. and Blaze, Matt and Landau, Susan and Pell, Stephanie K., *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law* (November 9, 2016). Harvard Journal of Law and Technology, Forthcoming. Available at: <https://ssrn.com/abstract=2791646>

Benhabib, S., 1993. Feminist theory and Hannah Arendt's concept of public space. *History of the Human Sciences*, 6(2), pp.97-114.

Michael Benisch, Patrick Kelley, Norman Sadeh, and Lorrie Cranor. Capturing location-privacy preferences: quantifying accuracy and user- burden tradeoffs. *Personal and Ubiquitous Computing*, pages 1–16. 10.1007/s00779-010-0346-0.

- Benyon, D., Höök, K., & Nigay, L. (2010, April). Spaces of interaction. In *Proceedings of the 2010 ACM-BCS Visions of Computer Science Conference* (p. 2). British Computer Society.
- Bernstein, D.E., Expressive Association After Dale, George Mason University School of Law - Working Paper Series, 2005, Berkeley Electronic Press, Available at: <http://law.bepress.com>
- Berry, D.M., The Computational Turn: Thinking About The Digital Humanities, Culture Machine, Vol 12, 2011, p.12, Available at: www.culturemachine.net
- Bijker, W.E., Hughes, T.P., Pinch, T. and Douglas, D.G., 2012. *The social construction of technological systems: New directions in the sociology and history of technology*. MIT Press.
- Bin S., Yuan L., & Xiaoyi W., Research on Data Mining Models for the Internet of Things, 2010, 2010 International Conference on Image Analysis and Signal Processing, Available at: <https://www.ceid.upatras.gr/webpages/faculty/vasilis/.../InternetOfThings05476146.pdf>, p.3
- Boyd, Danah & Crawford, Kate, Six Provocations for Big Data (September 21, 2011). A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011. Available at: <http://ssrn.com/abstract=1926431> or <http://dx.doi.org/10.2139/ssrn.1926431>
- Boyne, R., 2000. Post-panopticism. *Economy and Society*, 29(2), pp.285-307.
- Byford K., Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment, 24 RUTGERS COMPUTER & TECH. L.J. 1, 50 (1998)
- Buchanan, E., Aycock, J., Dexter, S., Dittrich, D., & Hvizdak, E. (2011). Computer science security research and human subjects: Emerging considerations for research ethics boards. *Journal of Empirical Research on Human Research Ethics*, 6, pp.71–83.
- Burns MN, Begale M, Duffecy J, et al. Harnessing context sensing to develop a mobile intervention for depression. *J Med Internet Res*. 2011; 13(3):e55. Available at: <http://eutils.ncbi.nlm.nih.gov/>
- Bygrave, L.A, 2010. Privacy and data protection in an international perspective, *Scandinavian studies in law*, 56
- Caliskan-Islam, A., Bryson, J.J. and Narayanan, A., 2016. Semantics derived automatically from language corpora necessarily contain human biases. *arXiv preprint arXiv:1608.07187*.

Calo, M. R., The Boundaries of Privacy Harm (July 16, 2010). *Indiana Law Journal*, Vol. 86, No. 3, 2011, Available at: <http://ssrn.com/abstract=1641487>

Calo, M.R., The Drone As Privacy Catalyst, 64 *STAN. L. REV. ONLINE* 29 December 12, 2011, pp. 29-33, Available at: <http://www.stanfordlawreview.org/>

Cappelli, R., Maio, D., Maltoni, D., Wayman, J.L., and Jain, A.K. (2006) 'Performance evaluation of fingerprint verification systems', *IEEE Transactions on Pattern Analysis Machine Intelligence*, Vol. 28, pp.3–18

Caliskan-Islam, A., Bryson, J.J. and Narayanan, A., 2016. Semantics derived automatically from language corpora necessarily contain human biases. *arXiv preprint arXiv:1608.07187*.

Casanovas, Pompeu and de Koker, Louis and Mendelson, Danuta and Watts, David, Regulation of Big Data: Perspectives on Strategy, Policy, Law and Privacy (June 1, 2017). *Health and Technology* (2017) DOI 10.1007/s12553-017-0190-6. Available at: <https://ssrn.com/abstract=2989689>

Anthony J. Casey & Anthony Niblett, The Death of Rules and Standards, (Univ. of Chi. Pub. Law Theory Working Paper Grp., Paper No. 550, 2015) at 10-11.

Cate, Fred H., "Principles of Internet Privacy" (2000). Faculty Publications. Paper 243. Available at: <http://www.repository.law.indiana.edu/facpub/243>

Cate, Fred H., Government Data Mining: The Need for a Legal Framework (June 2008). *Harvard Civil Rights-Civil Liberties Law Review* (CR-CL), Vol. 43, No. 2, 2008. Available at: <https://ssrn.com/abstract=1151435>

Cate, Fred H., The Failure of Fair Information Practice Principles (2006). *Consumer Protection in the Age of the Information Economy*, 2006. Available at: <https://ssrn.com/abstract=1156972>

Chainey S., Thompson L. (2008) *Crime mapping case studies: practice and research*. Wiley, Chichester, UK.

Chaitin, G., 2006. The limits of reason. *Scientific American*, 294(3), pp.74-81

Cheng, X., Fang, L., Hong, X. and Yang, L., 2017. Exploiting mobile big data: Sources, features, and applications. *IEEE Network*, 31(1), pp.72-79

Citron, D. K., Technological Due Process. U of Maryland Legal Studies Research Paper No. 2007-26; *Washington University Law Review*, Vol. 85, pp. 1249-1313, 2007. Available at: <http://ssrn.com/abstract=1012360>

Citron, Danielle Keats and Pasquale, Frank A., Network Accountability for the Domestic Intelligence Apparatus (2011). *Hastings Law Journal*, Vol. 62, p. 1441, 2011; U of Maryland Legal Studies Research Paper No. 2010-48. Available at: <https://ssrn.com/abstract=1680390>

Clarke R., The Regulation of Point of View Surveillance: A Review of Australian Law (August 17, 2012). UNSW Law Research Paper No. 2012-37. Available at: <http://ssrn.com/abstract=2134878>, p.2;

Cohen, J.E. (2016). The Surveillance-Innovation Complex: The Irony of the Participatory Turn. In D. Barney et al. (Eds.), *The Participatory Condition*. Minneapolis: University of Minnesota Press. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466708 (accessed 01 April 2016).

Cohen, Julie E., What Privacy Is For (November 5, 2012). *Harvard Law Review*, Vol. 126, 2013. Available at: <http://ssrn.com/abstract=2175406>

Cohen, J.E., Examined Lives: Informational Privacy and the Subject as Object, 52 *STAN. L. REV.* (2000); pp.1397-1398

Cohen, Julie E. "Irrational privacy." *J. on Telecomm. & High Tech. L.* 10 (2012): 241. Available at: http://www.jthtl.org/content/articles/V10I2/JTHTLv10i2_Cohen.PDF

Cohen, J. E., Privacy, Visibility, Transparency, and Exposure. *University of Chicago Law Review*, Vol. 75, No. 1, 2008; Georgetown Public Law Research Paper No. 1012068, p.186, Available at: <http://ssrn.com/abstract=1012068>

Constantiou, I.D. and Kallinikos, J., 2015. New games, new rules: big data and the changing context of strategy. *Journal of Information Technology*, 30(1), pp.44-57.

Crang, M. and Graham, S. 'Sentient cities: ambient intelligence and the politics of urban space.' *Information, Communication Society*, (2007); 10 (6). pp. 789-817.

Crawford K., *Think Again: Big Data*, Foreign Policy (9th May, 2013), Available at http://www.foreignpolicy.com/articles/2013/05/09/think_again_big_data

Crawford, K. and Schultz, J., 2014. Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review*, Vol. 55, Issue 1, p.93.

Dake K., Myths of Nature: Culture and the Social Construction of Risk, *Journal of Social Issues*, Volume 48, Issue 4, Winter 1992, pp.21-27

De Hert, P. & V. Papakonstantinou (2012), "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, Vol. 28, No. 2, pp. 130-142.

Deleuze, G., 1992. Postscript on the Societies of Control. *October*, 59, pp.3-7.

De Mul, Jos. 2008. "Digitally mediated (dis)embodiment. Plessner's concept of excentric positionality explained for cyborgs." *Information, Communication & Society* 6: pp.247-266.

Dernbach, Stefan; Das, B.; Krishnan, Narayanan C.; Thomas, B.L.; Cook, D.J., "Simple and Complex Activity Recognition through Smart Phones," Intelligent Environments (IE), 2012 8th International Conference

Determann, Lothar, Adequacy of Data Protection in the EU - General Data Protection Regulation as Global Benchmark for Privacy Laws? (January 17, 2017). Available at: <https://ssrn.com/abstract=2902228>

Dodge M., Kitchin R., CASA Working Paper 92, The ethics of forgetting in an age of pervasive computing, 1 March 2005, Available at: <http://www.bartlett.ucl.ac.uk/casa/publications/working-paper-92>

Dowdell E.M., (2005) You are here! Mapping the boundaries of the fourth amendment with GPS technology. *Rutgers Computer Technology Law Journal* 32:109

Martin Dodge and Rob Kitchin, "Code and the Transduction of Space," *Annals of the Association of American Geographers*, Vol. 95, Issue 1 (2005): pp. 162–180, Available at: http://personalpages.manchester.ac.uk/staff/m.dodge/cv_files/code_and_the_transduction_of_space.pdf

Dwork, C., Hardt, M., Pitassi, T., Reingold, O. and Zemel, R., 2012, January. Fairness through awareness. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference* (pp. 214-226). ACM.

C. Dwork & D. Mulligan, Aligning Classification Systems with Social Values through Design, 2012, Available at: <http://privacylaw.berkeleylawblogs.org/2013/05/23/cynthia-dwork-deirdre-k-mulligan-aligning-classification-systems-with-social-values-through-design/>

C. Dwork & A. Roth, The Algorithmic Foundations of Differential Privacy, *Foundations and Trends in Theoretical Computer Science* Vol. 9, Nos. 3-4 (2014), 211-407, Available at: <https://www.cis.upenn.edu/~aaroht/Papers/privacybook.pdf>, p.10

Dworkin, Gerald. "The Younger Committee Report on Privacy." *The Modern Law Review*, vol. 36, no. 4, 1973, pp. 399–406. <http://www.jstor.org/stable/1093890>

Dworkin, R., 1997. In Praise of Theory. *Arizona Stare Law Journal*, Vol. 29, p.353.

Eagle, N. and (Sandy) Pentland, A., Reality Mining: Sensing Complex Social Systems, *Personal and Ubiquitous Computing*, Vol 10, #4, (2006); pp. 255-268

Eagle, N. and (Sandy) Pentland, A., and David, L., Inferring friendship network structure by using mobile phone data, (2009); pp.15274-15278, Available at: <http://www.pnas.org/content/106/36/15274.full.pdf+html>

- Edwards, Lilian and Veale, Michael, Slave to the Algorithm? Why a 'Right to Explanation' is Probably Not the Remedy You are Looking for (May 23, 2017). Available at: <https://ssrn.com/abstract=2972855>
- Evans, A.C., 1981. European data protection law. *The American Journal of Comparative Law*, pp.571-582.
- Fairchild, A.L. and Bayer, R., 2016. In the Name of Population Well-Being: The Case for Public Health Surveillance. *Journal of health politics, policy and law*, 41(1), pp.119-128.
- Feldman, M., Friedler, S.A., Moeller, J., Scheidegger, C. and Venkatasubramanian, S., 2015, August. Certifying and removing disparate impact. In *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 259-268). ACM.
- Felin, T., Devins, C., Kauffman, S. and Koppl, R., 2017. The Law And Big Data. *Cornell Journal of Law and Public Policy*. Available at: <http://eureka.sbs.ox.ac.uk/6367/>
- Fischer-Hübner, S., Pettersson, J.S., Bergmann, M., Hansen, M., Pearson, S. and Mont, M.C., 2007. HCI Designs for Privacy-Enhancing Identity Management. *Digital Privacy: Theory, Technologies, and Practices*, pp.229-252
- Freiwald, S., Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact (April 20, 2011). *Maryland Law Review*, Vol. 70, p. 677, 2011; Univ. of San Francisco Law Research Paper No. 2011-10. Available at: <https://ssrn.com/abstract=1816762>
- Fuller G., "Perfect Match: Biometrics and Body Patterning in a Networked World," *Fibreculture Journal* 1 (2004). http://journal.breculture.org/issue1/issue1_fuller.html.
- Fuster, Gloria González. *The Emergence of Personal data Protection as a Fundamental Right of the EU*. Vol. 16. Springer Science & Business, 2014
- Gabrosek J., Cressie N., (2002) The effect on attribute prediction of location uncertainty in spatial data, *Geographic Anal.* 34(3), pp.262-285
- Galič, M., Timan, T. and Koops, B.J., 2016. Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology*, pp.9-37.
- Gelman, L.A., Privacy, Free Speech, and 'Blurry-Edged' Social Networks (November 1, 2009). *Boston College Law Review*, Vol. 50, No. 5, 2009, p.1329, Available at: <http://ssrn.com/abstract=1520111>
- Gibson, S., Open Source Intelligence An Intelligence Lifeline, *RUSI Journal*, February 2004, Available at: <http://www.rusi.org/downloads/assets/JA00365.pdf>

Glassman, M., (2012). Occupying the Noosystem: The Evolution of Media Platforms and Webs of Community Protest, *Berkeley Planning Journal*, 25(1).
ucb_crp_bpj_11730. Available at: <http://www.escholarship.org/uc/item/5ws9b7f5>

Gleeson M., ICO raises awareness of the privacy implications of the Internet of Things, 1st September 2014, Available at:
<http://www.lexology.com/library/detail.aspx?g=99ea0f7c-5c18-4f2f-b98f-9f650f33fc40>.

Goldman E., Data Mining and Attention Consumption. Eric Goldman, *Privacy And Technologies Of Identity: A Cross-Disciplinary Conversation*, Springer, 2005.
Available at: <http://ssrn.com/abstract=685241>

Goodchild M.F., Anselin L., Appelbaum R.P., Harthorn B.H., (2000) Toward spatially integrated social science *Int. Reg. Sci. Rev.* 23(2): pp.139-159

Gonzalez, M. C., Hidalgo, C. A., & Barabasi, A. L. (2008). Understanding individual human mobility patterns. *Nature*, 453(7196), 779-782.

D. Gray & D. Citron, The Right to Quantitative Privacy, 98 *MINN. L. REV.* 62, 67 (2013), Available at: <http://digitalcommons.law.umaryland.edu/>

Galetta, A. & De Hert, P., 2015. The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-Oriented Remedial System?. *Review of European Administrative Law*, 8(1),

Gandy Jr, Oscar H. "Exploring identity and identification in cyberspace." *Notre Dame JL Ethics & Pub. Pol'y* 14 (2000).

Gellman, R., Fair Information Practices: A Basic History (June 17, 2016). Available at: <https://ssrn.com/abstract=2415020> or <http://dx.doi.org/10.2139/ssrn.2415020>

Glenn T, Monteith S. New measures of mental state and behavior based on data collected from sensors, smartphones, and the Internet. *Curr. Psychiatry Rep.* 2014 doi:10.1007/s11920-014-0523-3.

Guzik, K., Discrimination by Design: Data Mining in the United States's 'War on Terrorism', *Surveillance & Society*, Vol 7, No 1 (2009), Available at:
<http://www.surveillance-and-society.org/ojs/index.php/journal/article/viewArticle/design>

Haggerty, K.D. and Ericson, R.V., 2000. The surveillant assemblage. *The British Journal of Sociology*, 51(4), pp.605-622.

David L. Hall & James Llinas, An Introduction to Multi-sensor Data Fusion, 85 *PROC. IEEE* 6, 6 (1997)

Hallinan, Dara, Michael Friedewald, and Paul McCarthy, "Citizens' Perceptions of Data Protection and Privacy", *Computer Law and Security Review*, Vol. 28, No. 3, 2012

Harcourt, Bernard E., *Against Prediction: Sentencing, Policing, and Punishing in an Actuarial Age* (May 2005). U of Chicago, Public Law Working Paper No. 94. Available at: <http://ssrn.com/abstract=756945>

Harcourt, B. E. (2003). The shaping of chance: Actuarial models and criminal profiling at the turn of the twenty-first century. *The University of Chicago Law Review*, 70

Harcourt, Bernard E., *An Answer to the Question: 'What is Poststructuralism?'* (March 2007). University of Chicago, Public Law Working Paper No. 156. Available at: <http://ssrn.com/abstract=970348>

Hart, H.L.A., 1958. Positivism and the Separation of Law and Morals. *Harvard law review*, pp.593-629.

Hier, S. P. (2002). Probing the surveillant assemblage: on the dialectics of surveillance practices as processes of social control. *Surveillance & Society*, 1(3), 399–411.

Hildebrandt, M., 2011. Who needs stories if you can get the data? ISPs in the era of big number crunching. *Philosophy & Technology*, 24(4), pp.371-390.

Hildebrandt, M., 2008. A vision of ambient law. *Regulating technologies*, pp.175-191.

Hildebrandt, M., 2016. Law as Information in the Era of Data-Driven Agency. *The Modern Law Review*, 79(1), pp.1-30. Available at: <http://www.law.nyu.edu/>
Hildebrandt, Mireille (2013), "Slaves to Big Data. Or Are We?" Available at: http://works.bepress.com/mireille_hildebrandt/52.

Hintze, Mike and LaFever, Gary, Meeting Upcoming GDPR Requirements While Maximizing the Full Value of Data Analytics (January 2017). Available at: <https://ssrn.com/abstract=2927540> or <http://dx.doi.org/10.2139/ssrn.2927540>

Hoel, Erik P. 2017. "When the Map Is Better Than the Territory." *Entropy* 19, no. 5: p.188.

Hoepman, J.H. (2012), Available at: "Privacy design strategies," <http://arxiv.org/pdf/1210.6621.pdf>.

Homes, Oliver Wendell. "The Path of the Law", 10 *Harvard law Review* 457 (1897): 461.

Hull, G., 2015. Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, 17(2), pp.89-101.

Huysmans, J., 2016. Democratic curiosity in times of surveillance. *European Journal of International Security*, 1(01), pp.73-93.

- Jiang, B., and Yao, X. 2006. "Location-Based Services and GIS in Perspective," *Computers, Environment and Urban Systems* (30:6), pp. 712-725
- Jones, R., Pykett, J. and Whitehead, M., 2013. Psychological governance and behaviour change. *Policy & Politics*, 41(2), pp.159-182.
- Jovanov, E., Poon, C., Yang, G.Z. and Zhang, Y.T., 2009. Guest editorial - Body sensor networks: from theory to emerging applications. *IEEE Transactions on Information Technology in Biomedicine*, 13(6), pp.859-863. Available at: http://www.ece.uah.edu/~jovanov/papers/J2009_Jovanov_TITB_BSN_Editorial.pdf
- Kang, Jerry, Information Privacy in Cyberspace Transactions. *Stanford Law Review*, Vol. 50, (1998); pp. 1193-1287, Available at: <http://ssrn.com/abstract=631723>
- Kaptein, M. and Eckles, D., 2010, June. Selecting effective means to any end: Futures and ethics of persuasion profiling. In *International Conference on Persuasive Technology* (pp. 82-93). Springer Berlin Heidelberg.
- Kayacik, H.G., Just, M., Baillie, L., Aspinall, D. and Micallef, N., 2014. Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors, Available at: <https://arxiv.org/abs/1410.7743>
- Keith et al, Information disclosure on mobile devices: Re-examining privacy calculus with actual user behaviour, *International Journal of Human-Computer Studies*, Volume 71 Issue 12, December, 2013, pp. 1163-1173
- Kennedy, L.W., Caplan, J.M. and Piza, E., 2011. Risk clusters, hotspots, and spatial intelligence: risk terrain modeling as an algorithm for police resource allocation strategies. *Journal of Quantitative Criminology*, 27(3), pp.339-362.
- Kerr, Orin S., The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution. *Michigan Law Review*, *Forthcoming*. Available at: <http://ssrn.com/abstract=421560>, p.157
- Kim, M., "The Right to Anonymous Association in Cyberspace: US Legal Protection for Anonymity in Name, in Face, and in Action", (2010), p.52, Available at: <http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/kim.asp>
- Kirchner, T.R. and Shiffman, S., 2016. Spatio-temporal determinants of mental health and well-being: advances in geographically-explicit ecological momentary assessment (GEMA). *Social Psychiatry and Psychiatric Epidemiology*, 51(9), pp.1211-1223.
- Kirstein, P.T., 2016. Edge Networks & Devices for the Internet of Things. *Daedalus*, 145(1), pp.33-42.
- Kitchin, R., 2014. The real-time city? Big data and smart urbanism. *GeoJournal*, 79(1), pp.1-14.

- Klasnja, P., Consolvo, S., Choudhury, T., Beckwith, R. and Hightower, J., 2009. Exploring privacy concerns about personal sensing. *Pervasive Computing*, pp.176-183. Available at: http://aiweb.cs.washington.edu/research/projects/aiweb/media/papers/Klasnja_et_al_2009_-_Exploring_privacy_concerns_about_personal_sensing.pdf
- Bert-Jaap Koops & Ronald Leenes, 'Code' and the Slow Erosion of Privacy, 12 Mich. Telecomm. & Tech. L. Rev. 115 (2005). Available at: <http://repository.law.umich.edu/mttlr/vol12/iss1/3>
- Koops, Bert-Jaap, Some Reflections on Profiling, Power Shifts, and Protection Paradigms (June 2008), p.1, Profiling The European Citizen, Hildebrandt & Gutwirth, eds., Springer, 2008. Available at: <http://ssrn.com/abstract=1350584>
- Koops, B.J., 2014. The trouble with European data protection law. *International Data Privacy Law*, 4(4), pp.250-261.
- Kosinski, M., Wang, Y., Lakkaraju, H. and Leskovec, J., 2016. Mining big data to extract patterns and predict real-life outcomes. *Psychological Methods*, 21(4), pp.493-506
- Kourtit, K., Nijkamp, P., & Arribas-Bel, D. (2012). Smart cities perspective—A comparative European study by means of self-organizing maps. *Innovation*, 25(2), 229–246.
- Kranzberg, M. (1986) 'Technology and History: Kranzberg's Laws', *Technology and Culture* vol. 27, no. 3, pp. 544-560
- Krumm, J., 2009. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6), pp.391-399.
- John Krumm and Eric Horvitz, "Predestination: Inferring Destinations from Partial Trajectories," *UbiComp 2006: Ubiquitous Computing, Proceedings of the 8th International Conference, September 2006*, (Springer Berlin, Heidelberg, 2006), 243–260.
- Kuner, C., An International Legal Framework for Data Protection: Issues and Prospects (January 24, 2009). *Computer Law & Security Review*, Vol. 25, pp. 307-317, 2009. Available at: <https://ssrn.com/abstract=1443802>
- Kuner C., *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law (Privacy and Security Law Report)*, Bloomberg BNA, 6 February 2012.
- Lambiotte, R. and Kosinski, M., 2014. Tracking the digital footprints of personality. *Proceedings of the IEEE*, 102(12), pp.1934-1939.

Lane ND, Miluzzo E, Lu H, Peebles D, Choudhury T, Campbell AT. A survey of mobile phone sensing. *IEEE Commun Mag.* 2010; 48:140–50. (September). doi:10.1109/MCOM.2010.5560598.

Langheinrich, M., 2001. Privacy by design—principles of privacy-aware ubiquitous systems. In *Ubicomp 2001: Ubiquitous Computing* (pp. 273-291). Springer Berlin/Heidelberg.

Lavrinec, J. and Zaporozhets, O., 2013. Shaping spaces of shared experience: creative practices and temporal communities. *Urban Public Space: Facing the Challenges of Mobility and Aestheticization*, pp.135-147.

Layton, Roslyn and Baranes, Edmond, GDPR: Short Run Outputs vs. Long Term Welfare. Mapping the EU's General Data Protection Regulation to Best Practices for Online Privacy (March 31, 2017). Available at: <https://ssrn.com/abstract=2944358>

Lazer D., (Sandy) Pentland, A., Adamic, L., Aral, S., Barabasi A.L, Brewer, D., Christakis, N., Contractor, N., Fowler, J., Gutmann, M., Jebara, T., King, G., Macy, M., Roy, D., Van Alstyne, M., Life in the Network: The Coming Age of Computational Social Science, *Science*, February 2009; pp. 721–723, Available at: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2745217>

Leenes, Ronald E. and Koops, Bert-Jaap, 'Code' and Privacy - Or How Technology is Slowly Eroding Privacy. *ESSAYS ON THE NORMATIVE ROLE OF INFORMATION TECHNOLOGY*, T.M.C. Asser Press, The Hague, Netherlands, 2005. Available at: <https://ssrn.com/abstract=661141>

Lerman, J., “Big data and its exclusions.” *Stanford Law Review Online* 66 (2013)

Lockwood, S., Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, 18 *HARV. J.L. & TECH* (2004); pp. 307-317

Loke, L., & Reinhardt, D. (2012, November). First steps in body-machine choreography. In *Proc. of The 2nd International Body In Design workshop, OZCHI 2012*.

Louail, Thomas, et al. “Uncovering the spatial structure of mobility networks.” *Nature Communications* 6 (2015).

Louail, Thomas, et al. “From mobile phone data to the spatial structure of cities.” *Nature, Scientific reports* 4 (2014)

Lupton, Deborah, Self-Tracking Modes: Reflexive Self-Monitoring and Data Practices (August 19, 2014). Available at: <http://ssrn.com/abstract=2483549> or <http://dx.doi.org/10.2139/ssrn.2483549>

Madhushri, P., Dzhagaryan, A., Jovanov, E. and Milenkovic, A., 2016. An mHealth Tool Suite for Mobility Assessment. *Information*, 7(3), p.47.

Mann, Jonathan. 1997. "Health and Human Rights: If Not Now, When?" *Health and Human Rights* 2, no. 3: 113–20.

Margulis S., "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues*, vol. 59, pp. 243-261, 2003.

Marx, L., in *Technology Review*, "Does Improved Technology Mean Progress?" , January 1987, pp.33-41

Marx L., *Technology The Emergence of a Hazardous Concept*, *Technology and Culture*, Volume 51, Number 3, July 2010, pp. 561-577

Mayer, J., Mutchler, P. and Mitchell, J.C., 2016. Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences*, p.201508081.

Melnick AL, Fleming DW. Modern geographic information systems: promise and pitfalls. *J Public Health Manag Pract* 1999;5(2):viii-x.

Miller, Arthur R., *Computer and Privacy*. In: *Michigan Law Review* 67 (1969), pp. 1162- 1246

Milošević, M., Shrove, M.T. and Jovanov, E., 2011. Applications of smartphones for ubiquitous health monitoring and wellbeing management. *JITA - Journal Of Information Technology And Applications*, 1(1).

Milošević, M., Milenkovic, A. and Jovanov, E., 2013. mHealth@ UAH: computing infrastructure for mobile health and wellness monitoring. *XRDS: Crossroads, The ACM Magazine for Students*, 20(2), pp.43-49.

Mishchenko, L., 2016. The Internet of Things: Where Privacy and Copyright Collide. *Santa Clara Computer & High Tech. LJ*, 33, p.90. Available at: <http://digitalcommons.law.scu.edu/chtlj/vol33/iss1/1>, p.

Mitsilegas, V., 2015. The transformation of privacy in an era of pre-emptive surveillance. *Tilburg Law Review*, 20(1), pp.35-57.

Mnookin, J.L., 2012. Atomism, holism, and the judicial assessment of evidence. *UCLA L. Rev.*, 60, p.1524.

Moerel, L. & Prins, C., *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things* (May 25, 2016). Available at: <https://ssrn.com/abstract=2784123>

Montjoye Y-A. et al, *Unique in the Crowd: The privacy bounds of human mobility*, *Nature.com - Scientific Reports* 3, Article number: 1376, 25 March 2013, Available at: <http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html>

Mountain, D. & Raper, J., 2001. Spatio-temporal representations of individual human movement for personalising Location Based Services. In *Proceedings for GISRUK 2001*. Available at:
<https://pdfs.semanticscholar.org/a16f/8fa27e833df3e49fe594ba0141b7764136dc.pdf>

Mountain, D. & Raper, J., 2001. Modelling human spatio-temporal behaviour: a challenge for Location-Based Services. In *Proceedings of 6th International Conference on Geocomputation*. Available at:
<http://www.geog.leeds.ac.uk/groups/geocomp/2001/papers/mountain.pdf>

Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 Cal. L. Rev. 721. (2007). Available at:
<http://scholarship.law.berkeley.edu/californialawreview/vol95/iss3/2>

G. Myles, A. Friday, and N. Davies, "Pre- serving Privacy in Environments with Location-Based Applications," *IEEE Pervasive Computing*, vol. 1, no. 1, Jan.–Mar. 2003, pp. 56–64.

Nafus D., Sherman J., *This One Does Not Go Up to 11: The Quantified Self Movement as an Alternative Big Data Practice*, *International Journal of Communication* 8 (2014), Available at:
<http://ijoc.org/index.php/ijoc/article/viewFile/2170/1157>, pp. 1784–1785

Nagel, T., 1998. Concealment and exposure. *Philosophy & Public Affairs*, 27(1)

Narayanan, A. and Shmatikov, V., 2009, May. De-anonymizing social networks. In *Security and Privacy, 2009 30th IEEE Symposium on* (pp. 173-187). IEEE.

Neff, G., "Why Big Data Won't Cure Us." *Big Data* 1.3 (2013): pp.117–123. PubMed Central. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4114418/>

Nelson, S. & J.Simek, J.Foltin, *The Legal implications of Social Networking*, 22 *Regent U. L. Rev.* 1 (2009-2010),

Newell, B.C., *The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe* (October 11, 2013). *I/S: A Journal of Law and Policy for the Information Society*: 9 ISJLP, 2014. Available at:
<http://ssrn.com/abstract=2339338>

NIH/National Institute of Biomedical Imaging & Bioengineering, "Smartphone data used in global study of physical activity: Large-scale study reveals targets for obesity prevention, wisdom of walkable communities." *ScienceDaily*. ScienceDaily, 10 July 2017. Available at: www.sciencedaily.com/releases/2017/07/170710113613.htm.

Ni Loideain, N. (2015). EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. *Media and Communication*, 3(2), 53-62.

Nissenbaum, H.F., *Privacy as Contextual Integrity*. *Washington Law Review*, Vol. 79, No. 1, (2004); pp. 119-158, Available at: <http://ssrn.com/abstract=534622>

Noveck, B.S., 2004. The electronic revolution in rulemaking. *Emory Law Journal*, 53, p.433.

Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). *UCLA Law Review*, Vol. 57, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at: <http://ssrn.com/abstract=1450006>

Ohm, P., (2014). Changing the rules: general principles for data use and analysis. In J. Lane, V. Stodder, S. Bender & H. Nissenbaum (Eds.), *Privacy, Big Data and the Public Good* (pp. 96-75) New York: Cambridge University Press., pp.96-122

Onnela, J.P., Arbesman, S., González, M.C., Barabási, A.L. and Christakis, N.A., 2011. Geographic constraints on social network groups. *PLoS one*, 6(4), p.e16939. Available at: <http://journals.plos.org/plosone>

Orcutt M., We Must Not Give Up on Privacy, *MIT Technology Review*, 10, October 2016, Available at: <https://www.technologyreview.com>

Parker, R.B., A Definition of Privacy, 27 *RUTGERS L. REV.* 275, 280 (1974)

Parsell, M., Pernicious virtual communities, *Ethics and Information Technology* (2008) 10:41–56, Springer Available at: <https://www.hci.iastate.edu/REU09/pub/Main/CraftOfResearch/Parsell.pdf>

Pasquale F., Restoring Transparency to Automated Authority, 9 *J. Telecommunications. & High Tech Law.* 235, 235–36 (2011). Available at: <http://digitalcommons.law.umaryland.edu>

Peppet S. R., Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Vol. 93 *Texas Law Rev.* 85, pp. 85-103 Available at: <http://www.texasrev.com/wp-content/uploads/Peppet-93-1.pdf>

Petkova, Bilyana, Towards an Internal Hierarchy of Values in the EU Legal Order: Balancing the Freedom of Speech and Data Privacy (May 26, 2016). *Maastricht Journal of European and Comparative Law*, 23:3 (2016); EUI Department of Law Research Paper No. 2016/02. Available at: <https://ssrn.com/abstract=2784841>

Phillips D. J., From Privacy to Visibility: Context, Identity, and Power in Ubiquitous Computing Environments, 23 *Soc Text* 95, (2005)

Posner, R.A. "Privacy, Surveillance, and Law." 75 *University of Chicago Law Review*, 245 (2008).

Proshansky, H M, Falian, A K and Kaminoff R (1983) Place-Identity: Physical World Socialisation of the Self. *Journal of Environmental Psychology* 3 (3).

Rachlinski, J.J., 2010. Evidence-based law. *Cornell Law Revue*, 96, pp.901-923. Available at: <http://scholarship.law.cornell.edu/clr/vol96/iss4/27>

Regan, P.M. 2011. Response to Bennett: Also in defence of privacy. *Surveillance & Society* 8(4): 497-499. Available at: <http://www.surveillance-and-society.org>

Reidenberg, J.R., 1997. Lex informatica: The formulation of information policy rules through technology. *Tex. L. Rev.*, 76, p.553.

Reiman, J.H., Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future Santa Clara Symposium on Privacy and IVHS , 11 Santa Clara Computer & High Tech. L.J. 27 (1995), Available at: <http://digitalcommons.law.scu.edu/chtlj/vol11/iss1/5>

Richards, N.M., 2013. The dangers of surveillance. *Harvard Law Review*, 126(7), pp.1934-1965.

Roberts, A., 2015. Privacy, data retention and domination: Digital rights Ireland Ltd v Minister for Communications. *The Modern Law Review*, 78(3), pp.535-548.

Roberts, J.A., Profiling Levels of Socially Responsible Consumer Behavior: A Cluster Analytic Approach and Its Implications for Marketing, *Journal of Marketing Theory and Practice*, Vol. 3, No. 4 (Autumn, 1995), pp. 97-117

Roemer, J.E., 2015. Kantian optimization: A microfoundation for cooperation. *Journal of Public Economics*, 127, pp.45-57.

Romein, E., & Schuilenburg, M. (2008). Are you on the fast track? The rise of surveillant assemblages in a post-industrial age. *Architectural Theory Review*, 13(3), 337–348.

Marc Rotenberg & David Jacobs, Updating The Law Of Information Privacy: The New Framework Of The European Union, *Harvard Journal of Law & Public Policy* Vol. 36, 2013, Available at: http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_605_Rotenberg_Jacobs.pdf

Rubinstein, Ira, Lee, Ronald D. and Schwartz, Paul M., Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. *University of Chicago Law Review*, Vol. 75, p. 261, 2008; UC Berkeley Public Law Research Paper No. 1116728. Available at: <http://ssrn.com/abstract=1116728>

D. Runtzen & J. Zenn, Association and Assembly in the Digital Age, *The International Journal of Not-for-Profit Law*, Volume 13, Issue 4, December 2011, Available at: <http://www.icnl.org/research/library/files/Transnational/Assoc%20Assemb%20Digital%20Age.pdf>

Ryan, M.R., The Boundaries of Privacy Harm (July 16, 2010). *Indiana Law Journal*, Vol. 86, No. 3, 2011. Available at: <http://ssrn.com/abstract=1641487>

Saxon, L.A. Ubiquitous wireless ECG recording: a powerful tool physicians should embrace. *J. Cardiovasc. Electrophysiol* 2013; 24

Schulhofer, S. J., "An International Right to Privacy? Be Careful What You Wish For" (2015). New York University Public Law and Legal Theory Working Papers. Paper 508. Available at: http://lsr.nellco.org/nyu_plltwp/508

Schwartz, P.M., Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 Iowa L. Rev., (1994-95) pp. 553-616

Schwartz, P.M., 1999. Internet privacy and the state. *Conn. L. Rev.*, 32, p.815.

Simitis, S., 1987. Reviewing privacy in an information society. *University of Pennsylvania Law Review*, 135(3), pp.707-746.

Slater, M.D., Reinforcing Spirals: The Mutual Influence of Media Selectivity and Media Effects and Their Impact on Individual Behavior and Social Identity, *Communication Theory*, Volume 17, Issue 3, pp. 281–303, August 2007

Sloot, B.V.D., 2015. Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data'. *Utrecht Journal of International and European Law*, 31(80)

Solove, D.J., 2008. Data mining and the security-liberty debate. *The University of Chicago Law Review*, 75(1), pp.343-362.

Solove, D.J. (2013), "Introduction: Privacy Self-Management and the Consent Dilemma," *Harvard Law Review*, 126.

Solove, Daniel J., Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*, Vol. 53, p. 1393, July 2001. Available at: <http://ssrn.com/abstract=248300>

Solove, Daniel J., Reconstructing Electronic Surveillance Law. *George Washington Law Review*, Vol. 72, 2004, p.1708 Available at: <http://ssrn.com/abstract=445180> or <http://dx.doi.org/10.2139/ssrn.445180>

Solove, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review*, Vol. 44, p.745, 2007; *GWU Law School Public Law Research Paper No. 289*. Available at: <http://ssrn.com/abstract=998565>

Solove, Daniel J., *Understanding Privacy*, Harvard University Press, May 2008; *GWU Legal Studies Research Paper No. 420*; *GWU Law School Public Law Research Paper No. 420*. Available at: <https://ssrn.com/abstract=1127888>

Son D. et al, Multifunctional wearable devices for diagnosis and therapy of movement disorders, *Nature Nanotechnology* 9, pp. 397–404 (2014) Available at: <http://www.nature.com/nnano/journal/v9/n5/abs/nnano.2014.38.html>

Srivatsa, M. and Hicks, M., 2012, October. Deanononymizing mobility traces: Using social network as a side-channel. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 628-637). ACM.

Strahilevitz, Lior, Toward a Positive Theory of Privacy Law (March 7, 2013). Harvard Law Review, Vol. 113, No. 1, 2013; University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 637; U of Chicago, Public Law Working Paper No. 421. Available at: <https://ssrn.com/abstract=2230151>

Sui, D.Z. and Goodchild, M.F., 2003. A tetradic analysis of GIS and society using McLuhan's law of the media. *The Canadian Geographer/Le Géographe canadien*, 47(1)

J. Suler, 'The online disinhibition effect', *Journal of Cyberpsychology and Behaviour* 7, no 3, 2004

Sunstein C. R., On the Expressive Function of Law, *University of Pennsylvania Law Review* 144:5 (1996) Available at: <http://scholarship.law.upenn.edu/>

Sunstein, Cass R., Irreversibility (July 12, 2008). Oxford University Press, Law, Probability and Risk, Forthcoming; Harvard Public Law Working Paper No. 08-25; Harvard Law School Program on Risk Regulation Research No. 08-1. Available at: <https://ssrn.com/abstract=1260323>

Sunstein C. R., Beyond The Precautionary Principle, The Chicago Working Paper Series, January 2003, Available at: Index: <http://www.law.uchicago.edu/Lawecon/index.html>

Sunstein C.R., John M. Olin Law & Economics Working Paper No. 165 (2D Series), Public Law And Legal Theory Working Paper No. 33, Hazardous Heuristics, Available at: <http://www.law.uchicago.edu/Lawecon/index.html>

Swan, M., 2013. The quantified self: Fundamental disruption in big data science and biological discovery. *Big Data*, 1(2), pp.85-99.

Swan M. Neural Data Privacy Rights: An Invitation For Progress In The Guise Of An Approaching Worry. The Edge Annual Question 2013. Available online at <http://edge.org/responses/q2013>

Peter Swire & Kenesa Ahmad, 'Going Dark' Versus a 'Golden Age for Surveillance', *Security & Surveillance*, November 28, 2011, Available at: <https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/>

Tam Cho, W.K. and Liu, Y.Y., 2016. Toward a Talismanic Redistricting Tool: A Computational Method for Identifying Extreme Redistricting Plans. *Election Law Journal*, 15(4), pp.351-366. Available at: <http://cho.pol.illinois.edu/wendy/papers/talismanic.pdf>

Tene, Omer and Polonetsky, Jules, Judged by the Tin Man: Individual Rights in the Age of Big Data (August 15, 2013), *Journal of Telecommunications and High Technology Law*, Forthcoming. Available at: <http://ssrn.com/abstract=2311040>

- Tene, O., & Polonetsky, J., Privacy In The Age Of Big Data: A Time For Big Decisions, 64 Stanford Law review ONLINE 63, February 2, 2012
- Tene, O., Privacy: The New Generations (November 17, 2010). International Data Privacy Law, 2010. Available at: <http://ssrn.com/abstract=1710688>
- Tenhaaf, N., 1996, February. Mysteries of the Bioapparatus. In *Immersed in technology* (pp. 51-71). MIT Press.
- Thompson, J.B., 2011. Shifting boundaries of public and private life. *Theory, Culture & Society*, 28(4), pp.49-70.
- Thompson, Marcelo, The Neutralization of Harmony: The Problem of Technological Neutrality, East and West (September 1, 2011). Boston University Journal of Science and Technology Law, Vol. 18, No. 2, 2012; University of Hong Kong Faculty of Law Research Paper No. 2011/012. Available at: <https://ssrn.com/abstract=1936067>
- Thompson, R., Radicalization and the Use of Social Media, Journal of Strategic Security Volume 4 Issue 4, 2011
- Nigel Thrift & Shaun French, The automatic production of space, Transactions - Institute of British Geographers, Volume 27, Issue 3, September 2002, pp. 309–335, Available at: <http://www.dourish.com/classes/readings/ThriftFrench-AutomaticProductionSpace.pdf>
- Tien, L., "Architectural regulation and the evolution of social norms." *Yale Journal of Law & Technology*. 7 (2004): 1.
- Tompson L., Townsley M., (2010) Looking back to the future: using space-time patterns to better predict the location of street crime. *International Journal of Police Science Management* 12(1)
- Tooby, J. and Cosmides, L., 1992. The psychological foundations of culture. *The adapted mind: Evolutionary psychology and the generation of culture*, pp.19-136.
- Torous, J., Staples, P. and Onnela, J.P., 2015. Realizing the potential of mobile mental health: new methods for new data in psychiatry. *Current psychiatry reports*, 17(8), pp.1-7. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4608747/>, p.2
- Townsend A., "Life in the Real-Time City: Mobile Telephones and Urban Metabolism," *J. Urban Technology*, vol. 7, no. 2, 2000, pp. 85–104.
- Tranberg, C.B., 2011. Proportionality and data protection in the case law of the European Court of Justice. *International Data Privacy Law*, 1(4), pp.239-248.
- Tufekci, Z., 2014. Engineering the public: Big data, surveillance and computational politics. *First Monday*, 19 (7).

Varian, H.R., 2014. Beyond big data. *Business Economics*, 49(1), pp.27-31. Available at: <http://www.edshare.soton.ac.uk/15212/7/BeyondBigDataPaperFINAL.pdf>

Vee, A., 2012. Text, speech, machine: Metaphors for computer code in the law. *Computational Culture*, 2, Available at: <http://computationalculture.net/article/text-speech-machine-metaphors-for-computer-code-in-the-law>

Wachter, Sandra and Mittelstadt, Brent and Floridi, Luciano, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (December 28, 2016). *International Data Privacy Law*, Forthcoming. Available at: <https://ssrn.com/abstract=2903469>

Weiser M, Gold R and Brown J S (1999), The origins of ubiquitous computing research at PARC in the late 1980s, *IBM Systems Journal*, 38 pp.83–97

Weiser, M., The computer in the 21st century, *Scientific American*, vol. 265, no. 3, (1991) pp. 78–89, Available at: <http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf>

Werbach K., (2007) Sensors and sensibilities, *Cardozo Law Review* 28, pp.2321-2371

Whitman J.Q., “The Two Western Cultures of Privacy: Dignity versus Liberty”, *The Yale Law School Journal*, 2004

White, J.B., 1985. Law as rhetoric, rhetoric as law: The arts of cultural and communal life. *The University of Chicago Law Review*, 52(3), pp.684-702.

Wisman, T.H.A., "Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things", *European Journal of Law and Technology*, Vol. 4, No. 2, 2013, Available at: <http://ejlt.org/article/view/192/379>

Yampolskiy, R.V. and Govindaraju, V. (2008) ‘Behavioural biometrics: a survey and classification’, *Int. J. Biometrics*, Vol. 1, No. 1, pp.81-113. Available at: <http://cecs.louisville.edu/ry/Behavioral.pdf>

Yeung, K., 2016. Algorithmic regulation and intelligent enforcement. *Regulation scholarship in crisis?*, Available at: <http://www.lse.ac.uk/accounting/>

Yeung, K., 2017. ‘Hypernudge’: Big Data as a mode of regulation by design. *Information, Communication & Society*, 20(1), pp.118-136. Available at: https://www.researchgate.net/profile/Karen_Yeung/publication/303479231_'Hypernudge'_Big_Data_as_a_mode_of_regulation_by_design/

Zang, H. and Bolot, J., 2011, September. Anonymization of location data does not work: A large-scale measurement study. In *Proceedings of the 17th annual international conference on Mobile computing and networking* (pp. 145-156). ACM.

Zhang, Z., Manjourides, J., Cohen, T., Hu, Y. and Jiang, Q., 2016. Spatial measurement errors in the field of spatial epidemiology. *International Journal of Health Geographics*, 15(1), p.21. Available at: <https://ij-healthgeographics.biomedcentral.com/articles/10.1186/s12942-016-0049-5>

Zittrain, Jonathan L., Engineering an Election (June 20, 2014). Harvard Law Review Forum, Vol. 127, p. 335, 2014; Harvard Public Law Working Paper No. 14-28. Available at: <https://ssrn.com/abstract=2457502>

Zuboff, S. (2015) 'Big Other: surveillance capitalism and the prospects of an informal civilization', *Journal of Information Technology* 30: 75–89.

D) Documents

Adams A., "Users' Perception of Privacy in Multimedia Communication," Proc. AMC Conf. Human Factors in Computing (CHI 99), ACM Press, 1999, pp. 53–54.

Acquisti A., & R. Gross, Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Privacy Enhancing Technologies Workshop (PET), 2006, Available at: <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf>

Andronikou V., Demetis D.S., Varvarigou T., Biometric Implementations and the Implications for Security and Privacy, 2007, Available at: http://journal.fidis-project.eu/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_Implications_for_Security_and_Privacy.pdf

Anjum, A.; Ilyas, M.U., "Activity recognition using smartphone sensors," Consumer Communications and Networking Conference (CCNC), 2013 IEEE, pp.914-919

ARTIS Research, Network Analysis, 2010, Available at: http://artisresearch.com/?page_id=2337

Asaro, P. (2007) Robots and Responsibility from a Legal Perspective, Proceedings of the IEEE Conference on Robotics and Automation, Workshop on Roboethics, Rome, April 14, 2007.

Bal G., Revealing Privacy-Impacting Behavior Patterns of Smartphone Applications, 2012, Available at: <http://mostconf.org/2012/papers/15.pdf>

Barkhuus, L. 2004. "Privacy in Location-Based Services: Concern Vs. Coolness," Mobile HCI 2004 Workshop: location System Privacy and Control, Glasgow, UK

Blum J., Prof. Evan Magill, M-Psychiatry: Sensor Networks for Psychiatric Health Monitoring, 28 August 2008, Available at:
<http://www.cms.livjm.ac.uk/pgnet2008/Proceedings/Papers/2008028.pdf>

Blumenstock, Chokkalingam et al, Probabilistic Inference of Unknown Locations - Exploiting Collective Behavior when Individual Data is Scarce, ACM DEV-5 (2014), December 5–6, 2014, San Jose, CA, USA, Available at:
<http://dx.doi.org/10.1145/2674377.2674387>

Bollier, D. (2010) ‘The Promise and Peril of Big Data’, Available at:
<http://www.aspeninstitute.org/publications/promise-peril-big-data>

Briggs, P., Future Identities: Changing identities in the UK – the next 10 years, UK Government Office for Science, January 2013

Burkert H. (1999) 'Privacy / Data Protection: A German/European Perspective' Proc. 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Mass., June 1999. Available at:
<http://www.coll.mpg.de/sites/www/files/text/burkert.pdf>

Bowker G C, 2003, “The past and the Internet” SSRC Items and Issues 4(4), Available at:
http://www.ssrc.org/programs/publications_editors/publications/items/online4-4/bowker-past.pdf

Cameron I., Venice Commission, Speaking Notes - European Parliament Hearing on Mass Surveillance, 7 November 2013, Available at:
<http://www.europarl.europa.eu/document/activities/cont/201311/20131114ATT74429/20131114ATT74429EN.pdf>

Camp, E., 2006. Metaphor in the Mind: The Cognition of Metaphor. *Philosophy Compass*, 1(2), pp.154-170.

Camp, L.J. and Connelly, K., 2008. Beyond consent: privacy in ubiquitous computing (UbiComp). *Digital privacy: Theory, technologies, and practices*, pp.327-343., p.333

Casady, T., Police Legitimacy and Predictive Policing, March 2011, Available at:
<http://www.nij.gov/topics/technology/maps/gps-bulletin-v2i4.pdf>

Casasanto, Daniel. “Perceptual Foundations of Abstract Thought.” Diss. MIT, 2005. Available at: https://www.researchgate.net/profile/Daniel_Casasanto/

Cate, Fred H., Peter Cullen, and Viktor Mayer-Schönberger. “Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines.” Available at: www.oii.ox.ac.uk/.../Data_Protection_Principles_for_the_21st_Century.pdf (2014).

Cisco Inc., Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011–2016, Available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

Clarke, R., Information Technology and Dataveillance, November 1987, Available at: <http://www.rogerclarke.com/DV/CACM88.html>

COE, Report on the application of data protection principles to the worldwide telecommunication networks, by Mr. Yves POULLET and his team, for the Council of Europe's T-PD Committee, point 2.3.1, T-PD (2004) 04 final, 13th December 2004, Available at: <https://rm.coe.int/168068416a>

Cope, S., & Ayres, I. (2007). *Super Crunchers: Why Thinking-by-Numbers Is the New Way to Be Smart*. Bantam Dell Publishing Group

David J. Crandall et al, Inferring social ties from geographic coincidences, Proceedings of the National Academy of Sciences of the USA 107, December 2010, Available at: www.pnas.org

Decker, M. 2008. "Location Privacy-an Overview", Mobile Business, 2008. ICMB '08. 7th International Conference on Mobile Privacy, pp. 221-230.

DEMOS, #Intelligence, 2012, Available at: http://www.demos.co.uk/files/_Intelligence_-_web.pdf

De Rosa, M., Data Mining and Data Analysis for Counterterrorism, March 2004, Center for Strategic and International Studies (CSIS), p.6, Available at: http://csis.org/files/media/csis/pubs/040301_data_mining_report.pdf

Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. PiOS: Detecting Privacy Leaks in iOS Applications. In Network and Distributed System Security Symposium, NDSS 2011, San Diego, CA, USA, 2011

Evans D., Cisco Internet Business Solutions Group, The Internet Of Things: How The Next Evolution Of The Internet Is Changing Everything, (2011), Available at: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

EDPS, Legitimate Reasons For Processing Of Personal Data, Available at: <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA6>

EDPS, The History of the General Data Protection Regulation, 2017, Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

Explanatory Memorandum, Recommendation No.R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, (Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies), Available at: www.coe.int/

EDPS, Internet of things: ubiquitous monitoring in space and time, European Privacy and Data Protection Commissioners' Conference Prague, Czech Republic, 29 April 2010, Available at:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Internet_Things_EN.pdf

EDPS, Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. C 128 of 6 June 2009

EU Commission, Full report on the public consultation on the ePrivacy Directive, December 2016, Available at: <https://ec.europa.eu/digital-single-market/news-redirect/37204>

EU Commission, REPORT FROM THE COMMISSION, First report on the implementation of the Data Protection Directive (95/46/EC), 15 May 2003, COM(2003) 265 final, Available at: <http://eur-lex.europa.eu/LexUriServ>

COM(92) 422 final — SYN 297 , Amended proposal for a COUNCIL DIRECTIVE on the protection of individuals with regard to the processing of personal data and on the free movement of such data, at p.26. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:1992:0422:FIN>

EU Commission, COMMISSION STAFF WORKING PAPER - Impact Assessment, General Data Protection Regulation and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC(2012) 72 final, Available at: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

EU Commission, Factsheet on privacy, data protection and information security, March 2013, Available at: http://ec.europa.eu/information_society/newsroom

EU Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4 November 2010, Available at: <http://eur-lex.europa.eu/LexUriServ>

EU Commission, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses - PRESS RELEASE, 25 January 2012, Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

EU Commission, European Commission sets out strategy to strengthen EU data protection rules - PRESS RELEASE: IP/10/1462, 4 November 2010, Available at: http://europa.eu/rapid/press-release_IP-10-1462_en.htm?locale=en

EU Commission, Data protection reform – frequently asked questions - PRESS RELEASE: MEMO/10/542, 4 November 2010, Available at: http://europa.eu/rapid/press-release_MEMO-10-542_en.htm?locale=fr

European Council — Council of the European Union, Data protection reform, September 2016. Available at: <http://www.consilium.europa.eu/en/policies/data-protection-reform/>

European Union Agency for Fundamental Rights, Handbook on European data protection law, 2014, Available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

European Police College (CEPOL), Cross-European Approaches to Social Media as a Tool for Police Communication, Issue 6 - Winter 2011/12, p.11, Available at: http://www.composite-project.eu/tl_files/fM_k0005/AB%20Downloads/Denef+Bayerl+Kaptein_6_Bulletin.pdf

Fast Company, Path Explores Ways To End Awkward Friendships: It's Not You, It's My Bot, 15 march 2013, Available at: <http://www.fastcompany.com/3007008/tech-forecast/path-explores-ways-end-awkward-friendships-its-not-you-its-my-bot>

Frank, R., C. Cheng, V. Pun, Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities, Research and National Coordination Organized Crime Division Law Enforcement and Policy Branch Public Safety Canada, Report No. 021, 2011, 2011, p.22, Available at: <http://www.sfu.ca/icrc/content/PS-SP-socialmedia.pdf>

FTC, Internet of Things - Privacy & Security in a Connected World, FTC Staff Report, January 2015, Available at: <http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

FTC, #484: FTC Seeks Input on Privacy and Security Implications of the Internet of Things, Available at: <http://www.ftc.gov/policy/public-comments/initiative-484>

FTC, Consumer Generated and Controlled Health Data, 7 May 2014, Available at: http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

FTC, Opening Remarks of FTC Chairwoman Edith Ramirez Privacy and the IoT: Navigating Policy Issues, International Consumer Electronics Show Las Vegas, Nevada, 6 January 2015, Available at: http://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf

Ghosh, A.K., and Swaminatha, T.M. 2001. "Software Security and Privacy Risks in Mobile E-Commerce," Communications of the ACM (44:2), pp. 51-57

Giannetsos, T., Dimitriou, T., R. Prasad, N., People-Centric Sensing in Assistive Healthcare: Privacy Challenges and Directions, Security And Communication Networks, (2010); pp.1-12, Available at: http://194.30.228.212/export/sites/default/ait_web_site/faculty/tdim/various/SensingHealthPrivChallenges.pdf

Gross, R. and Acquisti, A., 2005, November. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71-80). ACM.

The Guardian, How I became a Foursquare cyberstalker, 23 July 2010, <http://www.guardian.co.uk/technology/2010/jul/23/foursquare?INTCMP=ILCNETTX3487>

Hammond, S., Offender Profiling Of Sexual Offences, Broadmoor Hospital, 2007, p.3, Available at: http://www.ramas.co.uk/offender_prof.pdf

Hayashi, E., Das, S., Amini, S., Hong, J. and Oakley, I., 2013, July. Casa: context-aware scalable authentication. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (p. 3). ACM, p.2

HIDE FP7 Project, D3.3a Ethical Brief on Embedded Technology, 1 Feb 2008, Available at: <http://www.hideproject.org/documents/documents.html>

HMIC, The rules of engagement - A review of the August 2011 disorders, 2011, Available at: <http://www.hmic.gov.uk/media/a-review-of-the-august-2011-disorders-20111220.pdf>

HUMABIO FP6, Human monitoring and Authentication using Biodynamic indicators and behavioural analysis, D1.2 Scenarios of use and system requirements, December 2006, Available at: http://www.humabio-eu.org/docs/HUMABIO-D1_2.pdf

ICO, The Information Commissioner's response to Ofcom's consultation 'Promoting investment and innovation in the Internet of Things', October 1st 2014, Available at: <https://ico.org.uk/media/about-the-ico/consultation-responses/2014/2512/ico-response-to-ofcom-consultation-on-internet-of-things-20141001.pdf>

ICO, Jiang, B., and Yao, X. 2006. "Location-Based Services and GIS in Perspective," *Computers, Environment and Urban Systems* (30:6), pp. 712-725

ITU, The Internet of Things - Executive Summary, November 2005, Available at: www.itu.int/osg/spu/publications

Jain, A.K., Ross, A. and Prabhakar, S. (2004) 'An introduction to biometric recognition' *IEEE Trans. Circuits Systems Video Technologies*

Jain A.K., Dass S. C., and Nandakumar K., (2004) Soft Biometric Traits for Personal Recognition Systems, *Proceedings of International Conference on Biometric Authentication, LNCS 3072, Hong Kong, July 2004*

Joint Research Centre of the Commission and the Institute for Prospective Technological Studies, Future bottlenecks in the information society, June 2001, Available at: http://ec.europa.eu/justice/data-protection/document/studies/files/200106_ipts_itre_en.pdf, p. 104

Kosta, E. & Dumortier, J., 2015. ePrivacy Directive: Assessment of transposition, effectiveness and compatibility with the proposed Data Protections Regulation. Available at: <https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data>

M. Langheinrich, "Privacy by Design— Principles of Privacy-Aware Ubiquitous Systems," Proc. 3rd Int'l Conf. Ubiquitous Computing, Springer Verlag, 2001, pp. 273–291.

Lessig, L., Against Transparency, 9 October 2009, <http://www.tnr.com/print/article/books-and-arts/against-transparency>,

Michael Levi & David Wall, 'Crime and Security in the Aftermath of September 11: Security, Privacy and Law Enforcement issues relating to emerging information communication technologies' in 'Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)', July 2003, DG JRC, Available at: <http://www.jrc.es>

Lieshout M.V., Grossi L., Spinell G., Helmus S., Kool L., Pennings L., Stap R., Veugen T., Van der Waaij B., Borean C., (2007) RFID Technologies: emerging issues, challenges and policy options, Institute for Prospective Technological Studies, Seville.

Lohr, S., How privacy vanishes online, March 17 2010, Available at: <http://www.nytimes.com/2010/03/17/technology/privacy.html>

K. Lorincz, B. Chen, G. Challen, A. Chowdhury, S. Patel, P. Bonato, and M. Welsh. Mercury: A Wearable Sensor Network Platform for High-Fidelity Motion Analysis. In ACM SenSys, 2009. Available at: <http://www.eecs.harvard.edu/~mdw/papers/mercury-sensys09.pdf>

Manlio De Domenico, Antonio Lima, and Mirco Musolesi, Interdependence and predictability of human mobility and social interactions, Nokia Mobile Workshop, Newcastle, UK, June 2012, Available at: www.cs.bham.ac.uk/research/projects/nsl/mobility-prediction

Mann S. (1996) 'Smart Clothing: The Shift to Wearable Computing' Communications of the ACM 39, 8 (August 1996) pp. 23-24, Available at: http://www.eyetap.org/papers/docs/acm_comm96.pdf

Matheson R., Mental-health monitoring goes mobile, MIT News, 16 July 2014, Available at: <http://newsoffice.mit.edu/2014/mental-health-monitoring-goes-mobile-0716>

Microsoft Inc. Research, 'A Golden Era of Insight: Big Data's Bright Future', 15 February 2013, Available at: <http://www.microsoft.com/en-us/news/features/2013/feb13/02-15BigDataHorvitz.aspx>

MIT Technology Review, by Jamie Condliffe — New York City Has a Bold Plan to Fight Homelessness with Data, May 5, 2017. Available at: <https://www.technologyreview.com/s/604344/new-york-city-has-a-bold-plan-to-fight-homelessness-with-data/>

National Research Council, Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment, 2008, Available at: <http://www.nap.edu/catalog/12452.html>

The New York Times, Disruptions: And the Privacy Gaps Just Keep On Coming, 19 February 2012, <http://bits.blogs.nytimes.com/2012/02/19/disruptions-and-the-privacy-gaps-just-keep-on-coming/?ref=technology>

The New York Times, Web Site to Be Investigated for Posting Private Data, 13 March 2013, Available at: <http://www.nytimes.com/2013/03/13/us/personal-data-on-well-known-people-is-posted.html?hpw>

Nielsen, State Of The Media: The Social Media Report 2012, April 2012, p.2 Available at: <http://www.nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html>

OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", OECD Digital Economy Papers, No. 176, OECD Publishing.

OPINION OF ADVOCATE GENERAL CRUZ VILLALÓN - JOINED CASES C-293/12 AND C-594/12 DIGITAL RIGHTS IRELAND AND OTHERS - ECLI:EU:C:2013:845, 12 December 2013, Available at: <http://curia.europa.eu/juris/document/document.jsf?docid=145562&doclang=EN>

Pablo Paredes, David Sun, John Canny, Sensor-less Sensing for Affective Computing and Stress Management Technology, December 2013, Available at: <http://bid.berkeley.edu/stressmanagement/wp-content/uploads/2013/12/sensorless-sensing.pdf>

Patterson A., The Internet of Things: what is it and what does it mean for you?, 21 August 2014, Available at: <https://iconewsblog.wordpress.com/2014/08/21/the-internet-of-things-what-is-it-and-what-does-it-mean-for-you/>

PCAST, Report To The President - Forensic Science in Criminal Courts: Ensuring Scientific Validity, September 2016, Available at: https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf

Pentland, A. (2009). Reality mining of mobile communications: Toward a new deal on data, in The Global Information Technology Report, World Economic Forum & INSEAD, pp. 75–80.

Practis FP7, Privacy – Appraising Challenges to Technologies and Ethics, Deliverable D2.2: Final Horizon Scanning Report, July 2011, Available at: http://www.practis.org/docs/PRACTIS%20D2%20_130711final.pdf

P. Priya & Dr. J. C. Pamila, Discrimination in Data Mining, Available at: <http://www.europment.org/library/2014/venice/bypaper/OLA/OLA-19.pdf>, pp.1-7

Andrew Raij et al., Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment, in CHI 2011: Proceedings Of The Sigchi Conference On Human Factors In Computing Systems 11, 11 (2011), Available at: <http://pie.eng.usf.edu/wp-content/uploads/2011/12/raij-chi2011.pdf>

Reid D. A. et al, Soft Biometrics for Surveillance: An Overview, 2013, Available at: <http://core.ac.uk/download/pdf/9642804.pdf>

Reuters, by Alexei Oreskovic and Gerry Shih, Q+A-The complex interplay of social media and privacy, 20 February 2012, <http://www.reuters.com/article/2012/02/20/uk-privacy-explainer-idUSLNE81J01220120220>

Rosen, J. The Naked Crowd: Reclaiming Security And Freedom In An Anxious Age, 2003, Available at: <http://www.law.fsu.edu/faculty/2003-2004workshops/rosen.pdf>

Rosen L., Freedom and Open Source - The Language of Freedom, Prentice Hall, 2004, Available at: <http://www.rosenlaw.com/oslbook.htm>

Salvatore Ruggieri, Dino Pedreschi & Franco Turini, Data Mining for Discrimination Discovery, May 2010, 4(2) ACM Transactions On Knowledge Discovery From Data, Article 9

SAS Institute Inc., How Social Media Can Help Win the Battle for Public Security, 13 July 2012, Available at: <http://www.memex.com/content/how-social-media-analytics-can-help-win-battle-public-security>

Seifert, J. W., Data Mining And Homeland Security: An Overview, CRS Report RL31798, 2006.

Shoab, M.; Scholten, H.; Havinga, P.J.M., “Towards Physical Activity Recognition Using Smartphone Sensors,” Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), pp.80-87

Silberschatz, Korth & Sudarshan, Temporal and Spatial Data - Database System Concepts, 6 March 2007, Available at: <http://www.wis.win.tue.nl/~tcalders/teaching/dbmodels/pdf/>

Smith, D., Real-time Big Data Analytics: From Deployment to Production, Revolution Analytics, Available at: <http://www.revolutionanalytics.com/news-events/free-webinars/2012/real-time-big-data-analytics>

Spiekermann, S., Perceived Control: Scales for Privacy in Ubiquitous Computing (July 2005). 10th International Conference on User Modeling. Available at: <https://ssrn.com/abstract=761109>

Suler J., 'The psychology of cyberspace: the online disinhibition effect', Available at: <http://users.rider.edu/~suler/psycyber/disinhibit.html>

Taylor, A.S., Lindley, S., Regan, T., Sweeney, D., Vlachokyriakos, V., Grainger, L. and Lingel, J., 2015, April. Data-in-place: Thinking through the relations between data and community. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2863-2872). ACM.

Taylor R.B., (1997) 'Crime and place: what we know, what we can prevent, and what else we need to know,' Paper presented at the National Institute of Justice Annual Research Annual Conference, Washington DC, 1997

Technology Review, TR10: Reality Mining, March/April 2008, http://www.technologyreview.com/printer_friendly_article.aspx?id=20247

J. Ugander, B. Karrer, L. Backstrom & C. Marlow, The Anatomy of the Facebook Social Graph, 18 November 2011, p.1, Available at: <http://arxiv.org/abs/1111.4503>

UK Parliament, Independent Reviewer of Terrorism Legislation, A question of trust: report of the investigatory powers review, 11 June 2015, Available at: <https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review>

UK Parliament, Independent Reviewer of Terrorism Legislation, A question of trust: report of the investigatory powers review, 11 June 2015, Available at: <https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review>

UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26

UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988. Available at: <http://www.refworld.org/docid/453883f922a>

UN General Assembly Resolution, *The Right to Privacy in the Digital Age* - Report of the Office of the United Nations High Commissioner for Human Rights, A/RES/68/1670 of January 21, 2014, Available at: http://www.un.org/en/ga/search/view_doc.asp.

Upturn, David Robinson & Logan Koepke, Stuck in a Pattern - Early evidence on "predictive policing" and civil rights, August 2016, Available at: <https://www.teamupturn.com/reports/2016/stuck-in-a-pattern>

US Dept of Health, Education, and Welfare - United States of America. "Records Computers And The Rights Of Citizens." (1973), Available at: <http://epic.org/privacy/hew1973report/default.html>

Van der Ploeg, I., 'Biometrics and the body as information - Normative issues of the socio-technical coding of the body', in Lyon, David. *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge, 2003

Van der Ploeg, I., The illegal body: 'Eurodac' and the politics of biometric identification, *Ethics and Information Technology* 1: 295–302, 1999. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.200.9254&rep=rep1&type=pdf>

Wall Street Journal, Google's iPhone Tracking - Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy, 17 February 2012, <http://online.wsj.com>

David Wood & Stephen Graham, *Permeable Boundaries in the Software-sorted Society: Surveillance and the Differentiation of Mobility*, Paper for 'Alternative Mobility Futures' Lancaster University, 9-11 January 2004. Available at: http://www.academia.edu/1069340/Permeable_Boundaries_in_the_Software-sorted_Society_Surveillance_and_Differentiations_of_Mobility

World Economic Forum, *The Emergence of a New Asset Class*, January 2011, <http://www.weforum.org/reports/personal-data-emergence-new-asset-class>

WP29, Working document on biometrics, 12168/02/EN WP 80, 1 August 2003, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/>

WP29, Paper on health data in apps and devices, 9 February 2015, Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation>

WP29, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013, Available at: <http://ec.europa.eu/justice/policies/privacy>

WP29, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP131, 15 February 2007, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf

WP29, Opinion on the use of location data with a view to providing value-added services, 2130/05/EN WP 115, November 2005, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf, p.6

WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

WP29, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN WP 185, 16 May 2011, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

WP29, Opinion 15/2011 on the definition of consent, 13 July 2011, 01197/11/EN WP187, Available at:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

WP29, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

WP29, Opinion 15/2011 on the definition of consent, 01197/11/EN WP187, 13 July 2011, Available at:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf, p.7

WP29, ‘Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights’, 5143 /99/EN WP 26, 7 September 1999, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp26_en.pdf

WP29, ‘Statement on the role of a risk-based approach in data protection legal frameworks’. WP218 (2014) Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

Young, W., Blumenstock J. E., Fox, E. B., and McCormick, T. H. (2014). Detecting and classifying anomalous behavior in spatiotemporal network data. The 20th ACM Conference on Knowledge Discovery and Mining (KDD '14), Workshop on Data Science for Social Good, New York, NY.

E) Cases

European Court of Human Rights (ECHR)

Alkaya v. Turkey, judgment of 9 October 2012 (application no. 42811/06)

Amann v. Switzerland [GC], no. 27798/95, § 68, p.20, ECHR 2000-II

Biriuk v. Lithuania, No. 23373/03, § 37, 25 November 2008

Bykov v. Russia [GC], No. 4378/02, 10 March 2009

Cemalettin Canli v. Turkey, No. 22427/04, 18 November 2008

Copland v. the United Kingdom, April 3, 2007 [ECtHR]

Hasan and Chaush v Bulgaria, no 30985/96, 2000 [ECtHR]

Halford v United Kingdom (1997) 24 EHRR 523

Haralambie v. Romania, No. 21737/03, 27 October 2009

I. v. Finland, No. 20511/03, 17 July 2008

Khan v. the United Kingdom, no. 35394/97, ECHR 2000-V

Klass and others v. Federal Republic of Germany, [ECtHR] (Series A, NO 28) (1979-80) 2 EHRR 214

Kopp v. Switzerland, no. 23224/94 (1998)

Liberty and others v. United Kingdom (App. No. 58243/00)

Malone v. the United Kingdom, no. 8691/79 (1984)

S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04

Mikulić v. Croatia, ECHR, No. 53176/99, 7 Feb. 2002

Moreno Gómez v. Spain, Application no. 4143/02, 16 November 2004

Niemietz v. Germany (1992) 116 EHRR 97, §29

Peck v. United Kingdom (2003) 36 E.H.R.R. 41.

Pfeifer v. Austria, no. 12556/03, § 35, ECHR 2007

P.G. and J.H. v. the United Kingdom, no. 44787/98

Perry v The United Kingdom (2003) ECHR App. no. 63737/00

Rotaru v. Romania [GC], no. 28341/95, § 54, ECHR 2000-V

Uzun v. Germany (no. 35623/05, 2 September 2010)

Vogt v. Germany (1996) 21 EHRR 205, (17851/91)

Weber and Saravia v. Germany (dec.), no. 54934/00.

Z v. Finland, judgment of 25 February 1997, 1997-I

European Court of Justice (CJEU)

Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014

Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 13 May 2014

Case C101-01 *Bodil Lindqvist*, 6 November 2003

Case C-212/13, *Ryneš*, 11 December 2014

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015

Case C-112/00 *Schmidberger* [2003] ECR I-5659

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063

Other jurisdictions

United States

ACLU v. Reno, 929 F.Supp., 521 U.S. 844 (1997)

Boy Scouts of America v. Dale, 530 U.S. 640 (2000)

Carpenter v. United States, 16-402 (2017)

Denver Area Educational Telecommunications Consortium, Inc. v. FCC, 518 US 727 (1996)

Dodich v. Niantic Inc., 16-cv-04556, U.S. District Court, Northern District of California (2017)

Kyllo v. United States, 533 US 27 (2001)

Marder v. Niantic Inc., 16-cv-04300, U.S. District Court, Northern District of California (2017)

United States v. Jones, 132 S.Ct. 945 (2012)

Whitney v. California (No. 3), 274 U.S. 357 (1927)

Germany

Hessischer Datenschutzgesetz vom. 7 October 1970 GVBl. II 300-10

Gesetz zum Schutz vor Mißbrauch personenbezogener Date bei der Dateverarbeitung, Federal Data Protection Act (BDSG), Bundesgesetzblatt (BGBl) 1, S 201. (1977)