European University Institute

DEPARTMENT OF LAW

EUI Working Papers

LAW 2010/18
DEPARTMENT OF LAW

A LEGAL METHOD FOR SOLVING ISSUES OF INTERNET REGULATION; APPLIED TO THE REGULATION OF CROSS-BORDER PRIVACY ISSUES

Dan Jerker B. Svantesson

EUROPEAN UNIVERSITY INSTITUTE, FLORENCE
DEPARTMENT OF LAW

A Legal Method for Solving Issues of Internet Regulation; Applied to the Regulation of Cross-Border Privacy Issues

DAN JERKER B. SVANTESSON

EUI Working Paper **LAW** 2010/18

ISSN 1725-6739

Printed in Italy
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu
cadmus.eui.eu

Author contact details

Dr. Dan Jerker B. Svantesson
Associate Professor, Faculty of Law
Bond University
Gold Coast, Queensland, 4229
Australia

E-mail: Dan_Svantesson@bond.edu.au
Ph: +61 7 5595 1418
(www.svantesson.org)

This article was primarily written during the author's time as a Visiting Fellow at the European University Institute (Florence, Italy) in February 2010. The author wishes to thank all the friendly staff members at the EUI, and in particular Professor Giovanni Sartor, as well as the following people for their valuable input: Professor Ross Buckley, Dr Lee Bygrave, Professor John Farrar, Mr Christopher Kuner, Dr Radim Polčák and Professor William Van Caenegem.

Abstract

This article presents a legal method that can be used to find solutions to the challenges of regulating Internet technology. The method consists of ten steps and the reader is guided through the application of these steps. To illustrate the use of the method, it is applied to the research task of finding a solution to the conundrum of regulating cross-border data flows on the Internet.

Thus, the article has two distinct aims, and it should benefit anyone with an interest in research methodology, as well as those interested in the regulation of privacy in general, and on an international level, in particular.

Keywords

Legal method, Legal research, ICT law, Internet law, Privacy law, Data protection, Cross-border data flow

1. Introduction

This article has two distinct aims. First, it presents a legal method that can be used to find solutions to the challenges of regulating Internet technology. Second, applying this method, it seeks a solution to the conundrum of regulating cross-border data flows on the Internet. As such, the article is necessarily somewhat schizophrenic in its goals. However, by incorporating the second goal as an example of how the legal method is to be applied on a practical level, the two goals are, in a sense, merged. Put differently, the possible solution to the regulation of cross-border data flows on the Internet constitutes a useful by-product of the description of the legal method that is the first-mentioned goal of the article.

Consequently, a reader primarily interested in the article from the perspective of the method it describes, may treat the parts of the article that apply the method to the cross-border data flows on the Internet as cursory readings; or indeed, skip those parts all together. Similarly, a reader primarily interested in the solution presented here to the problems of regulating cross-border data flows on the Internet, may not need to give too much attention to the details of the method itself.

Having provided some necessary background observations regarding both the method and the issues surrounding the regulation of cross-border data flows on the Internet, the method, with its ten steps, is described and applied to the regulation of cross-border data flows on the Internet. The article concludes with some final remarks.

1.1. Background to the Aim of Developing a Legal Method that Can Be Used to Find Solutions to the Challenges of Regulating Internet Technology

Having been involved in research relating to the regulation of various forms of Internet technology for some years, it seems to me that the researcher is regularly exposed to certain recurring themes.[1] Some of those themes affect how we carry out our research, while others affect what we can expect from our research findings, and how we present them. However, we are so accustomed to these themes that we do not generally stop to reflect on them and their implications for our work, Here, I will highlight four such themes.

The law will always struggle to keep up with the pace of technological development. While this is only natural bearing in mind the typically lengthy process involved in law making, it has undesirable consequences where, for example, particular behaviour is lawful simply because the legislators have not had time to make it unlawful. At the same time, both dangers and difficulties arise where the law seeks to predict and/or influence the development path that technology will take. Thus, to a degree, it is understandable that the law is reactive, rather than proactive. As a consequence of this theme, researchers in the field of information technology law must always consider whether the regulatory approaches they propose ought to be technology neutral, or technology specific (discussed further below 4.7).

[1] *See* JAY FORDER & DAN SVANTESSON, INTERNET & E-COMMERCE LAW (2008) (where many of these themes have been highlighted).

Another recurring theme is that many practitioners in the legal professions struggle to understand the technology. While the fact that the law cannot keep up may be something we simply have to live with, this should not be an excuse for the legal profession. The unfortunate truth is that many interested parties, including judges, academics, solicitors and barristers, simply do not have sufficient understanding to deal with the legal challenges in an informed way. There is a lot of truth in the observation that "[j]udges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average . . . five-year-old tosses about with breezy familiarity."[2]

The results of technology-ignorance in the legal community can be devastating, with cases being decided and lost based on unsound arguments from the parties and/or unsound reasoning by the courts.[3] While highlighting the importance of legal research relating to information technology law, this also suggests that, where possible, research findings must be presented in an as simple and accessible manner as possible, so as to ensure they reach the audience.

A third recurring theme is that our society is increasingly globalised—our thinking is no longer centred on our immediate surroundings to the exclusion of the bigger picture. In the Internet context, when deciding what newspaper to read, or where to buy music, we consider sources from all over the world. Globalisation would have occurred to some degree also without the Internet, but there can be no doubt that the Internet encourages a global outlook in ways that were not previously possible.

In the context of globalisation, it is relevant to note that the Internet is an international medium, which has implications for how a country can regulate Internet activity. For example, if a country was to ban a certain online activity, this would have little impact if the activity continued to take place outside that country, and the people of that country could continue to access and participate in it over the Internet. This may lead to the conclusion that international cooperation is the only truly effective way forward when dealing with, at least some aspects of, Internet regulation.[4]

Another consequence of society's increasing globalisation is that researchers are encouraged to broaden the scope of their research to also consider developments in other jurisdictions – as most countries face the same issues in finding solutions to Internet law complications, a solution in one country may be helpful also in other countries.

A further reoccurring theme is that the Internet and e-commerce have had dramatic growth patterns. However, neither the Internet generally, nor e-commerce in particular, have reached their growth potential. The main reason for this is that many businesses as well as consumers fear the risks involved. These concerns may, for example, relate to things such as fraud, privacy, the validity of e-contracts and issues that arise from the international nature of Internet interactions. The question for the law is how it can help inspire confidence in the Internet so that it achieves its potential.

---

2 American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 170 (S.D.N.Y. 1997) (Preska, J.).

3 *See* Dan Svantesson, *The Times They Are A-changin' (Every Six Months) – The Challenges of Regulating Developing Technologies*, F. ON PUB. POL'Y: A J. OF THE OXFORD ROUND TABLE, at 9-11 (Online Spring 2008), *available at* http://forumonpublicpolicy.com/archivespring08/svantesson.pdf (last visited Apr. 9, 2010).

4 This is not least true in the privacy setting. *See, e.g.*, Joshua S. Bauchner, *State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate*, 26 BROOK. J. INT'L L. 689, 717 (2000-2001).

I suspect that, at least partly, due to these recurring themes, researchers in this field are repeatedly adopting a similar research method when dealing with matters of Internet regulation. However, for many of us this is probably done in the blindness that comes with routine, without much considered thought – we know what to do, and we do it without specifying or discussing how we do it. Some would say that is a good thing, and to a large degree, I would be inclined to agree with Radbruch's statement that "sciences which have to busy themselves with their own methodology are sick sciences."[5]

Nonetheless, suppose we allow ourselves to stop and consider how we do what we do. It is in this light that the method parts of the article are to be read. Thus, while there is not much about the method that is original, in the sense of ideas that never have been thought by anyone before, the method is novel in the sense that it has not been presented in a systematic manner until now.

I will not busy myself with delineating different methodologies for legal research and seeking to fit the method advocated here within such a framework. It suffices to say that the method proposed here is a pragmatic ten-step model that can be used to find solutions to the challenges of regulating Internet technology in a manner that meets the four goals of: (1) being reasonably simply to use; (2) providing for an adequate degree of research transparency; (3) being scalable, so as to be useful for a variety of types of research tasks; and (4) being flexible enough to suit a range of different styles of research.

Thus, the method will be beneficial for anyone starting out doing research on a topic that broadly falls within the field of Internet regulation. For example, doctoral candidates seeking to devise a suitable research project in this area of research may benefit from considering the method described here, whether they ultimately adopt it or not. However, it is hoped that, also researchers with many years of experience may find some aspects of the method interesting.

Indeed, it is hoped that, while the method is specifically designed to find solutions to the challenges of regulating Internet technology, it will also be useful for similar tasks in other areas of the law.

1.2. Background to the Aim of Finding a Solution to the Regulation of Cross-Border Data Flows on the Internet

To prepare ground for a discussion of the need for regulating cross-border data flows on the Internet, it is useful first to make some observations about privacy generally. However, the development of privacy as a legal concept, and the important functions that concept fills, have been well documented elsewhere, and will not be repeated here.[6] For the purpose of this article, it suffices to note that, despite its relatively lengthy history, and despite being a globally recognised fundamental human right, on a practical level privacy is not deeply rooted in the minds of the public. Instead, one frequently comes across the attitude that only those who are seeking to hide something are interested in privacy; or the corollary, if you have nothing to hide, why worry about privacy?

---

5 KONRAD ZWEIGERT & HEIN KÖTZ, INTRODUCTION TO COMPARATIVE LAW 33 (3d rev. ed. 1998) (referring to GUSTAV RADBRUCH, EINFÜHRUNG IN DIE RECHTSWISSENSCHAFT 253 (12th ed. 1969)).

6 *See, e.g.*, Wilbur Larremore, *Law of Privacy*, 12(8) COLUM. L. REV. 694 (1912); Gehan Gunasekara, *The 'Final' Privacy Frontier? Regulating Trans-border Data Flows*, 15(3) INT'L J. L & INFO. TECH. 362 (2007); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (1999-2000); Warren B. Chik, *The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on the Internet: A Comparative Case Study of Hong Kong and Singapore – Two Differing Asian Approaches*, 14 INT'L J.L. & INFO. TECH. 47 (2006).

Such views are sheer nonsense, and are particularly worrying when expressed by people who are in a position to seriously affect the privacy afforded to the public. For example, it is disappointing to see Google's CEO Eric Schmidt state that: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[7] Even worse, Facebook's Chief Executive, Mark Zuckerberg, has declared the age of privacy to be over.[8]

The significance of this type of attitude is emphasised by the fact that "[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive."[9] In some cases individuals are blissfully unaware of their privacy being violated, but in other cases individuals are knowingly and willingly sacrificing their privacy for the convenience of access to information technology resources:

> As consumers and as citizens, we repeatedly trade convenience for control, handing over growing amounts of information about ourselves to others in the process. Our lives are increasingly mediated by digital technologies and described by data held in digital formats. We are racing ahead quickly with the development of new technologies while the institutions-legal and otherwise-designed to protect user privacy have lagged behind. The tradeoffs involved are rarely conscious ones.[10]

Palfrey goes on to note that "[t]his growing problem has its roots in the fact that, as information technologies improve in efficiency and become more integrated in everyday life, fewer and fewer citizens are likely to know what information is being collected about them and by whom."[11]

While this certainly is true, the problem also has another cause; as exemplified in the recent developments of covert tracking and surveillance facilities for mobile phones, those involved in designing technologies frequently fail to assess the societal implications of the use of the products they develop.[12] The time for technology developers to realise that not everything technically 'doable' should be done is long overdue.

Schartum describes how data protection is being impaired by three major factors:

> i) changing statutory content as a result of a shift in the balance of interests, ii) inadequate formulation of data protection laws, and iii) insufficient ability to implement and enforce such laws. Factor i) refers to a re-evaluation of data protection in relation to other values and interests (cf. anti-terror measures, organised crime, health services etc.), and concerns mainly the political level. Factor ii) refers to how and where political intentions are placed and expressed in legal instruments (directives, national legislation, etc.), while factor iii) encompasses issues of awareness, communication and interpretation of data protection laws.[13]

---

7 Ryan Tate, *Google CEO: Secrets Are for Filthy People*, GAWKER, Dec. 4, 2009, http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people (last visited Apr. 8, 2010).

8 Bruce Schneier, Google And Facebook's Privacy Illusion, Forbes.com, Jun. 4, 2010, http://www.forbes.com/2010/04/05/google-facebook-twitter-technology-security-10-privacy.html?boxes=Homepagechannels (last visited Apr. 8, 2010).

9 United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

10 John Palfrey, *The Public and the Private at the United States Border with Cybserpace*, 78 MISS. L.J. 241, 243 (2008-2009).

11 *Id.*

12 Jordan Cressman, *Does Mobile Spying Software Go Too Far With Latest Update?*, I4U NEWS, Apr. 27, 2010, http://www.i4u.com/article33515.html (last visited May. 5, 2010).

13 Dag Wiese Schartum, *Designing and Formulating Data Protection Laws*, 18(1) INT'L J. L & INFO. TECH. 1, 1 (2010).

In the context of societal attitudes towards the right of privacy, it is interesting to look at that right from Olivecrona's perspective on rights. Discussing the meaning, or lack thereof, of the terms "rights" and "duties", Olivecrona observed that:

> The sentence that A is the owner of this piece of land functions as a *permissive sign* for himself with regard to this piece of land; at the same time it acts as a *prohibitive sign* for everybody else. The sentence is a green light for the owner, a red light for the others.[14]

Applying this to privacy, the sad truth is that one person's right of privacy far too seldom results in a red light for others. Indeed, as many people seem to struggle with what entitlements come with a right to privacy, the light that should have been green, may more often be amber, signalling the risks associated with an uncharted territory. Further, it seems that a large section of the younger generation simply ignore the lights altogether in their use of *Facebook* and other social media. Put in other, perhaps clearer, words, people in general either have a too vague idea of what entitlements stem from their right of privacy, or fail to appreciate the importance of privacy and the social, political and economical value that is attached to their personal data.[15] At the same time, businesses, governments and others, in whom we entrust our most personal information, do not feel significantly restrained in how they use and abuse our privacy. Taken together, this combination results in an inadequate privacy protection, and if we return to Olivecrona's terminology, it could be said that we need privacy rights to result in clearer green lights and clearer red lights.

This can be contrasted to other human rights, and perhaps most beneficially to a human right that often competes directly with the right of privacy; that is, the right of freedom of expression. When it comes to freedom of expression, most people see a very strong green light. Indeed, in many cases a stronger green light than what actually may be justified under the law – at least in most western countries, people feel they have a right to say what they want to say. This is one side of the coin. The other side consists of the fact that most people perceive a strong red light preventing them from interfering with other peoples' right of free expression.

If it is conceded that all this is correct, we must move on to ask how we can achieve a clearer understanding and stronger respect for the right of privacy. Olivecrona's writings can aid us also in this regard. In discussing "performative utterances" such as promises made in a contractual situation, he notes that:

> Their consequences are of a double nature. First, they have immediate, psychological effects. The promisor feels himself bound; the promisee feels entitled to expect the promisor to act accordingly; contrary behavior is apt to provoke hostile reactions. Secondly, the acts correspond to certain requirements in the law; they are relevant in one way or another for actions by the state organs. Since the state organs regularly apply the rules, the promisor is likely to be exposed to a sanction if he breaks his promise; his awareness of this fortifies the immediate psychological effect of the promise on him.[16]

---

[14] Karl Olivecrona, *Legal Language and Reality*, *in* ESSAYS IN JURISPRUDENCE IN HONOR OF ROSCOE POUND 151, 183 (R. A. Newman ed., 1962).

[15] As to the social, political and economical value of personal data, it has been noted that "[i]n some sectors, particularly in the on-line environment, personal data has become the de facto currency in exchange for on-line content". Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, at 5, WP 173 (adopted on Jul. 13, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

[16] Olivecrona, *supra* note 16, at 180.

Olivecrona also notes that: "The green and red lights do not express any notions. They are signs which have a social function because people have been taught to react to them in certain ways."[17] Combining these two observations, the effect a right has is consequently based on the immediate psychological reaction it causes and the extent to which the law enforces, and *is seen to enforce*, the right. As expressed by Schartum, "it is clearly insufficient to fight for a particular level of formal protection (law in book) unless this is combined with efforts to ensure reasonable conformity with the law in action."[18]

The solution would then seem to lie in changing the psychological reaction to privacy rights, and applying law more effectively and visibly.[19] Indeed, combined with public education, a more effective and visible application of the law to protect privacy may change the psychological reaction to privacy rights.[20]

Turning to the issue of cross-border data flows more specifically, it is clear that, with advances in communication technologies, the branch of privacy law that focuses on data protection has grown in significance. Indeed, with more and more data being collected, by an increasing number of diverse entities, it can reasonably be expected that data protection will continue increasing in significance.

One of the most interesting and controversial areas of data protection, in our interconnected world, is the regulation of cross-border data flows. The regulation of cross-border data flows goes back, at least, to the *Swedish Data Act* of 1973. Amongst other things, Section 11 of that Act made clear that:

> If there is reason to assume that personal data will be used for automatic data processing abroad, the data may be disclosed only after permission from the Data Inspection Board [Datainspektionen]. Such permission may be given only if it may be assumed that the disclosure of the data will not involve undue encroachment upon personal privacy.[21]

In his comprehensive work dealing with privacy regulation, Bygrave discusses the rationale of transborder data flow regulations:

> The chief aim of these rules [i.e. the rules regulating transborder data flows] is to hinder data controllers from avoiding the requirements of data protection laws by shifting their data-processing operations to countries with more lenient requirements (so-called 'data havens').[22]

---

17 *Id.* at 183.

18 Schartum, *supra* note 15, at 2.

19 Also other scholars have argued in favour of this combination. *See, e.g.*, Chik, *supra* note 8, at 97-98.

20 For an interesting discussion of the importance of proper reporting, *see* Graham Greenleaf, *Reporting Privacy Complaints Pt 1: A Proposal for Systematic Reporting of Complaints in Asia-Pacific Jurisdictions*, 9(3) PRIVACY L. & POL'Y REP. 41 (2002) (Austl.); Graham Greenleaf, *Reporting Privacy Complaints Pt 2: Complaint Reporting Practices of Asia-Pacific Privacy Commissioners*, 9(4) PRIVACY L. & POL'Y REP. 74 (2002); Graham Greenleaf, *Reporting Privacy Complaints Pt 3: Complaint Reporting Practices of Canadian Privacy Commissioners*, 9(6) PRIVACY L. & POL'Y REP. 111 (2002). *See also* Gunasekara, *supra* note 8, at 392.

21 11 § Datalag (1973:289) (Swed.). Translation of: "Finns det anledning antaga att personuppgift skall användas för automatisk databehandling i utlandet, får uppgiften lämnas ut endast efter medgivande av Datainspektionen. Sådant medgivande får lämnas endast om det kan antagas att utlämnandet av uppgiften icke kommer att medföra otillbörligt intrång i personlig integritet." Furthermore, through a latter amendment 7 a § made clear that "The responsible keeper of a file shall have in his possession an up-to-date list ol [sic] the personal tiles for which he is responsible. The list shall contain particulars of . . . the extent to which personal data are disseminated for automatic data processing abroad." (Translation of "Hos den registeransvarige skall finnas en aktuell förteckning över de personregister som han är ansvarig för. Förteckningen skall innehålla uppgift om […]i vad mån personuppgifter lämnas ut för automatisk databehandling i utlandet"). The translations were found at http://archive.bild.net/dataprSw.htm (last visited May. 6, 2010) and verified by the author.

22 LEE A. BYGRAVE, DATA PROTECTION LAW – APPROACHING ITS RATIONALE, LOGIC AND LIMITS 79-80 (2002).

So far, that aspect of privacy law has gained relatively limited academic attention. However, with an ever increasing degree of globalisation, there are reasons to think that the attention offered to the regulation of cross-border data transfers will increase.

There may be multiple reasons why academics so far have been loath to give this issue attention, despite the fact that, restrictions on cross-border data flows may severely impact on the use of modern communications technologies. For example, to discuss the regulation of cross-border data one must have a solid understanding of a difficult cross-section of jurisdictional issues, privacy law and technology. However, academics in frontier fields are rarely put off by a challenge, so it is likely that there are other contributing factors as well. One factor that is likely to have impacted negatively on the academic interest in the issue is the lack of cases in the field. Compared to many other interesting IT law areas, the regulation of cross-border data has only rarely been considered by the courts.[23] This lack of case law is significant as it may signal at least five different things:

1. that the law governing cross-border data transfers is so weak as to rarely be of significance;
2. that infringements of the law rarely are noticed;
3. that the victims are not in a position to pursue the infringements;
4. that the body's charged with ensuring compliance with privacy laws have not sufficiently prioritised cross-border data transfers; and/or
5. that cross-border data transfers are uncontroversial and, thus, unlikely to give rise to legal disputes.

While the first four alternatives seem likely causes for the lack of cases, it is not possible to conclude that cross-border data transfers are uncontroversial to such a degree as to be unlikely to give rise to legal disputes.

To understand the complexity of the regulation of cross-border data flows, it is interesting to stop and consider the wide range of types of transfers that occur on a daily basis:

Type of transfer:	**Example(s):**
Intentional cross-border personal communications	(1) Adam sends an e-mail to Bert (who lives in another country) describing his current state of health. (2) Adam sends an e-mail to Bert (who lives in another country) describing the current state of health of Adam's friend Cecilia.
Intentional cross-border consumer communications	Adam buys a product from a website in another country and in doing so provides personal information.

[23] *See, e.g., id.* at 223.

Type of transfer:	**Example(s):**
Behind the scenes cross-border personal communications	(1) Adam sends an e-mail to Donna (who lives in the same country as Adam) describing his current state of health. Donna uses an e-mail system where the e-mails are stored on a server outside that country. (2) Adam sends an e-mail to Donna (who lives in the same country as Adam). Donna uses Google's Gmail and Adams personal information is collected and transferred to Google's servers outside the country.
Unintended cross-border personal communications	(1) Adam places information about the current state of health of Cecilia on a website. (2) Adam uses a search engine to find information about a particular illness. The search is logged against his IP address by the search engine provider located in another state.
Commercial cross-border data export[24]	(1) Adam's bank exports his personal information to another country for business efficiency reasons. (2) Company A in state A sells a mailing list, containing personal information of people in state A, to company B in state B.[25]
Behind the scenes commercial cross-border data transfers	While surfing the 'net', 'cookies' are installed onto Adam's computer by website A. Those cookies are then used by website B (in a different country) to collect information about Adam's surfing habits.
Cross-border data exports as part of international judicial cooperation[26]	The authorities in state A export personal information about Adam to the authorities in state B.

[24] The prevalence of both so-called "back office outsourcing" and so-called "front office outsourcing" increased significantly over the past years. Holder and Grimes have explained this by noting that "[t]he convergence of the need for a portfolio of services to be sourced globally with the ability of business process outsourcers to do so on a cost effective basis has driven the outsourcers to geographical locations previously ignored by most business sectors", James T. Holder & David E. Grimes, *Government Regulated Data Privacy: The Challenge for Global Outsourcers*, 38 GEO. J. INT'L L. 695, 696 (2006-2007). Interestingly, and worryingly, Holder and Grimes concludes that "[t]here are simply no longer any geographical borders on the maintenance and use of the consumer's personally identifiable information", *id.*.

[25] The privacy issues that arise in this type of scenario, particularly in the EU/US setting are examined in Craig Martin, *Mailing Lists, Mailboxes, and the Invasion of Privacy: Finding a Contractual Solution to a Transnational Problem*, 35 HOUS. L. REV. 801 (1998-1999).

[26] For a discussion of such matters, *see, e.g.*, Patricia L. Bellia, *Chasing Bits across Borders*, U. CHI. LEGAL F. 35 (2001).

2. An Overview of the Method

The method outlined in the article consists of ten steps. The aim is that where a researcher follows these ten steps in her/his endeavour to find a solution to a regulatory problem falling within the discipline of Internet law, she/he will have a maximal chance of finding a suitable solution. Much of it is based on structures researchers may instinctively follow. However, it was felt that it would be useful to clearly outline what we as researchers may be doing without consciously thinking of what we are doing.

The first four steps can be viewed as the initial phase of the method, with step one involving defining the problem. When that is done, the researcher should seek to identify any constraints that fundamentally impact on the issue. For example, if one is to find a solution to the regulation of Internet defamation, one cannot ignore the human right of freedom of expression – the human right of freedom of expression is a *fundamental constraint* for any solution to the regulation of Internet defamation. The researcher can then move on to identifying other, less significant constraints that should be taken account of. We can call them *non-fundamental constraints*. Once all the constraints have been identified, it is necessary to assess how the constraints interact. For example, some constraints will strengthen each other, while others will be each others' opposites requiring careful balancing.

Applied correctly, steps, two (the identification of fundamental constraints), three (the identification of non-fundamental constraints) and four (the assessment of how the constraints interact) ensure that the method takes account of the context of the problem, thereby disposing of one of the traditional criticisms of stricter doctrinal research methodologies.[27]

The next phase (steps five to seven) – the information gathering phase – is doctrinal in nature and involves an examination of how the problem has been addressed so far, an examination of how similar problems have been addressed so far and finally a critical evaluation of the approaches identified.

In steps eight, nine and ten (the third and last phase; the construction phase), the researcher must construct the solution, and then test it against the fundamental, and non-fundamental, constraints, as well as against any relevant likely future technological developments and uses. Step nine (testing the solution against the constraints) and ten (testing the solution against any relevant likely future technological developments and uses) work to ensure that the solution serves the purposes it was intended to serve, and has the effects it ought to have when put in the context in which it will operate.

The method I am advancing in this article is scalable and flexible in virtually each of its ten steps. This is important as it makes it possible to utilise the method for research tasks of various character. For example, I used a version of this method in writing my PhD thesis, but it should also be useable for much smaller research tasks.

[27] WILLIAM TWINING, ACADEMIC LAW AND LEGAL DEVELOPMENT 20 (1976), *cited in* TERRY HUTCHINSON, RESEARCHING AND WRITING IN LAW 22 (3d ed. 2010).

3. Step One – Defining the Problem

As in any scientific endeavour, the first step is to define the problem that is to be addressed, and the research task must be specified with as much precision as is possible.

Some commentators have written about how a researcher ought to identify a topic for her or his research, and it seems that finding a topic can involve a very complex process consisting of both brainstorming and heuristics, as well as mind mapping and 'thinking hats'.[28] However, the best, and most enjoyable, research is typically done where there is a natural fit between the researcher and the topic, and where the researcher has chosen the topic out of a strong interest in it. Indeed, unless the topic 'comes to' you as the researcher, you should probably ask yourself at least two questions; first, do I really wish to devote the required time and effort to this particular research question, and second, am I a suitable researcher for this particular research question?

As is discussed below, the manner in which the problem is defined may affect the level of abstraction necessary for the solution. For example, where the problem is defined as producing legislation to address a certain technology, the solution may need to be drafted in great detail (i.e. at a low level of abstraction). In contrast, where the problem is defined as producing a standard of regulation on a global level for a certain technology, a rather higher level of abstraction may be required, with the solution being presented as general principles.

In defining the problem, it is also important to consider how the issue to be addressed fits within the overall picture. In other words, the researcher must contemplate how the solution will affect related areas of regulation, as well as how related areas of regulation will affect the solution. This is absolutely crucial as a solution for one regulatory task must be viewed as a component in the larger machinery that is the legal system.

Applying this step to the issue of the regulation of cross-border data flows, there are several options. For example, the problem, or research task, could be to identify a regulatory solution to suit the needs of a specific country, and the political goals that country is striving towards. However, as this is a global issue facing every nation connected to the Internet, I have opted for a more globally applicable research task. This is likely to require my solution to be presented at a relatively high level of abstraction.

The research task I set myself can then be expressed as follows:

> *Construct a set of principles that regulate cross-border data flows on the Internet.*

At least one problem with this definition is obvious. It is technology-specific where it may be more appropriate, not to say necessary, to adopt a technology-neutral solution. The reason I have opted to define my research task as an attempt to construct a technology-specific solution is found in the first aim of this article – to outline a method that can be used to find solutions to the challenges of regulating Internet technology. However, as is clear from the below, one of the fundamental constraints I identify for this task is that the solution must be technology neutral (see 4.7 below); to solve the technology-specific problem I set out to address, I end up having to adopt a technology-neutral approach after all.

---

[28] *See, e.g.*, Hutchinson, *supra* note 29, at 137-155.

This may of course seem like a rather round-about way of doing things, and the obvious alternative would be to rephrase the research task in technology-neutral language. However, as this article seeks to illustrate a method, I need to work through each step of that method in order, even where I normally may have been able to take a shortcut by anticipating the need for a technology-neutral solution. Technology neutrality is discussed in more detail below. It suffices at this stage to note that it is quite common that technology-specific problems are addressed by a technology-neutral solution.

As mentioned, one important component of the first step of the method is to assess how the solution will affect related areas of regulation, as well as how related areas of regulation will affect the solution. As far as my research task is concerned here, the regulation of cross-border data flows affects, and is affected by, at least two related areas of regulation, that is:

- The regulation of extraterritorial claims affecting cross-border data flows on the Internet;[29] and
- The regulation of cross-border cooperation efforts in the context of cross-border data flow on the Internet.

In a sense, the identification of these related areas of regulation sets the outer limits of what needs to be considered in this research task. Further, having identified these related areas of regulation will assist me in all the other steps of the method.

4. Step Two – Identifying Fundamental Constraints

At step two of the method, the researcher must identify any constraints that are of fundamental importance for the solution to the research task, or problem, as defined in step one; that is constraints of such fundamental importance that a solution that does not take account of them cannot be acceptable. Put differently, the fundamental constraints represent the *limits to any acceptable solution*.

The constraints discussed here come in at least three different, but partly overlapping, forms. There are practical constraints, such as technical and legal realities, regulatory constraints, such as applicable law that must be taken into account, and aspirational constraints, such as constraints justified by reference to societal goals. Using the constraints identified below as examples, the first kind of constraints – the practical constraints – include e.g. the observations that not all technologies are set up to be sensitive to data crossing borders. An example of the regulatory constraints is found in the fact that the solution must take account of the fact that there is such a thing as a basic human right of freedom of expression. Finally, the aspirational constraints are exemplified in the observation that modern society requires cross-border transfers of data.[30]

[29] For a comprehensive discussion of the issues associated with the regulation of extraterritorial claims in the context of online privacy, *see* Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 1)*, 18 INT'L J.L & INFO. TECH. 176 (2010), and Part 2 (to be published). *See also* Lee A. Bygrave, *Determining Applicable Law Pursuant to European Data Protection Legislation*, 16(4) COMPUTER L. & SECURITY REVIEW 252 (2000).

[30] Perhaps it could be argued that this aspirational consideration also could be classed as a practical constraint.

The identification of some such fundamental constraints – namely the practical and regulatory constraints – can be made simply by observing the surrounding realities. While that gives the illusion of objectivity, subjective judgements are involved in the selection of which constraints to include. For example, if one accepts Fuller's thinking, the fundamental constraints should always incorporate his eight "routes to disaster" in lawmaking, described in his influential *The Morality of Law*:

> The first and most obvious lies in a failure to achieve rules at all, so that every issue must be decided on an ad hoc basis. The other routes are: (2) a failure to publicize, or at least to make available to the affected party, the rules he is expected to observe; (3) the abuse of retroactive legislation, which not only cannot itself guide action, but undercuts the integrity of rules prospective in effect, since it puts them under the threat of retrospective change; (4) a failure to make rules understandable; (5) the enactment of contradictory rules or (6) rules that require conduct beyond the powers of the affected party; (7) introducing such frequent changes in the rules that the subject cannot orient his action by them; and finally, (8) a failure of congruence between the rules as announced and their actual administration.[31]

Such observations as to what the law ought to be, what Farrar terms "standards of good legal craftsmanship and process,"[32] have a long history going back at least to Roman jurists:

> Ulpian, summed up the basic precepts of the law as being "*honeste vivere, alterum non laedere, suum cuique tribuere*" which, being roughly translated, means that the law should cause one to live honestly, not to harm another and to give each person his or her due.[33]

Certain research tasks may justify all, or some, of these observations being treated as fundamental constraints. However, the researcher must carefully assess whether doing so is necessary.

The identification of other fundamental constraints – that is the aspirational constraints – will inevitably involve even more subjective value judgements. And of course, where subjective value judgements form part of a scientific method, that method is at risk of being criticised as being insufficiently objective, and thereby, insufficiently scientific. This is an important issue requiring some discussion.

First, and perhaps slightly off topic, I wonder whether social sciences, such as jurisprudence, have gone too far in the direction of natural sciences with their stricter adherence to objectivity. It seems that researchers are not allowed to make any assumptions based on what seems self-evident. Instead everything needs to be backed up by a footnote "proving" the legitimacy of the researcher's claim. Perhaps in some cases an exaggerated emphasis on scientific method actually stands as an obstacle for creative and pragmatic solutions? Furthermore, perhaps the area of information technology law is a particularly fertile ground for less orthodox research methods, involving subjectivity "based on wisdom, morals or sense for fairness."[34]

---

31 LON L. FULLER, THE MORALITY OF LAW 39 (2d ed. 1969).

32 JOHN FARRAR, LEGAL REASONING 258-259 (2009).

33 *Id.* at 259.

34 Radim Polčák, *ICT Law as a Discipline, in* INTRODUCTION TO ICT LAW – SELECTED ISSUES 18 (Radim Polčák ed., 2007).

This takes us to what we may call the dilemma of the validity of the unprovable self-evident. Certain assumptions a person make are self-evident to that person, without it being possible to prove the objective validity of the assumptions. While nine out of ten other persons might share all the assumptions, and while ten out of ten people may share nine out of ten of the assumptions, it is not possible to declare the assumptions as universally accepted. To borrow from Robert P. George's interesting discussion of Grisez-Finnis' theories[35]:

> The claim that they are self-evident does not imply that they are undeniable or, still less, that no one denies them. What it does imply is that the practical intellect may grasp them, and practical judgement can affirm them without the need for a derivation. (Which is not to say that they can be grasped without an understanding of the realities to which they refer.)[36]

Can then such assumptions legitimately make up the foundation for a solution to a regulatory problem? In my view they can. The simple truth is that some assumptions are sensible for the very reason that they are sensible. For such assumptions there is no need for attempts to anchor them in prior theories, studies or other works.

Furthermore, at least some of the negatives of a partially subjective method can be avoided by flagging the subjectivity when presenting the solution. For example, instead of proclaiming the research finding as an objective best practice model, the researcher ought to state that, given the, partially subjective, fundamental constraints taken into account, the proposed solution represents a best practice model.

Having said that, it is of course still advisable for the researcher to keep the subjectivity at a minimum. One way of achieving some degree of objectivity is to identify the fundamental constraints through a statistical study in which a relevant section is asked to select fundamental constraints e.g. from a list of possible alternatives in relation to the problem defined in step one.

One final observation must be made as to the fundamental constraints identified in step two and the non-fundamental constraints identified in step three. Some such constraints are so general in nature that they are likely to represent constraints for a wide range of regulatory research tasks. For example, one of the non-fundamental constraints identified in step three is that, where possible, the solution identified in step eight should be widely acceptable. This constraint is by no means unique to the research task to which the method is applied in this article. As a consequence, a researcher using the proposed method will often be able to draw upon some constraints identified in previous applications of the method. Furthermore, researchers, particularly those who are applying the method for the first time, will do well to look to what constraints their colleagues have identified when applying the method.

In identifying the fundamental constraints for the research task of constructing a set of principles that regulate cross-border data flows on the Internet, I have not used any statistical tools. Rather, my fundamental constraints represent what I personally perceive as the unprovable self-evident.

---

35 Those theories have, of course, no application here.

36 Robert P. George, *Recent Criticism of Natural Law Theory*, 55 U. CHI. L. REV. 1371, 1389 (1988).

4.1. People have a Basic, but Limited, Right of Privacy

Privacy is a fundamental human right recognised in several international instruments, such as the *International Covenant on Civil and Political Rights* (ICCPR). More specifically, Article 17 of the ICCPR states that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

As privacy is at the heart of the current inquiry, identifying this right and its scope is of great importance – there can be no doubt that this right constitutes a fundamental constraint on any solution to the task of constructing a set of principles that regulate cross-border data flows on the Internet.

The problem is, of course, that, so far, there have been no successful attempts at defining the scope of this right with any great precision. In other words, the question: "What is privacy?" does not have an obvious or universally accepted answer.

Put very simply, privacy could be said to mean the "right to be let alone"[37]. Another possible definition is that privacy is "[t]he interest of a person in sheltering his or her life from unwanted interference or public scrutiny."[38] An even more sophisticated definition would be to say that privacy relates to "[m]aterial that so closely pertains to a person to his[/her] innermost thoughts, actions and relationships that he[/she] may legitimately claim the prerogative of deciding whether, with whom and under what circumstances he[she] will share it."[39] Neither of these definitions could be said to be more correct than the others, but taken together they provide a rather clear picture of what we mean when we talk about privacy.

In relation to our discussion, we can, however, define privacy more accurately. Distinctions are typically drawn between different forms of privacy. The following, partly overlapping, categories are often distinguished:

- Information privacy;
- Personal privacy;
- Communications privacy; and
- Surveillance privacy.

Of these categories of privacy, it is so-called information privacy that is of relevance for the research task of constructing a set of principles that regulate cross-border data flows on the Internet.

Perhaps the most interesting question, as to the scope of the right of privacy, is its jurisdictional limitations. The simple fact is that, for a person's privacy to be adequately protected, it must be protected against abuse regardless of the geographical source of that abuse. It is not sufficient to be protected against abuse by individuals and organisations in one's own jurisdiction, if individuals or organisations located outside that jurisdiction can collect, use and distribute one's personal information in contravention of one's right of privacy.

---

37 S. Warren & L. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

38 PETER NYGH & PETER BUTT, BUTTERWORTHS CONCISE AUSTRALIAN LEGAL DICTIONARY (2d ed. 1998).

39 AUSTRALIAN LAW REFORM COMMISSION, UNFAIR PUBLICATION: DEFAMATION AND PRIVACY 110 (Report No. 11, 1979).

To understand how Article 17 is meant to work in a cross-border context, it is necessary to take account of Article 2(1) of the ICCPR:

> 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.

It seems possible to argue that the phrase "to respect and to ensure to all individuals *within its territory and subject to its jurisdiction* the rights recognized in the present Covenant" (emphasis added) in Article 2(1) of the ICCPR expresses two separate requirements rather than a double requirement.[40] From that vantage point, Article 17 means that each state that has signed and ratified the ICCPR has an obligation to provide legal protection against unlawful attacks on the privacy of people subject to the State's jurisdiction *and* those present within its territory, regardless of the origins of the attacks.

Either way it is clear that, each signatory is required to make jurisdictional and legislative claims over foreign people making unlawful attacks on the privacy of people within the jurisdiction and territory of the signatory state. While potentially controversial under the rules of jurisdiction under international law, this interpretation is supported in CCPR General Comment 16: "Provision must also be made for everyone effectively to be able to protect himself against any unlawful attacks that do occur and to have an effective remedy against those responsible."41 (emphasis added). If the privacy of a person in state B is negatively affected by material originating in state A, state B does arguably not provide "an effective remedy against those responsible" unless its laws provide for jurisdictional and legislative claims over the offender in state A.[42] In other words, Article 17(2) of the ICCPR appears to be a source of international law, requiring signatory states to make fairly wide jurisdictional claims in relation to the protection of the privacy of people within their jurisdiction or territory.

4.2. People Have a Basic, but Limited, Right of Freedom of Expression

Like the right of privacy, the right of freedom of expression is a basic human right. Article 19 of the ICCPR provides that:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

---

[40] *See* S. JOSEPH ET AL., THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS: CASES, MATERIALS, AND COMMENTARY 58-65 (2000); M. NOVAK, UN COVENANT ON CIVIL AND POLITICAL RIGHTS 26 (1993).

[41] Human Rights Committee, *General Comment No. 16: The Right to Respect of Privacy,Ffamily, Home and Correspondence, and Protection of Honour and Reputation (Art. 17)*, at ¶ 11 (Aug. 4, 1988), *available at* http://www2.ohchr.org/english/bodies/hrc/comments.htm (follow "Article 17 (Right to privacy" hyperlink).

[42] It can, of course, be said that even such a jurisdictional claim does not in itself provide "an effective remedy against those responsible" unless it can also be enforced. However, state B in our example cannot be required to do more than what is in its power to do.

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

The right of freedom of expression has also, directly or indirectly, made its way into many countries' fundamental laws. The most obvious example is perhaps the First Amendment to the US Constitution which states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

Other countries do not so clearly proclaim this right. In Australia, for example, the High Court has, in the absence of express provisions in the Constitution, recognised an implied right of free political speech.[43] Yet other countries include freedom of speech in their fundamental law without applying it in a manner that conforms to what perhaps most people in the western world would regard as essential for an effective protection of free speech. For example, Article 35 of the 1982 Constitution of the People's Republic of China states that: "Citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession and of demonstration."

Either way, to make my research task manageable, I will only look at freedom of expression from the perspective of how it works under the ICCPR.

Like with the right of privacy, it is necessary to examine the jurisdictional scope of the right of freedom of expression. Put differently, while it is clear that there is a right of freedom of expression, we must ask whether there is a right of freedom of expression across borders. If there is no right of freedom of expression across borders, the right of freedom of expression would not be a fundamental constraint for a solution to the problem of constructing a set of principles that regulate cross-border data flows on the Internet.

To assess the jurisdictional scope of the right of freedom of expression it is necessary to return to ICCPR Article 2(1) (discussed above, 4.1). It will be recalled that the relevant part of that Article made clear that State Parties to the ICCPR undertake to respect and to ensure "to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant".

Imagine that a person in state A places content on a website, and as a result is prosecuted in state B. State B can only do so successfully if it regards itself to have jurisdiction over the offender in state A. In that case, state B should reasonably also view itself as having jurisdiction for the purposes of Article 2(1) of the ICCPR, with the consequence that state B must respect the offender's right of freedom of expression.

In light of this, it seems clear that, like the right of privacy, the right of freedom of expression can cross borders. Any other conclusion would mean that the freedom of expression does not apply where the expression is made using Internet technologies with a global reach – a disturbing outcome indeed.

It is, however, necessary to distinguish between situations where a state is applying its laws in a manner that restricts people in other states exercising their freedom of expression on the one hand, and situations where a state applies its laws in a manner that allows free expression within its borders, but does not allow the expression to cross its borders, on the other hand.

---

[43] Refer to the landmark cases of: Nationwide News Pty Ltd v. Wills (1992) 175 C.L.R. 1 (Austl.); Australian Capital Television Pty Ltd v. The Commonwealth (1992) 175 C.L.R. 106. For a brief discussion of the position of Human Rights in Australia, *see* FARRAR, *supra* note 34, at 247-255.

The first type of situation would, for example arise where a person in state A places content on a website, and as a result is prosecuted in state B. The second type of situation would arise, for example, where special rules regulate cross-border data flows – a person has freedom to express herself/himself within the borders of the state, but does not have the right to express herself/himself in the same manner where the expression represents the export of personal data.[44]

While the first of these situations would represent a violation of the freedom of expression, the status of the latter is less certain.

4.3. Modern Society Requires Cross-Border Transfers of Some Data

Possibly the easiest way of avoiding privacy violations stemming from personal data crossing borders would be to proclaim that no such transfers are allowed. Yet such an approach is utterly incompatible with the needs of modern society.[45] Indeed, several diverse aspects of modern society, such as commerce, law enforcement, and even some aspects of health care, require cross-border data flows.

Further, modern technologies like the Internet would simply not work in the absence of such transfers. Cross-border flow of personal data is a pre-requisite for all aspects of Internet communication. It is, after all, a global network of networks. Further, restrictions on cross-border data transfers may often be an impediment to cross-border e-commerce, and other valuable international interaction, such as social networking.

In light of this, one fundamental constraint, placed on any solution to the research task of constructing a set of principles that regulate cross-border data flows on the Internet, is that it must allow cross-border data flows to such a degree, so as to not unduly restrict or limit the proper function of Internet communication. Further, while not all forms of personal information must cross borders in all imaginable situations, the regulation must not restrict such data flows unless such restriction is necessary.

4.4. Some of the Data that Necessarily Crosses Borders for the Proper Function of Internet Communication is Personal in Nature

Privacy laws will typically only protect information that is personal. Consequently, to determine whether a particular instance of cross-border data transfer amounts to a privacy concern under current laws, it is necessary to establish whether the information, or data, in question falls within the definition of "personal information" or "personal data". This brings us to the actual definition of "personal information" or "personal data", which, as can be expected, varies from jurisdiction to jurisdiction. Despite the diversity, certain general observations can be made. For example, The Organisation for Economic Co-operation and Development and Asia-Pacific Economic Cooperation both define personal information/data to mean any information about/regarding an identified or identifiable individual.[46]

---

[44] Care must, however, be taken in the determining the circumstances in which such restrictions may be placed on the freedom of expression. This is particularly so bearing in mind the important role cross border information flows may play for human rights developments in places where such developments are most needed. *See* Dina Koutouki, *Human Rights: Benefits of Information Technology*, 48 U.N.B.L.J. 265 (1999); Aisha Husain, *Framing the International Standard on the Global Flow of Information on the Internet*, 3 INTERDISC. J. HUM. RTS. L. 35 (2008-2009).

[45] PETER BLUME, RETLIG REGULERING AF INTERNATIONALE PERSONDATAOVERFØRSLER 166 (2006).

[46] *See* Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, at Part 1 (1980), *available at* http://www.oecd.org/ (search "protection of privacy"; then follow "OECD Guidelines on the Protection of Privacy" hyperlink under "Documents"); Asia-Pacific Economic

The EU definition, as well as the definition found in the Australian *Privacy Act 1988* (Cth), are more detailed:

> '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 (EU Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 2(a))
>
> "personal information" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. (*Privacy Act 1988* (Cth), s. 6)

Looking at these provisions, there can be little doubt that, if, for example, a medical practitioner in one country exports identifiable patient data about one of her patients to a medical practitioner (or drug company) in another country, that will amount to a transfer of person information. Similarly, where a company in state A collects data relating to the shopping habits of its consumers in state A, and then transfers that data to another company in state B, we have a case of transfer of personal data. This is uncontroversial and needs no further discussion. But there are important borderline cases and more interesting questions arise if we ask whether the type of data that necessarily is transferred across borders, as part of the Internet's basic operation, meets the test of constituting personal data. For example, is the name of an e-mail account (e.g. dasvante@bond.edu.au) personal information? And, can an Internet Protocol (IP) address (e.g. 131.244.15.161) amount to personal information?

These matters have gained considerable attention in recent time, and it is necessary to discuss e-mail addresses and IP addresses separately.

There are several factors that affect whether an e-mail address can amount to personal information. For example, there is a difference between an address that includes a person's name (e.g. Dan_Svantesson@bond.edu.au, or dan@svantesson.org) and addresses that do not in themselves include sufficiently clear identity clues (e.g. asdfghj1234@hotmail.com). It is of course more likely that the former type can be viewed as being personal information than the latter.

Furthermore, there is a difference between an e-mail address indicating an organisation to which a person is attached (e.g. @eui.eu) and more generic e-mail addresses (e.g. @gmail.com). In a similar manner, an e-mail address indicating a specific geographical region (e.g. @qld.gov.au) may be more likely to amount to personal information than an e-mail address that does not do so.

At the basis of it all are considerations as to whether the e-mail address as a whole, combined with any other accessible data, reasonably identifies a person (whether correctly or incorrectly) as being the data subject.

The conclusion reached immediately above is valid also for IP addresses. However, the question of whether an IP address, combined with any other accessible data, reasonably identifies a person (whether correctly or incorrectly) as being the data subject, is typically more complicated.

(Contd.)

Cooperation, APEC Privacy Framework, ¶ 9 (Oct. 29, 2004), available at http://www.apec.org/ (search "privacy framework"; then follow "APEC Privacy Framework" hyperlink).

There are several cases from various jurisdictions that have considered this issue. In some cases, the court has decided that IP addresses are not personal in nature. For example, in the US case *Columbia Pictures Indus. v. Bunnell*,[47] the Court stated that: "As an IP address identifies a computer, rather than a specific user of a computer, it is not clear that IP addresses [...] are encompassed by the term 'personal information' in defendants' website's privacy policy".[48] Other US courts have reached virtually identical conclusions.[49]

Similarly, in Hong Kong (SAR) the Administrative Appeals Board has upheld the Hong Kong Privacy Commissioner's view that an IP address does not *per se* satisfy the definition of personal data since it is "information about an inanimate computer, not an individual."[50]

In contrast, the Article 29 Data Protection Working Party[51] takes the view that "IP addresses attributed to Internet users are personal data and are protected by EU Directives 95/46 and 97/66."[52] The Working Party reached its conclusion in light of the fact that "[i]n the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may be other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means."[53]

Interestingly, there is a diversity of opinion amongst the member states of the EU. "The Appeal Court of Paris has ruled in several judgments that an IP address only allows one to identify a computer, and, therefore, its processing does not allow one to identify its user."[54] While there no doubt may be strong political reasons[55] motivating such a conclusion, the better view was expressed by a Swedish court, Stockhom Länsrätt, in 2006. The case stemmed from the actions of Antipiratbyrån (a private organisation aiming at identifying file sharers and bringing them to prosecution). That organisation had collected data, including IP addresses, for their purposes. It was undisputed in the case that ISPs can identify subscribers based on the IP address. But the Antipiratbyrån argued that, as the actual user could be a person other than the subscriber, the IP address is not personal information. The Court (Länsrätten) did not agree. The majority held that:

> The physical person that can be identified by reference to the IP number need not be the actual user. Rather, already the fact that a physical person can be identified as the subscriber is sufficient for the IP number to be regarded as personal information under PUL ["Personuppgiftslagen" i.e. the relevant Act].[56]

---

47 C.D. Cal. (May. 29, 2007).

48 *Id.*

49 *See, e.g.*, Johnson v. Microsoft, W.D.Wa. (Jun. 23, 2009).

50 Shi Tao v. The Privacy Comm'r For Pers. Data, 16 Administrative Appeals Board 2007 (H.K.), *available at* http://www.pcpd.org.hk/english/publications/files/Appeal_Yahoo.pdf (last visited May. 3, 2010).

51 The Article 29 Data Protection Working Party was established by Article 29 of Directive 95/46/EC as an independent EU Advisory Body on Data Protection and Privacy.

52 Article 29 Data Protection Working Party, *Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6*, WP 58, at 3 (adopted on May. 30, 2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp58_en.pdf.

53 *Id.*

54 Fanny Coudert & Evi Werkers, *In The Aftermath of the Promusicae Case: How to Strike the Balance?*, 18(1) INT'L J.L & INFO. TECH. 58 (2010).

55 *See, e.g., id.* (discussing the impact this interpretation has in relation to copyright societies).

56 Case number 15646-05 (decided 2006) of the Stockhom Länsrätt. Author's translation of "Den fysiska person som med hjälp av IP-numret kan identifieras måste inte vara den faktiska användaren utan redan det faktum att en fysisk person kan identifieras som abonnemangsinnehavare är tillräckligt för att IP-nummer skall anses vara en person uppgift i PUL:s mening."

The view expressed by Stockhom Länsrätt is, thus, in line with the approach taken by the Article 29 Data Protection Working Party.

The Australian Law Reform Commission took a position representing some form of middle ground. It stated that "Information that simply allows an individual to be contacted—such as a telephone number, a street address or an IP address in isolation—would not fall within the recommended definition of 'personal information'."[57] However, it also stated that:

> While stand alone telephone numbers, street addresses and IP addresses may not be personal information for the purposes of the *Privacy Act*, such information may become personal information in certain circumstances. The ALRC acknowledges that telephone numbers relate to telephones or other communications devices, IP addresses to computers, and street addresses to houses, rather than individuals, but notes that such information may come to be associated with a particular individual as information accretes around the number or address.[58]

In light of the above, it is no wonder that commentators conclude that the debate is still open as to whether IP addresses amount to personal information.[59] However, perhaps it can be concluded that, (1) in some instances IP addresses are highly likely to be widely recognised as personal information; (2) in some instances IP addresses are unlikely to be widely recognised as personal information; and (3) in some instances, whether or not IP addresses are recognised as personal information, will vary from jurisdiction to jurisdiction, and possibly from court to court.

To conclude the discussion of how some of the data that necessarily crosses borders for the proper function of Internet communication is personal in nature, there can be no doubt both e-mail addresses and IP addresses can amount to personal information in some circumstances.

4.5. Data Crossing Borders Represent a Loss of Control for the Data Subject

One fundamental constraint is found in the fact that once data crosses borders, the data subject loses a degree of control over the data.[60] While this proposition may be rather self-evident, it is nevertheless necessary to expand on what is meant by 'control' in this context.

I am here not primarily referring to any actual ability to influence how an organisation uses or discloses our personal data. The reality is that, once data is in the hands of a organisation, data subjects have no actual control over its use and the disclosure of the data; such is the nature of information. Instead, what I am referring to as 'control' has, at least, four aspects:

- The ability to detect misuse;
- The ability to identify the party responsible for the misuse;
- The ability to hold that party accountable for the misuse; and
- The ability to prevent further misuse by that party.

---

57 AUSTRALIAN LAW REFORM COMMISSION, FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE ¶ 6.61 (Report No. 108, 2008).

58 *Id.* at ¶ 6.60.

59 Coudert & Werkers, *supra* note 56, at 60.

60 *See also* BLUME, *supra* note 47, at 22.

Thus, 'control' in this context relates to retroactivity rather than prevention, and all four aspects of control are typically negatively affected through cross-border data transfers. In most cases, it is harder to detect misuse overseas, and it is harder to identify the party responsible for the misuse, where the misuse takes place overseas. Further, holding a party located overseas accountable is made more difficult in several ways. First, once the responsible party has been identified, it may be hard to find that party. Second, once identified and located, holding that party accountable involves finding an appropriate forum in which to seek redress and establishing a liability under the applicable law. Third, the victim is often faced with severe enforcement difficulties.

Finally, once data has been misused overseas, it may be more difficult to ensure that the data cannot be misused there in the future.

4.6. Not All Technologies are Set Up to Be Sensitive to Data Crossing Borders

The Internet was designed with certain requirements in mind. As it, and its uses, have developed, it has become abundantly clear that the thinking in the original design does not cater for all its uses today. Indeed, some aspects of the Internet's design are directly contrary to some of the Internet's present uses. For example, while designed as an open network, modern e-commerce relies heavily on encryption.

For our purposes, it is relevant that the Internet was designed to allow for seamless data transfer across borders. As a direct consequence, on its most basic level, Internet technology does not recognise geographical borders. Internet communication can flow freely between most countries, without there being any border checks. And indeed, without the persons involved in the communication being aware of the exact extent to which their communications cross any borders.

Looking at the Internet from the perspective of what it is used for, it is clear that many uses depend on this borderlessness. For example, users are typically unaware of, and uninterested in, where their data is stored when they use cloud computing solutions such as some e-mail services (e.g. Hotmail) and social networking tools (e.g. *Facebook*). The impact of cloud computing is discussed in more detail below (12.2).

However, what has been said above is not the full story. Some countries have chosen to exercise a degree of border control. For example, the Internet in the People's Republic of China (PRC) is structured according to a four-tier system not dissimilar to that of many other states. Starting from the bottom we have the individual Internet users (tier four). They connect to the Internet through Internet Service Providers (ISP)[61] (tier three). The ISPs connect to an Internet Access Provider (IAP)[62]. The IAPs, representing the second tier, are the ones that actually own the physical networks, which are leased by ISPs. Finally the IAPs connect to the Government's gateway (tier one) and can thereby access the global Internet. What makes this system different from the system of many other states is the fact that this is not merely the system normally used, but the system prescribed by law.[63] Thus, for

---

[61] Or "Access Networks" as they are referred to in the *Provisional Regulations of the People's Republic of China for the Administration of International Connections to Computer Information Networks* (1997).

[62] Or "Interconnecting Networks" as they are referred to in the *Provisional Regulations of the People's Republic of China for the Administration of International Connections to Computer Information Networks* (1997).

[63] *See Provisional Regulations of the People's Republic of China for the Administration of International Connections to Computer Information Networks* (1997). I have been unable to confirm whether this Provisional Regulation still is in force. However, the key point, that the PRC exercises a relatively strict control over what crosses the border to the PRC part of the Internet, is beyond doubt. *See also* OpenNet Initiative, *Internet Filtering in China in 2004-2005: A Country Study*, ALL CONTENT RELATED TO CHINA, http://www.opennetinitiative.net/studies/china/ (last visited Apr. 25, 2006).

example, an Internet user may not connect to the Internet via a foreign ISP in order to circumvent the system.[64] Similar structures can be found, for example, in Saudi Arabia.

In contrast most other countries cannot exercise any effective border control due to the fact that Internet communications, both domestic and foreign, go through a multitude of private and public carriers – there simply are no effective 'strangle points'. Against this background, the 'international Internet' is to be viewed as borderless, while, for example, the domestic sub-Internet in the PRC is borderless only within China, but not in relation to the rest of the world.

Either way, the fact that Internet technology (both on its fundamental level and on an applications level) typically ignores geographical borders, with the consequence that Internet users do not always know when and where their data crosses geographical borders, must be considered a fundamental constraint for the research task addressed here.

4.7. The Regulation of Cross-Border Data Flows Must Be Technology Neutral[65]

As indicated in the discussion above about the reoccurring themes in this area of research, researchers in the field of information technology law must always consider whether their research findings will be technology-neutral, or technology-specific. Regulation is technology specific where it expressly, or implicitly, specifies the type of technology it applies to. In contrast, regulation is technology-neutral where it is expressed in such a manner as to be applicable to any technology.

The New Zealand Law Commission's *Electronic Commerce Part One: A Guide for the Legal and Business Community*, describes "technological neutrality" in the following manner:

> Technology has advanced with great speed in recent years. It is likely to continue to do so. Unlike technology, the law tends to develop slowly, usually by reacting to situations only as they arise. It is therefore vital that any reform of the law be drafted so as to take account not only of the technology currently available, but also that which has yet to be developed.[66]

The aims of technological neutrality, and the related concept of functional equivalence,[67] could be seen as extensions of a more general goal applicable to any form of regulation; that is, all laws must be drafted at a suitable level of generalisation. In other words, all laws have to aim to be applicable where such application is desirable, but not applicable where application is undesirable. Despite this foundation in an undisputable goal for legal drafting, and despite the fact that functional equivalence and technological neutrality have become widespread guiding principles for how legal drafters approach Internet regulation, the two concepts have not been free from criticism.

In an interesting article Escudero-Pascual and Hosein demonstrate the potential downside of technology-neutral solutions:

---

64 Any such attempts will be punished. *See, e.g.*, The Supreme People's Procuratorate, *Official Reply of the Supreme People's Procuratorate on the Application of Laws to Acts of illegally Operating International, Hong Kong, Macao, or Taiwan Telecommunication Services*, ISINOLAW, Feb. 6, 2002, *available at* http://www.isinolaw.com.

65 In part, this section draws upon aspects of Svantesson, *supra* note 5.

66 NEW ZEALAND LAW COMMISSION, ELECTRONIC COMMERCE PART ONE: A GUIDE FOR THE LEGAL AND BUSINESS COMMUNITY 17 (Report 50, 1998).

67 "[T]he functional equivalence approach . . . is based on an analysis of the purposes and functions of the traditional paper based requirement with a view to determining how those purposes or functions could be fulfilled through electronic commerce techniques. . . . [T]he adoption of the functional-equivalent approach should not result in imposing on the users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment." UNCITRAL, MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT 1996 WITH ADDITIONAL ARTCLE 5 BIS AS ADOPTED IN 1998 at 20-21, U.N. Sales No. E.99.V.4 (1996).

> [A] reason for technology-neutrality is to ensure that new laws do not need to be passed every time a new technology is invented. However, technology-neutral language may be used to ignore, willful or not, the challenges, risks, and costs to applying powers to different infrastructures.[68]

In other words, a good technology-neutral solution of today is no guarantee for it being a suitable form of regulation in relation to a future technology. A hypothetical example will provide more detail.

Imagine the work on an Internet-related international convention, perhaps having lasted for ten years or more, resulting in a technology-specific text. If such a convention was completed in the late 80's or early 90's, it would presumably have addressed, for example, BBS communication, but certainly not WWW communication.[69] Keeping in mind the current high speed of technical development, and the slow legislative process both domestically and internationally, it may be pointless to create Internet-related technology-specific law. At the same time we must question what effect a technology-neutral rule constructed in the late 80's or early 90's to perhaps address a BBS-specific concern would have on the WWW or P2P communications in use today.

Furthermore, we need not look far to find examples of serious consequences lying in store where there is an overreliance on technology neutrality. For years, copyright regulations around the world have failed to cope with the peculiarities of digital media, such as music and movies. The stubborn attachment to a principally technology neutral regulation has effectively rendered the copyright law in a state of bankruptcy.

To conclude, in the drafting of legal rules one must balance the risk of those rules becoming outdated and thereby useless (which, in turn, will call for new rules to be constructed), and the risk of those rules being applicable in situations they were not suited for.

Further, it is not always obvious how the concepts of functional equivalence and technological neutrality successfully are to be applied in relation to electronic communications.[70]

---

[68] A. Escudero-Pascual & I. Hosein, *The Hazards of Technology-Neutral Policy: Questioning Lawful Access to Traffic Data*, http://www.ssrc.org/programs/itic/publications/civsocandgov/hosein.pdf (last visited Feb. 12, 2008).

[69] The reader will recall that the use of the WWW is largely a mid-90's and onwards trend.

[70] Svantesson, *supra* note 5.

Despite there being both pros and cons associated with a technology neutral approach, I have concluded that, the construction of a set of principles that regulate cross-border data flows on the Internet requires those principles to be technology neutral. In other words, I have made the assessment that, to construct principles that regulate cross-border data flows on the Internet, I have to construct a set of principles that regulate cross-border data flows irrespective of the technology used to facilitate the transfer.

This is probably a rather orthodox conclusion, and it can be expected that researchers faced with other research tasks will also conclude that technological neutrality is a fundamental constraint on their solutions.

5. Step Three – Identifying Non-Fundamental Constraints

Once the fundamental constraints have been identified, it is appropriate to consider whether there are any other, less important, constraints to take account of. The necessity of this step may vary depending on the research task, but it would often be the case that, in identifying the fundamental constraints, a researcher identifies other factors that it is appropriate, but not necessary, to take into account. As such non-fundamental constraints are likely to impact on the solution adopted in step eight, they should be announced and discussed, which is why step three is important – it provides structure for, and additional transparency into, the researcher's thinking.

Distinguishing between fundamental and non-fundamental constraints will not always be an easy task. Indeed, subjectivity will again be an issue. However, in determining whether a particular constraint is fundamental or not, the research should ask whether a solution can be acceptable where it does not take account of the restraint in question. If the answer is yes, then the constraint in question is not fundamental. If the answer is no, then the constraint is a fundamental one.

Like the fundamental constraints, the non-fundamental constraints come in at least the three different forms of practical constraints, regulatory constraints, and aspirational constraints.

Looking at the research task of constructing a set of principles that regulate cross-border data flows on the Internet, I have identified the following non-fundamental constraints.

5.1. Where Possible, the Solution Should Be Widely Acceptable

The solution benefits from being widely acceptable; that is, it is better if a solution is palatable to all relevant parties than if it is not; that much is self-evident and beyond intelligent dispute. The real question is whether a palatable solution always is better than an unpalatable solution. Put differently, of how great importance is it that the solution is palatable to the relevant parties, compared to the importance of other considerations?

First and foremost, the researcher should not be too willing to sacrifice the solution's quality on the altar of widespread acceptance and acclaim. Sometimes, the clarity of an objectively better solution is more beneficial long-term than is an alternative solution, reached by compromise, that is more palatable at the time; if a researcher finds that the earth rotates around the sun, it is better to say so, than try to compromise to gain acceptance for the discovery.

In any event, it is highly unlikely that a researcher, applying this method or any other method, will be able to find a solution that meets all the interests of all the relevant parties. Thus, widespread acceptance may not always be an option; to quote a musical genius, "after all is said and done, you can't go pleasing everyone".[71]

---

[71] JOHN LENNON, I'M STEPPING OUT (1984).

To conclude, finding a solution that is palatable to all the relevant parties is a desirable, but not essential, goal – a non-fundamental constraint – for most research tasks.

5.2. Effective Protection of Privacy is Dependent on a Widespread Understanding of the Right of Privacy

As was discussed above, in the context of Olivecrona's red light/green light approach to rights, privacy as a right suffers from a lack of public awareness. With some notable exceptions,[72] governments have done too little to promote privacy. Furthermore, privacy advocates typically do not have access to the necessary resources to do anything but ensure a minimum of attention being reserved for this 'ugly duckling' amongst the fundamental human rights.

In light of the low awareness of the right of privacy, I think it is beneficial that the solution contains elements that work to emphasise the right of privacy both for the data subjects and for those involved in the data handling.

5.3. Simplicity

The solution constructed in step eight ought to be expressible in the simplest language possible. The truth is that, the simpler language that can be used to accurately describe a solution, the better. Researchers can perhaps seek inspiration in the manner in which great scientists such as Galileo Galilei managed to explain complex matters by use of simple examples.

Indeed, for law more than any other science, simple language is of the essence; otherwise, it may not be realistic to expect people to be able to abide by the law.

Having said that, it may of course not always be possible to construct solutions that can be expressed in simple language. Indeed, some areas of law are so complex that any attempt at expressing a solution in simple language will inevitably lead to a loss of accuracy and precision in how the solution is to be applied.

5.4. One Rule to Fit All

While the parties engaging in cross-border data transfers are diverse indeed, it is desirable that the solution constructed in step eight can be suitably applied to all persons equally. I am not here talking about the necessity of avoiding discriminatory rules. Rather, I refer to the applicability of the solution to various kinds of persons such as natural persons (e.g. consumers), legal persons (e.g. businesses and other organisations) and governments.

Thus, for example, where a solution can be constructed in such a manner that it can apply to the conduct of both individuals, organisations and governments, that approach is preferable to the solution being constructed to include separate rules for each of those types of actors. But once again, reality and practicality may stand in the way of such a drafting style, and the research will in many cases be forced to devise separate rules for separate kinds of persons.

Furthermore, some scholars convincingly express a preference for sectoral data protection regulation.[73]

---

[72] Such as, for example, the proactive approach taken on several occasions by the Canadian Privacy Commissioner, Jennifer Stoddart.

[73] Schartum, *supra* note 15, at 12-14.

6. Step Four – Assessing How the Constraints Interact

Typically, steps two and three will identify some constraints that clash with each other. Where that is the case, the researcher must evaluate how serious the clashes are. In a worst case scenario, step four may illustrate that two fundamental constraints clash so directly and to such a degree as to make it impossible to construct a solution. In such a case, the researcher may take some comfort in having discovered that at a relatively early stage, and may seek to reformulate the research question so as to eliminate one of those fundamental constraints.

In most cases, however, step four will not lead to such a disappointing conclusion. Rather, most clashes will be such that the researcher will need to balance two competing constraints. Therefore, in a sense, step four is the researcher's chance to identify what aspects of the project are going to require particularly delicate attention.

Step four may also show that a fundamental constraint clashes with a non-fundamental constraint, thereby putting the researcher on notice that she/he may not be able to take account of the non-fundamental constraint.

In addition, the assessment of how the constraints interact will not only highlight clashes of constraints. It will also show instances where several constraints are in conformity, and, thus, strengthen each other.

For the research task of constructing a set of principles that regulate cross-border data flows on the Internet, I have found one instance of constraints strengthening each other, and, two clashes that require attention. I will start by discussing the two clashes individually, and then address the instance where constraints strengthen each other.

6.1. Privacy vs. Freedom of Expression

Perhaps the most interesting and important clash of fundamental constraints is that between the right of freedom of expression and the right of privacy.

As this project is restricted to the regulation of cross-border data, it would seem that the right of privacy trumps the right of freedom of expression for our purposes. First, for a signatory to comply with its obligations under Article 17 of the ICCPR, it needs to protect all individuals *within its territory and subject to its jurisdiction* regardless of whether the attack is a domestic one, or one originating overseas. In contrast, it is possible to suggest that there is no suggestion that a state would not comply with Article 19 unless it allows for cross-border communications – arguably, a state ensures its compliance with Article 19 as long as all individuals *within its territory and subject to its jurisdiction* have a freedom of expression within its territory and jurisdiction.

Thus, it is clear that the right of protection against privacy invasions, regardless of the geographical origins of the invasions, is more clearly and solidly a part of international human rights law, than is the right of free expression across borders.

In any case, it is immediately clear to the reader of ICCPR Article 19, that this right is not absolute. However, while it is clear that one person's right of freedom of expression may be restricted by reference to the protection of other peoples' right of reputation, no specific reference is made to such restrictions based on the protection of other peoples' right of privacy. This may be thought of as being odd when one considers that the right of privacy, like the right of reputation, is established in Article 17 of the ICCPR.

As odd as this may seem, the negative implications of this peculiarity are mitigated by the broad reference to the "rights of others". As will be recalled, Article 19(3) makes clear that the freedom of expression may be restricted by necessary laws for the respect of rights of others:

> The permissible limitations of protection of 'rights of others' is a catch all limitation, and is potentially very broad. The HRC [Human Rights Committee] has never commented on its outer limits. It is hoped that 'rights' refers to other human rights, though not necessarily those in the ICCPR.[74]

Thus, in light of this interpretation, the clash between the right of freedom of expression and the right of privacy is an example of what we can call a *solvable*, or *illusory*, clash – a solution can be found that caters for both needs as neither constraint is absolute.

6.2. Loss of Control vs. the Needs of Modern Society and the Structure of Relevant Technologies

There is also a clash between, on the one hand, the fundamental constraint that there is a loss of control where data crosses borders, and, on the other hand, the fundamental constraints that cross-border data transfers are required by modern society and that not all technologies are sensitive to data crossing borders.

This clash is, of course, significantly affected by, or indeed dependent on, another fundamental constraint; namely the fact that some of the data that necessarily crosses borders for the proper function of Internet communication is personal in nature.

What we find in this is an example of an *unsolvable* clash – a solution cannot be found that caters for both needs in their entirety. Whenever a researcher comes across such a situation, she/he must assess whether the fundamental constraints in question can be balanced against each other in a manner that allows for each of them to be met to a sufficient degree.

Fortunately, the unsolvable clash present here, can be addressed by a balancing of the clashing fundamental constraints in such a manner that each constraint is catered for to a sufficient degree. The solution lies in allowing cross-border transfers, but at the same time placing some restrictions on the circumstances under which such transfers can take place, and possibly also restrict the types of data that can be transferred (i.e. treating different types of personal data differently).

The difficulty with unsolvable clashes is that the researcher must constantly be aware that in catering for one constraint, she/he is at the same time undermining the other, competing, constraint.

6.3. The Relationship between Simplicity, One Rule to Fit All, Technological Neutrality, and a Widespread Understanding of the Right of Privacy

Above I have made observations as to clashes between some of the constraints identified in steps three and four. However, instances can also be found of various constraints emphasising and amplifying each other. For example, there is a clear correlation between privacy rules being expressed in simple language and a widespread understanding of the right of privacy being created.

Furthermore, a technology neutral rule, applicable to all different types of parties being regulated, is more likely to be sufficiently simple, than is a set of technology-specific rules, or a set of different rules for different types of parties.

---

[74] JOSEPH ET AL., *supra* note 42, at 541.

7. Step Five – Examining How the Problem Has Been Addressed So Far

Possibly the easiest manner in which a researcher can find a solution to a regulatory problem is to examine how the issue in question is currently regulated, and to examine how the problem has been treated, to date, in academic discourse. Of course, for that to be possible, there must necessarily be some existing attempts at addressing, or at least discussing, the problem.[75] In the fast-moving discipline of Internet law, that is not always the case. Yet, in the absolute majority of cases, it is likely that some relevant materials can be found:

> The beginner often jumps to the conclusion that a foreign system has 'nothing to report' on a particular problem. The principle of functionality applies here. Even experienced comparatists sometimes look for the rule they want only in the particular place in the foreign system where their experience of their own system leads them to expect it: they are unconsciously looking at the problem with the eyes of their own system. If one's comparative researches seem to be leading to the conclusion that the foreign system has 'nothing to report' one must rethink the original question and purge it of all the dogmatic accretions of one's own system. . . . It is only when one has roamed through the entire foreign system without avail, asking a local lawyer as a last resort, that one can safely conclude that it really does not have a solution to the problem. This hardly ever happens[.][76]

Where a researcher cannot find, or cannot access[77], any existing attempts at addressing or discussing the research task, she/he will have to skip step five and move directly to step six. However, for most research projects, step five may constitute the most time consuming of the ten steps. And this step may itself present a solution, or even a list of possible solutions, to the problem identified in step one.

Step five is guided by one simple truth – the greater the number of sources taken account of, and the greater the level of detail with which the researcher studies those sources, the greater is the likelihood of step five providing useful materials for the researcher's solution. In other words, the researcher should seek to take account of as many sources as possible, and should study those sources at as great detail as possible.

So what sources should be studied? The answer to that question will inevitably depend, at least in part, on the nature of the research task. Nevertheless, the researcher should consider whether useful information may be gained from any of the following sources:

- International instruments;
- Customary international law;
- National and super-national laws;
- Publications, and other statements, by relevant organisations; and
- Academic discourse.

At the same time, in choosing the sources to be studied, the researcher must be realistic, taking account of time constraints, language limitations and accessibility to relevant materials.

---

[75] I am here talking about specific attempts at regulating the issue in question. This is quite different to the fact that, all legal systems will, one way or another, resolve legal conundrums when asked to do so; be as it may that it may have to resort to legal principles of great generality.

[76] ZWEIGERT & KÖTZ, *supra* note 7, at 35.

[77] As all researchers are limited in the materials they can access and digest, for example due to certain material not being accessible where the researcher is located or not being accessible in a language the researcher can work with, there will be unfortunate instances where a researcher is aware of relevant materials but simply cannot use them. Where that is the case, the researcher may need to seriously consider whether she/he should proceed anyhow, seek external assistance, or perhaps simply abandon the project.

A related question is how the researcher should approach the materials she/he can collect for the purpose of step five. In other words, does step five require the researcher to examine each of the sources of information systematically, or can the researcher "pick and chose" what aspects of each of the sources she/he will focus on? The answer to this question may in part be guided by the research task. Further, the answer may be influences by matters such as time constraints, or indeed, word limitations imposed by the publisher of the anticipated research output. In the end, it is a personal choice that each researcher is faced with. And yet again, the warning bells of subjectivity ring.

In relation to some research tasks it may be seen as careless, or even unprofessional, to adopt anything but a systematic approach to the materials collected for the purpose of step five. In other contexts, a systematic approach may be unnecessarily cumbersome and distract from the real research task by making the writing excessively descriptive. The most important considerations is that, by including step five, anyone wanting to draw upon, or otherwise use, the researcher's output can assess the validity of the research findings by reference to how the researcher dealt with the materials gathered for step five. This *research transparency* is of great importance.

For the purpose of the research task I have opted to undertake in this article, I commence by examining the impact of the Organisation for Economic Co-operation and Development 1980 Guidelines on the field of study, followed by the relevant work of the Asia-Pacific Economic Cooperation. I then examine some of the relevant parts of the law of three different jurisdictions; namely Australia, the European Union, and the United States of America. Finally, I make some observations as to what is revealed in this field in academic discourse. All of these sources are studied in a more or less eclectic manner, and particular emphasis is placed on the EU approach and that taken in Australia.

7.1. The Organisation for Economic Co-operation and Development

The Organisation for Economic Co-operation and Development (OECD) has played a major role in the development of the regulation of privacy in general, and cross-border data transfers in particular. The 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* concerning the collection and management of personal information have been highly influential and crucial in the developments to date.

Those Guidelines, developed by a group of government experts chaired by The Hon. Mr. Justice Kirby, "represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it."[78]

[78] OECD, *supra* note 48, at Preface.

Part Three of the Guidelines provides basic principles regarding free data flows and legitimate restrictions on such data flows:

> 15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
>
> 16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.
>
> 17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
>
> 18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.[79]

7.2. The Asia-Pacific Economic Cooperation

Asia-Pacific Economic Cooperation (APEC) was established in 1989. It has as its goal to facilitate "economic growth, cooperation, trade and investment in the Asia-Pacific region."[80] APEC's 21 members[81] include, for example, Australia, Canada, the People's Republic of China, Japan, Malaysia, the Russian Federation, Singapore and the United States of America.

In 2004, APEC Ministers endorsed the APEC Privacy Framework.[82] The Framework is intended "to provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted."[83]

Principle IX regulates cross-border data flows:

> A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

---

79 *Id.* at Part Three.

80 APEC, *About APEC*, Jan. 14, 2009, http://www.apec.org/apec/about_apec.html (last visited Apr. 12, 2010).

81 Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Republic of the Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America; Viet Nam.

82 APEC, *supra* note 48. For a more detailed discussion of the APEC framework, *see* Carla Bulford, *Between East and West: The APEC Privacy Framework and the Balance of International Data Flows*, 3 ISJLP 705 (2007-2008).

83 APEC, supra note 48.

The commentary attached to the relevant principle is illustrative of the manner in which this Principle is intended to operate:

> Efficient and cost effective business models often require information transfers between different types of organizations in different locations with varying relationships. When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, information controllers should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between the personal information controller and the third party to whom the information is disclosed. In these types of circumstances, personal information controllers may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these
>
> Principles. However, in cases where disclosures are required by domestic law, the personal information controller would be relieved of any due diligence or consent obligations.[84]

Interestingly, the APEC privacy work recently developed further with the launch of its new Cross-border Data Privacy Initiative focused on information sharing and cooperation between data protection authorities in the APEC region and beyond.[85]

7.3. The European Union

The primary privacy regulation in the European Union (EU) stems from 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.[86] Chapter IV of that Directive regulates the transfer of personal data to third countries. Importantly, Article 25(1) states that:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

Article 26(1) and (2) provides exceptions to this main rule:

> 1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
>
> (a) the data subject has given his consent unambiguously to the proposed transfer; or
>
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
>
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

---

84 Id. at ¶ 26.

85 *See* News Release, APEC Secretariat, APEC launches new Cross-border Data Privacy Initiative (Jul. 16, 2010), *available at* http://www.apec.org/apec/news___media/media_releases/20100716_ecsg_cpea.html (last visited Aug. 23, 2010). For more details, *see* APEC, *APEC Cross-border Privacy Enforcement Arrangement (CPEA)*, http://www.apec.org/apec/news___media/fact_sheets/201006cpea.html (last visited Aug. 31, 2010).

86 1995 O.J. (L 281) 31.

> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
>
> (e) the transfer is necessary in order to protect the vital interests of the data subject; or
>
> (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
>
> 2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.
>
> 3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

One of the most interesting cases relating to these provisions is the Swedish *Lindqvist* case.[87] There, a woman – Bodil Lindqvist – uploaded a website on which she made available personal information about herself and her husband, as well as personal information relating to a number of her colleagues in the church community she worked for.

The website, which was published without the permission of her colleagues, generated some complaints and the matter ended up in court. The legal proceedings related to a range of matters. Interestingly, one of them was whether Lindqvist's conduct meant she had transferred the data in question to a third country. Göta Hovrätt stayed the proceedings and referred seven questions to the European Court of Justice (ECJ). Question five asked the ECJ to address the 'transfer' issue:

> [Directive 95/46] prohibits the transfer of personal data to third countries in certain cases. If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden - with the result that personal data become accessible to people in third countries - does that constitute a transfer of data to a third country within the meaning of the directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?[88]

The Court answered this question in the negative.[89] However, it is interesting to examine how the Court reached that conclusion.

Having noted that "it is necessary to take account both of the technical nature of the operations thus carried out and of the purpose and structure of Chapter IV of that directive where Article 25 appears,"[90] the Court made some observations as to the relevant technical setup:

> It appears from the court file that, in order to obtain the information appearing on the internet pages on which Mrs Lindqvist had included information about her colleagues, an internet user would not only have to connect to the internet but also personally carry out the necessary actions to consult those pages. In other words, Mrs Lindqvist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access to those pages.

---

87 I have discussed this case in more detail elsewhere, and the description provided here draws upon Dan Svantesson, *Privacy, the Internet and Transborder Data Flow – An Australian Perspective*, CYBERSPACE 2009: NORMATIVE FRAMEWORK (November 2009), Brno Czech Rep.

88 Case C-101/01, Criminal Proceedings against Bodil Lindvist, ¶ 18, Nov. 6, 2003, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET (last visited Nov. 24, 2009).

89 *Id.*

90 *Id.* at ¶ 57.

> It follows that, in circumstances such as those in the case in the main proceedings, personal data which appear on the computer of a person in a third country, coming from a person who has loaded them onto an internet site, were not directly transferred between those two people but through the computer infrastructure of the hosting provider where the page is stored.[91]

While it is true that Lindqvist could not transfer the content of her website to an Internet user that was not connected to the Internet at the time, or who did not wish to take the steps necessary to visit her website, that is no different to the fact that a TV station cannot provide TV programs to somebody who does not turn on their TV, or who does not chose the TV station's particular channel.[92] Consequently, the Court's justification of their approach, by reference to the relevant technology, is weak indeed.

The Court then turned to the purpose of the relevant part of the Directive:

> Chapter IV of Directive 95/46 contains no provision concerning use of the internet. In particular, it does not lay down criteria for deciding whether operations carried out by hosting providers should be deemed to occur in the place of establishment of the service or at its business address or in the place where the computer or computers constituting the service's infrastructure are located.
>
> Given, first, the state of development of the internet at the time Directive 95/46 was drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression 'transfer [of data] to a third country' to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.[93]

This conclusion is somewhat surprising. The fact that the Directive does not make specific mention of the Internet, suggests that it is drafted in technology-neutral language. Where that is the case, it cannot be assumed that the drafters did not intend the Directive to apply to Internet related activities such as in the *Lindqvist* case. Rather, the technology-neutral language suggests that the application of the Directive should not be dependent on the technology in question. The Court's conclusion is perhaps even more extraordinary when one considers that the Internet was in use (albeit on a different scale) at the time the Directive was drafted. Consequently, had the drafters wanted to exclude Internet activities, they would presumably have made that clear.

The third justification the Court presented for their conclusion is more interesting:

> If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.[94]

---

91 *Id.* at ¶ 60-61.

92 A technical difference exists in that the TV station in my example is actively sending a signal that can be picked up in another country. However, unless someone picks up the signal, there simply is no transfer of data.

93 *Criminal Proceedings against Bodil Lindvist*, at ¶ 67-68.

94 *Id.* at ¶ 69.

This argument is much harder, if not impossible, to dismiss, and it shows a type of thinking that is far too rare amongst courts having to address legal issues associated with rapidly developing technologies. Instead of merely applying the law to the situation at hand, the Court made an assessment of the likely consequences of finding that Lindqvist's conduct amounted to a transfer. In other words, while it may be difficult to argue that Lindqvist's conduct did not amount to a transfer, the consequences of reaching such a finding would be devastating for the technology in question – a reasonableness test was applied.

Finally, for the European context, it is also interesting to note how data protection *per se* now is recognised as a human right in the EU.[95] This strong stance can no doubt serve as an explanation, as well as justification, for the EU relatively heavy-handed approach to data protection in general, and transborder data flows in particular.

7.4. The United States of America

The regulation of privacy in the US is made up of a complex web of federal and state law, stemming from case law and legislation. However, one characteristic feature of the approach taken by the US towards privacy is that it is heavily influenced by the Clinton administration's preference for self-regulation, and it is this feature I will focus on briefly here.[96]

Rubinstein distinguishes between three components of self-regulation:

> Privacy self-regulation generally involves a trade association or group of firms establishing a set of substantive rules concerning the collection, use and transfer of personal information along with procedures for applying these rules to member firms. More specifically, the self-regulatory model has three components: (1) an industry group issuing guidelines or a code of conduct governing members' privacy practices; (2) enforcement by the industry group, or perhaps a dispute resolution mechanism administered by an independent third party, but no enforceable legal remedies (other than the FTC's inherent power to prosecute firms for unfair and deceptive trade practices, including misrepresentation of their privacy policies); and (3) procedural rules related to amending existing guidelines and related internal matters.[97]

Having done so, Rubinstein concludes that:

> The opposing sides in the privacy debate tend to treat self-regulation and government regulation as if they were mutually exclusive options from which policy makers have to choose, either one or the other. But this is short-sighted. […] it is better to think of "pure" self-regulation and "strict" command-and-control regulation as opposing ends of a regulatory continuum, with most regulatory schemes falling somewhere in the middle.[98]

The US/EU 'safe harbour' arrangement[99] has gained considerable attention[100], but it will not be discussed separately here. It suffices to note that, essentially, US organisations are afforded the option of joining the safe harbour arrangement so as to be deemed to provide an adequate protection of privacy, thereby meeting the EU standard.

---

95 Article 29 Data Protection Working Party, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, at 9, WP 168 (adopted on Dec. 1, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

96 Ira S. Rubinstein, *Privacy, Self-regulation and Statutory Safe Harbors*, 4, http://www.law.nyu.edu/ecm_dlv3/groups/public/@nyu_law_website__centers__information_law_institute/documents/documents/ecm_pro_063460.pdf?q=2008-nai-principles (last visited Sep. 1, 2010).

97 *Id.* at 2.

98 *Id.*

99 *See* EXPORT.GOV, http://www.export.gov/safeharbor/ (last visited May. 6, 2010).

100 *See, e.g.*, Robert Bond, *International Transfers of Personal Data – An Update*, 5 BUS. L. INT'L 423 (2004).

7.5. Australia

Australia is a particularly interesting jurisdiction to include in the study. The reason is that Australian privacy law is currently undergoing a fundamental makeover. After extensive consultation, the Australian Law Reform Commission presented its findings regarding privacy regulation in May 2008. The 2,694 page document outlined 295 recommendations. The Australian Government is currently working its way through those recommendations. At the time of writing, the Government has released its response to 197 of the recommendations.[101]

In this tumultuous time, Australian privacy law on cross-border data flows provides both an example of inadequate regulation (the current scheme) and misguided regulation (the proposed scheme – i.e. the Governments proposed implementation of the relevant ALRC recommendations).[102]

To see what restrictions Australia's current scheme places on cross-border data flows on the Internet, we have to look at the *Privacy Act 1988* (Cth), and more specifically at National Privacy Principle (NPP) number nine:

> NPP 9
>
> An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:
>
> (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or
>
> (b) the individual consents to the transfer; or
>
> (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
>
> (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
>
> (e) all of the following apply:
>
> (i) the transfer is for the benefit of the individual;
>
> (ii) it is impracticable to obtain the consent of the individual to that transfer;
>
> (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
>
> (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

Interestingly, there is an almost complete lack of decisions dealing with this provision.

---

[101] In its response, the Government is accepting 141 of the recommendations, either in full or in principle, and is accepting another 34 with qualifications. The responses to the remaining 98 recommendations – many of which are crucial for the overall operation of the regulatory system – will be presented during the second stage of the process.

[102] My reasons for viewing the current scheme as being inadequate, and the proposed scheme as being misguided, are elaborated on below.

One of the ALRC's recommendations that has been considered, and that has been adopted with amendments, is Recommendation 31-2 which relates to transborder data flow. Guided by that recommendation, the Australian Government is proposing to regulate such matters in the following manner:

> Australian Privacy Principle 8—cross-border disclosure of personal information
>
> (1) Before an entity discloses personal information about an individual to a person (the overseas recipient):
>
> (a) who is not in Australia; and
>
> (b) who is not the entity or the individual;
>
> the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.
>
> (2) Subsection (1) does not apply to the disclosure of personal information about an individual (the affected individual) by an entity to the overseas recipient if:
>
> (a) the entity reasonably believes that:
>
> (i) the overseas recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least
>
> substantially similar to the way in which the Australian Privacy Principles protect the information; and
>
> (ii) there are mechanisms that the affected individual can access to take action to enforce that protection of the law or binding scheme; or
>
> (b) both of the following apply:
>
> (i) the entity expressly informs the affected individual that if he or she consents to the disclosure of the information, subsection (1) will not apply to the disclosure;
>
> (ii) after being so informed, the affected individual consents to the disclosure; or
>
> (c) the disclosure of the information is required or authorised by or under an Australian law, or an order of a court or tribunal; or
>
> (d) each of the following applies:
>
> (i) the entity is an agency;
>
> (ii) the disclosure of the information is required or authorised by or under an international agreement relating to information sharing;
>
> (iii) Australia is a party to the international agreement; or
>
> (e) both of the following apply:
>
> (i) the entity reasonably believes that the disclosure of the information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to
>
> public health or safety;
>
> (ii) it is unreasonable or impracticable to obtain the affected individual's consent to the disclosure; or
>
> (f) both of the following apply:
>
> (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may
>
> be engaged in;
>
> (ii) the entity reasonably believes that the disclosure of the information is necessary for the entity to take appropriate action in relation to the matter; or
>
> (g) each of the following applies:
>
> (i) the entity is an agency;

(ii) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities by, or on behalf of, an

enforcement body;

(iii) the overseas recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body; or

(h) both of the following apply:

(i) the entity is an agency;

(ii) the entity reasonably believes that the disclosure of the information is necessary for the entity's diplomatic or consular functions or activities; or

(i) the entity is the Defence Force and the entity reasonably believes that the disclosure of the information is necessary for any of the following occurring outside Australia:

(i) war or warlike operations;

(ii) peacekeeping or peace enforcement;

(iii) civil aid, humanitarian assistance, medical or civil emergency or disaster relief.

As it has not yet been implemented, there are of course no decisions that can help us understand how this provision will be applied in practice.

7.6. Academic Discourse

Some scholarly works, such as Blume's excellent book *Retlig Regulering af Internationale Persondataoverførsler*[103], deal with the problems associated with transborder data flows in great detail. However, here, I will focus on a few select works addressing specific issues of particular interest.

While discussing online privacy in general, Wafa identifies three major schools of thought that encompass the debate on what the future of online privacy should look like:

> One view, which espouses "top-down regulation," favors stringent regulatory oversight and would require companies to follow a well-defined minimal standard of privacy. The closest real-world example of such a system would be the privacy framework put forth by the European Union, which emphasizes government participation in regulating online privacy. A second view discourages mandated enforcement of any privacy protection. Supporters of this view are: (1) authoritarian and despotic governments, (2) individuals/groups who view government and corporate entities as untrustworthy, and (3) free-market ("laissez-faire") capitalists who believe the market should be left to its own devices. A third view advocates for industry self-regulation on grounds that companies in control of technology are in a better position than government actors to create privacy rules, implement compliance monitoring, and manage enforcement. Proponents of this view can be seen as straddling the other two views, since they do not necessarily want weak consumer protection, but also resist top-down regulation and enforcement.[104]

Another valuable part of Wafa's work is found towards the end of the article where he identifies three features that systems regulating privacy should have: "Finding a viable solution that balances efficiency concerns while still ensuring privacy and respecting cultural sensitivities is no easy task, but there are several important features that a successful system should contain. These include, (1) top-down regulation, (2) aggressive enforcement, and (3) innovative auditing procedures."[105]

---

[103] BLUME, *supra* note 47.

[104] Tim Wafa, *Global Internet Privacy Rights: A Pragmatic Approach*, 13 INTELL. PROP. L. BULL. 131, 150 (2008-2009) (internal footnotes omitted).

[105] *Id.* at 154.

Also Bulford has sketched some general features necessary for the success of any regulatory scheme in this field:

> Legislation grounded in common principles provides a predictable and stable business environment, which benefits both industry and individuals. Corporations that deal in personal, non-public information can tailor their internal policies around the same principles that will control new policy, and will benefit from increased consumer confidence. Predictability reduces compliance concerns and streamlines the legislative process by setting uniform parameters for legislative activity. Consumers benefit from a framework that places informed consent at the center of every policy decision, because it encourages accurate disclosure from companies that manipulate consumer data.[106]

In an article published in 2006, Gunasekara outlines several interesting approaches to the regulation of cross-border data flows.[107] The first is focused on contract law, with transfers being allowed where there are adequate contractual guarantees protecting the data subjects privacy rights. The most interesting part of that discussion is how Gunasekara proposed to overcome the difficulties created by the common law doctrine of privity. Privity of contracts essentially means that only the parties to the contract can take action under the contract. The consequence, in the context of cross-border data transfers, is obvious; the data subject cannot take action against a recipient of data where the recipient does not comply with the contract entered into with the party that provided the data. Gunasekara's interesting solution to this problem is as follows:

> One option in developing a 'fourth generation' of privacy principles may be to allow national data protection authorities the power to enforce contractual stipulations or deem contravention of them to be a breach of privacy rules. Some jurisdictions already have provisions of this nature. Another might be to require registration of such contractual clauses so that subsequent purchasers are put on notice, actual or constructive, as to the data subject's rights. It should be possible to attach a symbol such as the '©' symbol for copyright or abbreviations used in commerce such as 'cif', and the like. Perhaps the 'p' symbol might delineate the fact that standard privacy rights are covenanted in relation to information concerning the subject. Another requirement should be that the initial 'privacy statement' given to an individual be attached to any subsequent transfer of the data: third parties will then be unable to claim that they received the information in ignorance of its intended uses and recipients.[108]

Another of Gunasekara's approaches is termed "Corporate Law Solution". One of the aspects of this approach is focused on auditing and reporting requirements:

> Special audit arrangements should be set up with regard to the transfer of information across borders. In this regard, analogies may be drawn with existing models where more stringent safeguards exist. For instance, it has been observed that, in the UK, the procedures mandated by the Financial Services Regulator significantly exceed those of the data protection authority. These require, amongst other things, that the adequacy assessments are carried out, documented and retained for inspection by all financial services organizations. If adopted, such a paradigm may represent a half-way house between the approach of some data protection authorities that carry out a prior approval process before sanctioning personal data exports, and others that carry out monitoring after the exports have occurred. Audits should also be carried out of the adequacy of standard contractual clauses—once again this is a task that can properly be entrusted to private sector specialists, such as law firms.

---

[106] Bulford, *supra* note 84, at 722.

[107] Gunasekara, *supra* note 8.

[108] *Id.* at 387 (footnote omitted).

> Companies also have periodic reporting obligations. Not only must they report to registry offices but reports must from time to time be compiled in compliance with health and safety, and a myriad other regulations. Compliance with data protection rules ought to be subject to similar reporting obligations. In this regard, the onus is on national data protection authorities to formulate simple yet functional forms (most forms can be downloaded through the internet nowadays) that data controllers must return at least annually.[109]

The last approach discussed by Gunasekara stems from the observation that:

> In principle, there is no reason why binding international treaties cannot be adopted in relation to the protection of information privacy. Intellectual property has witnessed such treatment and there is much in common, as personal information, like all information, shares characteristics including the ease of copying and transmission.[110]

In light of this, Gunasekara suggest that: "One option would be for an international privacy regime that would apply in the absence of 'substantially similar' domestic legislation. Conceivably an 'International Privacy Commissioner' may be set up."[111]

Support for an international harmonisation of privacy regulation is widespread. For example, Wafa notes that:

> Technologists and business leaders have long disapproved of a fragmented privacy law framework and worried that inability to comply with multiple standards would hinder the capacity of the Internet to attract consumers. These critics share a basic desire to convince lawmakers and enforcement agencies around the globe to coalesce around uniform standards.[112]

At the same time, as has been discussed in detail e.g. by Kuner, the difficulties associated with international harmonisation should not be underestimated.[113]

Turning to the reception academics have given to the two very different approaches taken by the EU and APEC, it is no surprise that the views are divided. Equally predictably, with some notable exceptions, the dividing line seems to be drawn somewhere in the Atlantic. Some commentators view the European Court of Justice's decision in the *Lindqvist* case as "draconian and abusive"[114] and see the EU approach as "heavy-handed centralized legislation"[115]. They suggest that the better approach is to focus on whether any damage has actually been caused:

> An action such as this [i.e. the Lindqvist case] would be highly unlikely in the United States without at least the perception of harm by some party. In the United States, the party perceiving harm would seek to remedy that harm, generally as an individual with an equity or tort claim.[116]

---

[109] *Id.* at 389-390 (footnote omitted).

[110] *Id.* at 392 (footnote omitted).

[111] *Id.* at 391.

[112] Wafa, *supra* note 106, at 144-145.

[113] Christopher Kuner, *An International Legal Framework for Data Protection: Issues and Prospects*, 25 COMPUTER L. & SECURITY REVIEW 307 (2009).

[114] F. J. Garcia, *Bodil Lidnqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators*, Vol. XV FORDHAM INTELLECTUAL PROPERTY, MEDIA & ENTERTAINMENT LAW JOURNAL 1233 (2005).

[115] *Id.*

[116] *Id.*, 1229.

Others criticise the EU approach for its inevitable extraterritorial effect, noting, for example, that the EU Privacy Directive, as a regulatory scheme "has a far reaching and significant impact beyond the borders of the regulating entity."[117] Bauchner concludes that:

> [T]he point at which a third country has exercised its own right to legislate within the privacy sphere represents the point at which the Directive must cease to control, The problem is that at this rather penumbral barrier a polarized conflict of interests arises between various states.[118] (internal footnotes omitted)

In response to this sort of concerns, the EU has responded as follows:

> There is no desire to "export" the EU system to other countries. There are clearly different ways of arriving at the same results, but we need to ensure that the personal data of EU citizens transferred outside the EU is being processed with due respect for certain widely accepted principles, that citizens can enforce their rights and that they are entitled to redress if they suffer damage as a result of a breach of these principles. We are conscious of the need to avoid procedures for blocking data transfers which are exclusively unilateral. Non-EU countries concerned need to be informed and given the chance to express their views.[119]

Surprising to no one, criticism has also been raised against the APEC framework,[120] and commentators have expressed strong concerns about the effect the APEC framework may have on the regulation of major Internet companies. For example Wafa concludes that:

> Google's push for global regulators to adopt the APEC framework should be of great concern to the general public. By taking advantage of its huge user base and functional superiority, Google could easily undermine the rights of users by (1) deceptively portraying themselves as privacy advocates; (2) taking advantage of this image to slowly and methodically monetize and exploit increasing amounts of customer data; and (3) push for a purely self-regulated global framework (like APEC) which would facilitate their ability to exploit vague language in order to operate in a regulatory vacuum.[121]

8. Step Six – Examining How Similar Problems Have Been Addressed So Far

As mentioned above, researchers in a dynamic field like Internet law may find that the problem they are seeking to address has never been addressed before. Indeed, as noted in the introduction, the law typically lags behind the developments of technology, and, thus, such situations are not rare. Where that is the case, researchers may be unable to gain any knowledge from step five.

Suppose now that one is not satisfied by this. What options remain then? Fortunately, regardless of how novel the research question itself is, it is fruitful to consider how similar problems have been addressed, if some sufficiently similar problem can be identified. That is not to suggest that step six is to be treated as an alternative to step five. Wherever possible, the researcher should apply both step five and step six.

---

[117] Bauchner, *supra* note 6, at 696.

[118] *Id.* at 707.

[119] E.U. Commission Directorate General 15, *Data Protection: Background Information* (Nov. 3, 1998), http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/background-info_en.htm (last visited May. 6, 2010).

[120] *See, e.g.*, Chris Pounder, *Why the APEC Privacy Framework is Unlikely to Protect Privacy*, OUT-LAW.COM, Oct. 15, 2007, http://www.out-law.com/page-8550 (last visited May. 6, 2010); Graham Greenleaf, *Five years of the APEC Privacy Framework: Failure or Promise?*, 25/1 COMPUTER LAW AND SECURITY REVIEW 28 (2009).

[121] Wafa, *supra* note 106, at 153.

The obvious question of method is then how one determines what problems are similar enough to be considered, and which are not. As can be expected, there is no simple answer to that question. The most that can be said is that, it may be better to cast the net widely and then be selective in what aspects of the findings one takes account of, than to be too limiting in what is considered similar enough to be relevant.

For the research task of constructing a set of principles that regulate cross-border data flows on the Internet, I was, however, unable to identify a sufficiently similar problem,[122] and thus, step six does not assist me in this research task.

9. Step Seven – Critically Evaluating the Approaches Identified in Steps Five and Six

Steps five to seven all have somewhat of a comparative law flavour. Yet, these steps are not amounting to comparative law in its narrow sense. Strictly speaking, the aim is not to compare different legal approaches, but rather to identify valuable solutions or components that can be used for such solutions.

Having said that, it can be expected that researchers with a background in comparative law will feel more at home with steps five to seven, than will other researchers. This is not least so due to the fact that approaching a foreign legal system always involves a rather steep learning curve.

In performing the critical evaluation that is step seven, the researcher must examine the approaches identified in steps five and six, both as systems and as individual components making up those systems. In other words, the approaches should first be looked at as the interesting creations they are, and then the researcher should look at the individual building blocks that make up the systems. If it is concluded that one of the systems identified meets all the fundamental constraints and is, in all other respects, an ideal solution, step eight will merely involve the imitation of the approach found in step five. However, it is perhaps more likely that the researcher is not so lucky as to find a ready-made solution to the problem defined in step one. In such situations, the researcher will do well to look closely at the benefits and disadvantages of the individual building blocks that make up the systems studied in step five, and assess whether they can be combined and assembled in a different manner to meet the requirements of the fundamental constraints.

A few words should also be said about how one ought to structure one's work in step seven. While there is not necessarily a right and a wrong way of doing this, it may be advisable to first dispose of any unrealistic and unhelpful approaches, and then focus on those approaches that are likely to contribute to the solution devised in step eight. For example, below I start by disposing of the self-regulation model as it is obvious that it does not fit within the fundamental constraints identified in step two.

Looking at what was revealed through the application of step five to the research task of constructing a set of principles that regulate cross-border data flows on the Internet, several approaches, and components of approaches, need to be evaluated.

---

[122] There are, of course, other areas of regulation that share some similarities with the regulatory task at hand. For example, the regulation of defamation involves a balancing of two fundamental human rights, not entirely dissimilar to that I am faced with here. Further, many, not to say most, countries restrict the cross-border flow of state secrets which, in a very broad sense, is similar to the goal of restricting the cross-border flow of personal information. However, both of these areas of regulation are so fundamentally different to what I am dealing with that no sensible conclusions could be drawn from how the law operates in those areas.

9.1. Self-Regulation

Of all the options identified through steps seven and eight, the only approach that can be dismissed *a priori* is the US' approach of self-regulation. This approach has been the subject of extensive criticism by several distinguished commentators, and the criticism is well summarised by Rubinstein:

> According to its many critics, privacy self-regulation is a failure. It suffers from weak or incomplete realization of Fair Information Practice Principles, inadequate incentives to ensure wide scale industry participation, ineffective compliance and enforcement mechanisms, and an overall lack of transparency.[123]

Looking at the Safe Harbor arrangement as an example, Connolly has shown that:

> 2170 US companies claim to be safe harbor privileged; whereof 388 were not even registered with the Department of Commerce (DOC). Among the registered companies 181 certificates were found to be not current due to lapse of time. The check on the 7th principle concerning enforcement alone showed that 940 out of the 2170 US companies do not provide information on how to enforce individuals' rights. 314 companies provide a dispute rsolution scheme that costs between 2000 and 4000 US dollars. Thus, it is hardly surprising that not a single complaint procedure has been carried out. Despite the more than 2000 annual complaints about non-compliance with the safe harbor principles, the Federal Trade Commission (FTC) has prosecuted only seven organisations for falsely claiming safe harbor self-certification.[124]

Further, while speaking of self-regulation in general terms, Clarke has noted the following:

> I have long characterised self-regulation as the herding of the sheep by the wolves. Any benefits to the sheep are incidental. The primary beneficiaries are the wolves, through the lulling of the less aware sheep into a false sense of security, and the avoidance of actual regulation of the behaviour of the wolves, and of the provision of actual protections for the sheep.

The simple facts are that:

- there are tensions between the interests of wolves and those of sheep;
- wolves are individually powerful, and capable of acting as a pack;
- sheep are individually weak, and generally very poor at using collectivism to achieve countervailing power against threats like the wolves.

> In such circumstances, Governments have the responsibiity [sic] to impose appropriate forms of regulation on the wolves.[125]

---

[123] Rubinstein, *supra* note 98, at 1.

[124] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, *10th Anniversary of Safe Harbor – Many Reasons To Act, But None To Celebrate*, PRESSEMITTEILUNG, Jul. 23, 2010, http://www.datenschutzzentrum.de/presse/20100723-safe-harbor_en.html (last visited Aug. 23, 2010).

[125] Roger Clarke, *Submission Treasury Taskforce on Industry Self-Regulation,* Nov. 23, 1999, http://www.rogerclarke.com/EC/SubCons991123.html (last visited May. 4, 2010).

In contrast, proponents of self-regulation suggest that organisations will automatically adjust their use of personal information so as to avoid tarnishing their reputation: "the principal asset that online marketers have is their reputation with consumers, and any use of information in a way that reduces the value of those reputations is counterproductive for the firm"[126]. This thinking is not fully supported by the attitude to privacy shown by how major Internet corporations, such as *Google* and *Facebook*, approach privacy. Indeed, any fear of negative publicity due to privacy abuse or misuse would seem to be an incentive to adopt a strong degree of secrecy as to any such events.

In the end, what I want to say is this; a fear of negative publicity resulting in reputational damages is a potentially strong deterrent. However, alone it is not enough, and it needs to be backed up by legal regulation.

I agree with Clarke's arguments, and to expand on them, we can link this reasoning to the fundamental constraints identified in step two. One of the fundamental constraints identified at that step was that a solution to the research task at hand must take account of the fact that privacy is a widely recognised fundamental human right. In light of that, governments do, indeed, have a responsibility to impose appropriate forms of regulation on the 'wolves'. That responsibility is such that governments cannot be seen to have met their international obligations where they attempt to outsource the protection of a fundamental human right, such as privacy, through self-regulation.

Consequently, self-regulation, at least in the various shapes seen so far, cannot be the mechanism that gets us out of the current quagmire and lets us regain firm ground – it is not the answer to the task of constructing a set of principles that regulate cross-border data flows on the Internet.

9.2. Border Control

Both the EU's and Australia's current privacy regulations are based on border control – cross-border data flows are allowed only where they meet certain requirements. Further, the OECD Guidelines certainly contemplate border control regimes. In contrast, the approach advocated in the APEC Framework, as well as the approach opted for in the US self-regulation model, and in Australia's proposed privacy regulation, do not impose border control, or are only placing limited emphasis on such control.

Taking account of the fact that, as is made clear in the discussion of one of the fundamental constraints, data crossing borders represent a loss of control for the data subject, I conclude that some form of border control is a necessary element of any sound model for the regulation of cross-border data. At the same time, I acknowledge that the restrictions imposed by the border control must not be of such a nature as to inappropriately interfere with modern society's requirements for cross-border transfers of data, including the needs stemming from the fact that not all technologies are set up to be sensitive to data crossing borders.

Once one concludes that it is necessary to implement some form of border control, one is immediately faced with the task of identifying the circumstances in which data may be exported in line with the limitations flowing from the border control. There is a relatively great consistency between how the EU and Australia have engaged in this task. At the same time there are fundamental differences.

---

[126] Paul H. Rubin & Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*, 49-52 (2002), *cited in* Rubinstein, *supra* note 98, at 8.

Consent is a vital component in both the Australian and EU regulation. Indeed, consent is an absolutely crucial component of privacy regulations in many parts of the world. However, it is a complex concept[127], and one that would benefit from being the object of further research, both from a strictly legal perspective, and more broadly.

Unfortunately, consent is also a concept that frequently is abused and stretched to such a degree that it loses its relevance. For example, under Australia's NPP 9 (discussed above in 7.5), as is the case in relation to several of Australia's NPPs, 'consent' is treated as a miracle cure for virtually any abuse imaginable.[128] As people in general are unable to assess the risks associated with a transfer of their personal information to another country, consent given is typically not sufficiently informed - it would be naive to think that the average consumer ever could fully evaluate the legal implications of consenting to their personal information being transferred overseas. However, there can be no doubt that much more could be done to ensure that data subjects are informed about the risks involved.[129]

Making matters worse, data exporters frequently bundle consent for transfer to a third country with consent for other uses. Such bundled consent may be justifiable in some context, but never in relation to overseas transfer of personal information.

Both the EU and the Australian regulation contain several rules that overlap significantly with the consent rule. For example, in addition to allowing transborder data flows where consent has been given, NPP 9 of Australia's regulation allows such transfers where "the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request". A similar rule is found in Article 26(1)(b) of the relevant EU regulation. As consent can be inferred in such situations, at least where adequate information about the process has been provided, this overlap is undesirable.

While the wording differs, both the EU and Australia allows transborder data transfers to countries that provide an adequate level of privacy protection.[130] However, there are two key differences. First, unlike the approach taken in Europe, the Australian Privacy Commissioner does not currently identify states with privacy protection meeting the test of a "substantially similar" privacy protection. The second different is related to the first. In the absence of a published 'white list', an organisation may export data if it "reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles".

---

[127] *See* BLUME, *supra* note 47, at 41-42, 98-101.

[128] The weakness of the consent requirement is arguably illustrated in the only reported decision of the Australian Privacy Commissioner that deals with the relevant aspect of NPP 9. In E v. Money Transfer Services [2006] PrivCmrA 5 (Austl.) the Privacy Commissioner held that the complainant had impliedly consented to the overseas transfer of personal information. However, as is reflected in the very fact that a complaint was made, that implied consent may not have been sufficiently informed.

[129] Perhaps the very confronting warnings placed on cigarette packs in Australia, *see Australian Cigarette Warnings*, http://www.smoke-free.ca/warnings/australia-warnings.htm (last visited Nov. 29, 2009), could serve as an example of how consumers can be informed of the risks involved in allowing their personal information be transferred to another country?

[130] For a discussion of some of the key difficulties of assessing the adequacy of a foreign country's privacy regulation, and the questions that arise when doing so, *see* BYGRAVE, supra note 24, at 225-228. *See also* Nikhil S. Palekar, *Privacy Protection: When is "Adequate" Actually Adequate?*, 18 DUKE J. COMP. & INT'L L. 549 (2007-2008).

The reference to a "reasonable belief" creates a significant, and unnecessary, uncertainty without adding any benefits. The appropriate approach would be to require the organisation in question to meet a higher standard of proof by asking them to show that show that the recipient of the information is subject to a law or binding scheme which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles. An example I have used elsewhere illustrates the enormous practical differences:

> Imagine that company A wishes export data to country X. It contacts a privacy consultant (or a law firm) asking the consultant to assess whether a recipient in country X is subject to a law or binding scheme which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles. The consultant writes a statement to the effect that such a law or binding scheme is in place in country X. Imagine further that it turns out that the advice is incorrect, that country X lacks adequate privacy protection and that a data subject suffers loss due to the fact that company A exported their personal information to country X.
>
> If in this scenario the regulation of transborder data flows merely requires a reasonable belief, company A has surely met the test. Indeed, the ALRC Report makes clear that legal advice is sufficient.[131] As a consequence, the affected data subject can make no claim against company A. This has the flow on consequence that, since company A has not suffered any harm from the consultant's poor advice it may not have much of a case to make against the consultant.
>
> In contrast, if the regulation of transborder data flows requires company A to show that the recipient in country X is in fact subject to a law or binding scheme which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles, company A would be unable to do so in our scenario. As a consequence, the data subject can take action against company A, and company A can, in turn, make a claim against the consultant for e.g. negligent misrepresentation or a breach of section 52 of the *Trade Practices Act 1974* (Cth).
>
> As can be seen from this example, the practical consequences are dramatically different, and if one allows oneself to be cynical, it is not difficult to see why some law firms and privacy consultants, as well as data exporting organisations, would be very eager to avoid a change from the inadequate 'reasonable belief' test.[132]

As seen above (7.3) the EU regulation is considerably stricter in this regard.

While the EU adequacy process is widely regarded as dysfunctional and may be subject to reform,[133] it is doubtlessly superior to the Australian approach, and it is possible that Australia's law follows some aspects of the EU approach in relation to the first of these issues if the law is modified as envisaged by the ALRC.

Other grounds for allowing transborder data flows are less controversial. For example, transfers required by law and transfers for the protection of an individual's, or the public's, health and/or safety ought to be acceptable by most standards.

Yet other grounds for allowing transborder data flows are plainly misguided. For example, Australia's proposed regulation would allow an organisation to export personal information about Australian's based on that organisation having "reason to suspect" that unlawful activity or serious misconduct has been, or is being, or even may be, engaged in.

---

131 AUSTRALIAN LAW REFORM COMMISSION, *supra* note 59, at ¶ 1100.

132 Svantesson, *supra* note 89.

133 *See, e.g.*, Christopher Kuner, *Developing an Adequate Legal Framework for International Data Transfers*, *in* S. GUTWIRTH ET AL., REINVENTING DATA PROTECTION? 263-273 (S. Gutwirth ed. 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1464323 (last visited Aug. 31, 2010).

It is not difficult to see how such a provision, for example, can be used to export personal data about Australians suspected of having played some role in illegal file sharing. While it here would be impossible to engage in a discussion of the conflict between legitimate privacy concerns on the one hand, and copyright owners' legal right to find out who infringes their copy right on the other hand, it is submitted that allowing export as proposed will seriously undermine Australians' legitimate privacy expectations.

9.3. Exporter Liability

As is noted above, both the APEC model and the proposed approach for Australia focus on exporter liability. However, exporter liability has a much longer history. For example, taking effect on 1 January 1988, an amendment to the 1973 Swedish Data Act imposed liability on exporters of personal data.[134]

There are clear benefits of holding exporters accountable for how data is used after it has been exported. It may mean that exporters take greater care in selecting to whom they entrust the data, and as noted by the Australian Law Reform Commission, another benefit of this approach is that it does not prevent information from being transferred.[135] This latter benefit fits well with the fundamental constraint that modern society requires cross-border transfers of data, as well as with the right of freedom of expression. Finally, exporter liability goes some way towards disposing of the negative impact of the common law doctrine of privity as discussed above (7.6).

However, overreliance on accountability is dangerous. Greenleaf has observed that:

> The supposed virtue of the new approach is that although your personal information can be exported to anywhere that does *not* have 'substantially similar' privacy protections to Australia, if the exporter does so then theoretically they 'remain accountable' for overseas misuses of your personal information. 'Theoretical' is the key word, because the onus of proof (on the civil balance of probabilities) of a specific breach of a privacy principles by a specific overseas party still rests with you; as does the requirement to prove that the party in breach received the information directly or indirectly (but foreseeably) from the Australian exporting party; as does the requirement to prove that there was a causal connection between that breach and damage to you. And of course the country from which the damage to you emanated might not be the same as the country to which the data was exported, but you are the one who has to join the dots.
>
> How do you satisfy these requirements of proof when your data has travelled to Nigeria, India, Russia, the USA or 'all of the above', and you may not even know? Might it be dangerous to try? Might it be expensive?
>
> The so-called 'accountability' principle is a sham: the absence of any real likelihood of accountability is what is rotten at the core of the ALRC and Rudd Government approach.[136]

---

[134] 23 § Datalag (1973:289), as amended through Justitiedepartementet, Prop. 1986/87:116: "Should criminal damage as specified in Section 20, first paragraph [e.g. due to wilful or negligent dissemination of personal data in violation of Section 11] . . . arise, the person committing the said offence shall provide indemnification for the damage." (Translation of: "Om någon tillfogas skada genom brott som avses i 20 § första stycket eller 21 §, skall den som har gjort sig skyldig till brottet ersätta skadan." The translation was found at http://archive.bild.net/dataprSw.htm (last visited May. 6, 2010) and verified by the author. Breaches of the data export rule outlined in 11 § Datalag (1973:289) (see 1.2 above), were also associated with fines or up to one year's imprisonment, 20 § Datalag (1973:289).

[135] AUSTRALIAN LAW REFORM COMMISSION, *supra* note 59, at ¶ 1095.

[136] Graham Greenleaf, *Rudd Government abandons border security of privacy*, AUSTRALIAN POLICY ONLINE, Oct. 23, 2009, http://www.apo.org.au/commentary/rudd-government-abandons-border-security-privacy (last visited Nov. 29, 2009).

Any inclusion of an accountability scheme necessitates rules governing the burden of proof. As pointed out above, the data subject will typically always be in a weak position in seeking to prove a breach – the data subject will experience the damages flowing from the breach, but may not be in a position to know where or how the breach occurred. This is particularly so, where the breach occurs overseas.

In light of this, accountability alone does not adequately cater for the fundamental constraints that people have a basic right of privacy or that data crossing borders represent a loss of control for the data subject.

The accountability approach should work as an added layer of protection – not as an alternative. Suggestions that accountability can replace imposing limitations on transfers, or that the limitations to when transfer can take place makes accountability unnecessary, are quite simply misguided. To use an analogy, the fact that we have torts law does not mean we do not need traffic rules, and the fact that we have traffic rules does not mean we do not need torts law. Similarly, we need both limitations on when transfer can take place, and accountability rules for when transfer takes place.

Discussing the 'accountability' principle, Kuner brings attention to another problem; that is, the potential conflict between the law of the place of data collection on the one hand, and mandatory laws of countries of data processing on the other hand:

> It is inevitable that there will be conflicts between the 'personal' law of the place where the data were originally collected and the place to which the data are transferred. To take a possible example, personal data in an Australian online political forum might be operated by the Australian online provider via a company located in China. If an Australian member of the forum seeks to assert a right to delete some postings he made in the forum about a Chinese political activist, this might conceivably be illegal under Chinese law.[137]

One option to address this would be to develop rules to assess the reasonableness, in each individual case, of the exporter remaining liable where a privacy violation is prompted by mandatory laws at the place of data processing. It is, however, hard to imagine how such a system would look; without doubt, at least in its application, it would be cumbersome in the extreme.

In order to seek a way out of this dilemma, it is advisable to place the burden on the data exporter's shoulders. After all, the destination for the export, and thereby also the potential application of any mandatory laws found there, lie within the data exporter's control. Put differently, in choosing the destination, the exporter chooses which mandatory laws will affect the data processing. It is then only natural that the data exporter remains liable for privacy violations even where they are prompted by mandatory laws at the place of data processing.

[137] Christopher Kuner, *Global Data Transfers on the Internet: Lessons from the Ancient World*, at 9 (Aug. 7, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1445458 (last visited Aug. 31, 2010).

9.4. Separating the Acts of Organisations and the Acts of Individuals

One thing that was not discussed in the examination of the sources of information relied upon in step five was whether the studied regulations apply to the acts of individuals. As was highlighted in the table presented in 1.2 above, there are many different forms of cross-border data flows; some involving individuals, others involving organisations, and yet others involving governments.

In that context an interesting and highly significant distinction can be seen between the EU approach and that taken in Australia. While the EU regulation applies to individuals, Australia's regulation is weakened by a range of exception to such a degree that it does not apply to acts of individuals.[138]

It is submitted that, any regulation, of cross-border data flows, that applies to the conduct of individuals, must meet certain different needs that regulation that exclude individuals can ignore. There is a greater need for flexibility. This was made clear in the ECJ's third justification of its conclusion in the *Lindqvist* case.[139]

10. Step Eight – Construct Solution at Appropriate Level of Abstraction

Steps two to seven should have placed the researcher in a favourable position to construct a sensible and balanced solution to the research task identified in step one. However, at the same time it must be recognised and remembered that "perfect" solutions to complex regulatory problems are few and far between. In other words, even a researcher that diligently follows the method is likely to be faced with some hard decisions in step eight – decisions that, however they are made, cannot produce a perfect solution.

This is of course neither new, nor uniquely associated with the method proposed here. Every researcher must learn to accept that certain problems do not have a perfect solution.

The researcher may also take some comfort in what we can call the *Pisa effect*. The well-known leaning tower was not intended to lean, but had it not been constructed in a manner that caused it to start leaning, it would never have reached the popularity it now has gained. Similarly, a non-perfect solution may reveal unexpected research findings, and turn out to be much more useful than could have been anticipated from the intended solution.

One of the first tasks facing a researcher that has reached step eight is finding an appropriate level of abstraction for the solution. And yet again, there is no simple answer; or perhaps more accurately, simple answers to this complex question will invariably be nonsensical.

---

138 *Privacy Act 1988* (Cth) (Austl.).

139 See in particular the statement addressed above that: "If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet." Case C-101/01, Criminal Proceedings against Bodil Lindvist, ¶ 69, Nov. 6, 2003, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET (last visited Nov. 24, 2009).

For example, many people would agree that transfers should only occur were appropriate. Thus, one solution would be to have a rule saying that transfers should only occur "were appropriate". However, it is unlikely that consensus can be reached as to when transfer is appropriate. Indeed, it is unlikely that consensus can be reached as to who should decide when transfer is appropriate. Consequently, while this type of abstract rule could gain widespread support as such, it simply would not work on a practical level as we do not mean the same thing when using the word 'appropriate' – the level of abstraction is too high and the result would be a harmful lack of uniformity.

Another important consideration in step eight is the researcher's use of creative solutions. The earlier steps may be seen as rather "mechanical". The question then arises whether the researcher is tied to the possible approaches identified in steps five and six, or whether creativity can be used in step eight to go beyond those approaches in devising the researcher's solution. In my view, the researcher not only *can*, but *should* use her/his creativity in step eight. Steps five and six are not intended to limit the researcher's thinking; rather they are meant to inspire the researcher and provide a suitable point of departure for the researcher's creativity.

While the mentioned creativity is useful to an eminent degree, it can in many cases be combined with the application of established regulatory theories.[140] While the use of regulatory theories in step eight deserves close attention, it would be impossible to go into this now. Here, it suffices to note that the choice of regulatory theory is likely to be guided both by the research task as such, and by the researchers preferences.

As far as my research task is concerned, I have opted for a high level of abstraction with my solution presented in four general principles that must be observed in the regulation of cross-border data flows on the Internet. As can be seen, I draw heavily upon the approaches identified in step five, and the conclusions drawn, as to those approaches, in step seven. However, as also can be seen, I have also ventured outside those approaches drawing upon other sources of possible solutions:

1. *The regulation of cross-border data flows on the Internet must be the same as the regulation of other forms of cross-border data flows* – All of the approaches studied in step five are technology-neutral. Furthermore, convincing arguments were discussed above suggesting that the solution to my research task must be technology-neutral. While it also was noted that technological neutrality may be associated with risks, it is suggested here that, the obvious benefits outweigh the potential risk in this particular context, and any regulation of cross-border data flows should be technology-neutral.
2. *In relation to data exports by organisations, or otherwise systematic export, the regulation of cross-border data flows should take "border control" as its starting point, with export only allowed where specific requirements are met* – Border control ought to be the cornerstone of any regulation addressing data exports by organisations, or otherwise systematic export. However, as noted above, if one concludes that it is necessary to implement some form of border control, one is immediately faced with the task of identifying the circumstances in which data may be exported in line with the limitations flowing from the border control; and that is where the headaches begin. I have identified four such circumstances. In doing so, my aim has been to keep those circumstances few in number, yet adequately broad in nature.

[140] *See, e.g.*, Matthew D. Adler, *Regulatory Theory*, (U. of Penn. Law Sch. Pub. Law & Legal Theory Research Paper Series, Paper No. 10-07, 2010), *available at* http://ssrn.com/abstract=1553781.

The first of those circumstances relates to consent – cross-border data transfers are allowed here the data subject has given genuine consent to the transfer. Genuine consent must be:

- Informed;
- Identifiable;
- Freely given; and
- Variable.

For consent to be sufficiently informed to be valid, the data subject must, for example, be informed of:

- the country or countries which are the destination(s) of the transfer;
- the intended recipient(s);
- the protective measures that will be taken in relation to the personal information;
- how the personal information will be used at the destination; and
- whether the personal information will be transferred from the destination country (where the personal information will be transferred from the destination to a third country, all the information outlined here must also be provided in relation to the third country).[141]

Furthermore, consent given for cross-border data transfers is ineffective if bundled with consent for other issues.

Where the treatment of consent respects these requirements, people have a fair opportunity to inform themselves of what will be involved, including the risks, in consenting to a cross-border transfer. One should hold no illusions that the majority of people will take advantage of this opportunity. However, as we are here balancing requirements imposed by fundamental constraints, I suspect this is as far as this issue sensibly can be taken.

The second circumstance in which cross-border data transfers ought to be allowed involve situations where the transfer is required by the law. As is widely recognised, it is of course necessary to ensure that a data exporter is not acting in violation of the provisions that regulate cross-border data flows, where the exporter is required by the law (e.g. for law enforcement purposes) to export the data in question. In the absence of such an approach, the law would place the exporter in a 'damned if I do, damned if I don't' situation, which the law always must seek to avoid.

Further, the other side of this coin is, of course, that the law must be suitably restrictive in when it requires cross-border data transfers.

When speaking of "the law" in this context, I am referring to the domestic law of the state that regulates the data export. Thus, we must for example separate a situation where the laws of state A both requires and forbids the data export in question, from a situation where the laws of state A forbids the data transfer while the laws in state B requires it. In the latter situation, the location of the data subject is decisive.

[141] Some commentators have expressed concern about the use of consent as a ground for cross-border data transfers. For example, Gunasekara has noted that: "consent cannot be truly informed unless the data subject is aware, at the outset, of all the downstream uses to which the information will be put, making it difficult at least to use this as the basis for allowing the transfer of data overseas." Gunasekara, *supra* note 8.

Where the laws of state A forbids the data transfer, and the data subject is located in state A, the fact that state B's laws require the data export does not justify a cross-border transfer of the data. Otherwise, all forms of data export restrictions would be avoided where a country implemented laws requiring organisations to reveal all the data they hold, and can get hold of, regardless of the location of that data and regardless of the location of that organisation.

Finally, while it is of course not feasible to require that the data subject gives her/his consent to this type of transfers, it should typically be required that the data subject is informed of the transfer, unless doing so would e.g. interfere with law enforcement operations.

Third, cross-border data transfers must also be allowed where they are of vital importance for the health and/or safety of an individual or the public in general, and it is not possible to gain the individuals consent prior to the transfer. Also in this situation, the data subject should typically be informed of the transfer.

The fourth and final circumstance in which cross-border data transfers ought to be allowed is where adequate privacy protection is provided at the place the data is exported to. Whether or not adequate privacy protection is provided at the place the data is exported to should be established by reference to a 'white' list published by each jurisdiction's data authority, and it would be useful if various such data authorities cooperated more intensely in their pursuit of that task. Indeed, data authorities could usefully strengthen, and harmonise, the manner in which their decisions on matters such as white list inclusions are published.

Where export is desired to other places not included on the white list, the exporter needs to gain consent from the data subject. The prospect of consent being granted could, of course, be improved where the data exporter seeks to secure adequate privacy protection e.g. through contractual arrangements with the party to whom the data is exported.

3. *In relation to data exports by individuals, the regulation of cross-border data flows should take the form of abuse regulation* – Having concluded that it would be unrealistic to apply the regime outlined in principle 2 to individuals, an alternative had to be found. Inspiration can here be drawn from the abuse regulation found in current Swedish privacy law.[142]

   A detailed discussion of this abuse regulation goes beyond the scope of this article, but put simply, the Swedish privacy law exempts from its normal regulation, processing of personal information where the personal information is not included in, and not intended to form part of, a structured collection of personal information.[143] Such data processing is only subject to abuse rules. In other words, that type of processing is allowed provided that it does not amount to an abuse of the personal integrity of the data subject(s).

   It has to be acknowledged that there can be no clear rules as to when such a violation has taken place, but any assessment would have to take account of all the circumstances including: the purpose for the processing, the context of the processing, the spread of the processing and the likely consequences of the processing.

[142] Personuppgiftslag (1998:204) (Swed.) as amended.

[143] 5 a § Personuppgiftslag (1998:204) (Swed.).

In providing guidance for assessing whether or not data processing amounts to abuse, *Datainspektionen*[144] states that, for example, the data must not be processed (1) for the purpose of harassment, stalking or scandalising the data subject, (2) in great quantities about a data subject without there being a legitimate reason for the processing, (3) in a defamatory manner or (4) in a manner that violates confidentiality.[145] Finally, the data subject must have the right to have inaccurate information corrected.[146]

This form of abuse regulation is not entirely dissimilar to the application of a tort of invasion of privacy. In fact, observations made as to the limit of such a tort can usefully be taken into account in assessing whether an instance of transborder data flow amounts to abuse. For example, Skoien J's astute observations as to the elements he anticipated would make up the tort of privacy could very well be applied as a guidance as to whether an instance of transborder data flow amounts to abuse:

> In my view the essential elements would be:
>
> (a) a willed act by the defendant,
>
> (b) which intrudes upon the privacy or seclusion of the plaintiff,
>
> (c) in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities,
>
> (d) and which causes the plaintiff detriment in the form of mental psychological or emotional harm or distress or which prevents or hinders the plaintiff from doing an act which she[/he] is lawfully entitled to do.[147]

The problem with any flexible approach is, of course, its flexibility – the flexibility is both the strength and the problem. Ideally, regulation should be more predicable than what this approach is. However, the reality is that every attempt to spell out a rigid definition of when individuals can export data will end in failure, as flexibility is an absolute necessity in such situations.

4. *The regulation of cross-border data flows should ensure that the exporter remains accountable* – As concluded above (9.3) exporter liability should work as an added layer of protection for the data subject in cases of cross-border data flows – it is not an alternative to border control. Similarly, in the case of individuals, the accountability should work side-by-side with the abuse regulation.

Any inclusion of an accountability scheme makes necessary rules governing the burden of proof. As pointed out above, the data subject will typically always be in a weak position in seeking to prove a breach – the data subject will experience the damages flowing from the breach, but may not be in a position to know where or how the breach occurred. This is particularly so, where the breach occurs overseas. In light of this, it is submitted that where it is reasonable to assume that damages suffered by a data subject are due to the data export, the exporter is held accountable unless it shows that no harm stems from the export.

---

144 The Swedish data protection authority.

145 *See* Datainspektionen, *Questions and Answers*, at Question 5, http://www.datainspektionen.se/fragor_svar/personuppgifter/ny_pul5.shtml (last visited Feb. 25, 2007).

146 *See id.*

147 Grosse v. Purvis [2003] Q.D.C. 151, at ¶ 444 (Austl.). For a detailed discussion of a privacy tort in Australia, *see* Des Butler, *A Tort of Invasion of Privacy in Australia?*, [2005] *MULR* 11 (Austl.).

To limit the negative implications of this, exporters can, of course, structure their contracts with the party to whom the data is transferred in such a manner that costs incurred are transferred to that party.

11. Step Nine – Assess Solution against the Fundamental, and Non-Fundamental, Constraints Identified in Steps Two and Three

Once a solution has been constructed in step eight, one may have thought that the process would come to an end. However, a prudent researcher ought to subject her/his solution to tests determining how well the solution will work in practice. Polčák suggest one fruitful way of testing a solution:

> [W]hen assessing some new solution presented for an ICT [information and communication technologies] issue by theoretic or practical jurisprudence, we have to apply a kind of test of amiable compositeur, i.e. of the legal reasonableness and fairness of the presented solution. This test is, however, very simple from a methodological point of view as we just need to confront any given or elaborated solution with one simple question: "Does it make sense?" If we know (reason) or feel (sensitivity, ethical consideration) that it does not, then that solution is not valid and we have to search for another.[148]

One way of applying Polčák's suggestion is to construct a series of case-scenarios[149] to which the solution is applied, and ask whether the result stemming from that application of the solution 'makes sense'. Where a sufficient diversity of such scenarios is crafted and applied in a careful manner, they stand a good chance of revealing inadequacies in the solution.

Under the method put forward in this article, the solution identified in step eight is subjected to two tests. In step ten, the solution is assessed in light of likely future technological developments and uses. In other words, step ten assesses whether the solution 'makes sense' in light of likely future technological developments and uses. However, before that takes place, the solution must be subjected to an even more important test – the researcher must assess the solution against fundamental constraints identified in step two, and against the non-fundamental constraints identified in step three.

As noted in step two, the fundamental constraints represent the *limits to any acceptable solution*. Thus, a solution that does not take appropriate account of the fundamental constraints (bearing in mind how these interact as established in step four) cannot be accepted. In light of this, it is suitable to assess the solution's compliance with the fundamental constraints first, before considering the less important compliance with the non-fundamental constraints.

Applying this test to the four principles outlined in step eight, it will be recalled that no less than seven fundamental constraints were identified in step two, and four non-fundamental constraints were identified in step three.

The easiest of the fundamental constraints to prove compliance with is the requirement that the regulation of cross-border data flows must be technology-neutral. The solution constructed in step eight is doubtlessly expressed in technology neutral language. Indeed, the importance of a technology-neutral approach is such that, the very first principle constructed in step eight relates directly to technology neutrality by making clear that the regulation of cross-border data flows on the Internet must be the same as the regulation of other forms of cross-border data flows.

---

[148] Polčák, *supra* notes 36, at 20.

[149] For an interesting discussion of the use of scenarios for the purpose of assessing privacy regulationsee David Wright et al., *Privacy, Trust and Policy-making: Challenges and Responses*, 25 COMPUTER LAW & SECURITY REVIEW 69, 81-82 (2009).

In allowing for cross-border data flows, provided certain requirements are met, the solution respects the right of freedom of expression, and caters for our modern society with its requirement of cross-border transfers of some data. Furthermore, in being particularly flexible in the regulation of cross-border data flows caused by individuals, the solution takes account of the fact that not all technologies are set up to be sensitive to data crossing borders – it can be expected that organisations are equipped to use cross-border technologies in a more sophisticated manner than individuals.

At the same time, by placing restrictions on when cross-border transfers can take place, and by imposing exporter liability for privacy violations, the solution ensures an appropriate protection of the right of privacy. In the same way, it seeks to address the issues stemming from the fact that data crossing borders represent a loss of control for the data subject. Doing so is crucial in light of the fact that some of the data that necessarily crosses borders for the proper function of Internet communication is personal in nature.

While the solution caters for all the fundamental constraints, it fails in relation to some of the non-fundamental constraints. For example, in separating the regulation of individuals and the regulation of organisations, the solution fails to meet the aim of being made up of one rule to fit all different types of parties being regulated. For the same reason, it could be said that the solution does not meet the simplicity aim. On the other hand, being expressed in only four broad principles, the solution is not overly complex.

Whether the solution will be widely accepted remains to be seen. However, bearing in mind that it goes further than the current regulation in many countries, it can perhaps be expected that its acceptance will not be widespread. In more detail, the solutions acceptance is likely to vary throughout the world, with European countries, and other countries with far-reaching privacy protection, being more likely to accept the solution than countries with little previous experience of privacy protection.

The final non-fundamental constraint to be addressed is that effective protection of privacy is dependent on a widespread understanding of the right of privacy. Perhaps this article, in itself, represents one small step towards an increased appreciation for the right of privacy. However, more importantly, in principle two (in the context of the constructions white lists), it was noted that data authorities could usefully strengthen, and harmonise, the manner in which their decisions on matters such as white list inclusions are published. Indeed, an increased emphasis on making public various data authority decisions, may help create a more widespread understanding of the right of privacy.

12. Step Ten – Assess Solution in Light of Likely Future Technological Developments and Uses

Whether or not technological neutrality was identified as a constraint affecting the solution designed in step eight, it is useful to view, or even test, that solution in the light of emerging technological developments.

In the drafting of her/his solution, the researcher must balance the risk of that rule becoming outdated and thereby useless, and the risk of that rule being applicable in situations it was not suited for, and thereby becoming dangerous.

Thus, whether the researcher's solution is technology neutral or not, step ten – the final step in the method – involves an assessment of how:

1. any likely future technological developments and uses will affect the solution; and
2. how the solution will affect any likely future technological developments and uses.

This step is necessary to avoid the solution getting outdated too quickly. It will also help limiting the risk of the solution having a negative impact on future technological developments and uses. Importantly, this is different to attempts at specifically regulating future technologies.[150] For our purposes, focus is placed on the regulatory approach and how it will interact with future technological developments, rather than on particular future technologies and how best to regulate them.

As could be expected, the difficulty with step ten lies in identifying likely future technological developments and uses, and the researcher's ability to do so successfully will depend in part on her/his technical knowledge. Further, the research question's level of abstraction may impact on the difficulty of step ten; that is, the higher the level of abstraction, the more difficult will it be to identify all relevant technological developments.

In the end, we must admit that we, as lawyers, are typically rather poorly equipped to predict the direction technology will take. However, in most cases, a reasonable level of engagement with newsletters and other news reports, combined with a conscious effort to stay up-to-date with the latest journal publications, should at least give the researcher a 'crystal ball' to look at (be as it may that acquiring the skill to use the crystal ball is more difficult), and position the researcher to cope as well as can be hoped with this part of the research endeavour.

For the research task I have undertaken in this article, I have identified two emerging technological developments against which I will test the solution I presented in step eight.

12.1. Server Farms in International Spaces

There have been attempts at localising server farms to international spaces, such as the high seas, so as to avoid falling within then jurisdictional competence of any regulatory body. For example, some years ago *HavenCo Ltd* sought to use a World War II-era antiaircraft deck in the North Sea as an offshore server farm.[151] More recently, *Google* has been showing interest in pursuing the idea of offshore data storage centres.[152]

In light of this, any regulation of cross-border data that focuses on transfer to a third country may be inadequate. For example, it is doubtful whether Article 25 of EU Directive 95/46 could be applied to a situation where the data is being transferred to a server farm on the high seas, since it specifically refers to "transfer to a third *country*" (emphasis added).

In contrast, the solution developed here (like the proposed Australian regulation) uses a more neutral terminology referring to export generally without specific reference to the location to which the data is exported to.

---

[150] Such attempts are fraught with danger, not least the very real risk that regulatory speculations will stifle technological developments. Indeed, it has been noted that, if lawyers were to *a priori* assess future technological developments, we would most likely not even have a wheel today.

[151] *See, e.g.*, S. Garfinkel, *Welcome to Sealand. Now Bugger Off*, WIRED, July 2000, *available at* http://www.wired.com/wired/archive/8.07/haven.html (last visited Nov. 27, 2009).

[152] R. Miller, *Google Planning Offshore Data Barges*, DATA CENTRE KNOWLEDGE, Sept. 6, 2008, http://www.datacenterknowledge.com/archives/2008/09/06/google-planning-offshore-data-barges/ (last visited Nov. 29, 2009). *See also* U.S. Patent No. 7,525,207 (filed Feb. 26, 2007).

Thus, it can be concluded that, the development of server farms being localised to international spaces, such as the high seas, will not undermine the solution presented in step eight.

12.2. Cloud Computing

The term 'cloud computing' is associated with great ambiguity. However, Clarke has provided a useful definition:

> Cloud computing refers to a service that satisfies all of the following conditions:
>
> - The service is delivered over a telecommunications network;
> - Users rely on the service for access to and/or processing of data;
> - The data is under the legal control of the user;
> - Some of the resources on which the service depends are 'virtualised', which means that the user has no technical need to be aware which server running on which host is delivering the service, nor where the hosting device is located; and
> - The service is acquired under a relatively flexible contractual arrangement, at least as regards the quantum used.[153]

Consequently, the term cloud computing encompasses both relatively novel developments such as social networking sites and *Google Docs*, as well as well established services such as Microsoft's *Hotmail*.

As cloud computing has been hailed as a major shift in how we use ICT facilities, it is useful, or indeed necessary, to test how the solution developed in step eight copes with cloud computing. In fact, bearing in mind the obvious tension between the geographical nature of law and the ubiquitous nature of cloud computing, cloud computing may be seen as the ultimate challenge for any regulation of cross-border data transfers. This is one side of the coin. The other side consist of the fact that, the regulation of cross-border data may amount to the single largest obstacle for all forms of cloud computing where data is not contained within one particular jurisdiction.

To test how the solution presented in step eight will work in the context of cloud computing, it is convenient to use a hypothetical scenariio.

Imagine that company A places personal information about person B on company A's *Facebook* site. Imagine further that the person responsible within company A is aware that several of company A's *Facebook* "friends" are located outside the country in which both company A and person B are located. Has company A in this case transferred personal data to a third country, and if so, would that transfer be allowed under the solution outlined above?

The first thing to note in this situation is that we are here dealing with an organisation. That knowledge helps us decide whether principle two or principle three is applicable. In this case principle two is applicable and we must look to the border control provisions. As the scenario does not seem to involve transfer based neither on a legal requirement nor on a health and/or safety justification, the transfer in this case would only be allowed if the data subject had given genuine consent to the transfer, or adequate privacy protection is provided at the place the data is exported to. Either of these grounds for transfer requires company A to know where *Facebook* will store the data, and where company A's *Facebook* "friends" are located. Furthermore, in either case, the exporting company would remain liable for the use of the data.

---

[153] Roger Clarke, *User Requirements for Cloud Computing Architecture*, PROC. 2ND INT'L SYMPOSIUM ON CLOUD COMPUTING (forthcoming May 2010), *available at* http://www.rogerclarke.com/II/CCSA.html (last visited Jan. 31, 2010).

If we change the imaginary example so that instead of a company posting the information on its *Facebook* site it is an individual doing so, we need to consider principle three of the solution instead. In that case, we need to assess whether, all things considered, the data transfer amounts to an abuse. This would, for example, depend on the type of data being exported and whom the recipients are. However, also other factors could be considered such as the level of privacy protection in the country to which the data was exported.

Neither of these outcomes is surprising or out of line with the aims of the solution presented in step eight.

13. Concluding Remarks

In this article, I have tried to outline a method that can be used to find solutions to the challenges of regulating Internet technology. To provide an example of how this method can be used, I have applied it to the area of regulating cross-border data flows on the Internet. Consequently, the article has served a dual purpose.

Focusing on the research method advocated here, it consist of ten different steps during which the researcher goes from defining the problem to identifying the outer limits within which a solution is to be found, finding inspiration for the solution and finally constructing and testing the solution. It is hoped that the research method meets all of the following four goals. First, it should be reasonably simply to use. Second, it ought to provide for an adequate degree of research transparency. Third, the method is scalable, so as to be useful for a variety of types of research tasks. Finally, it is flexible enough to suit a range of different styles of research.

Turning to what was concluded from the application of the method to the research task of constructing a set of principles that regulate cross-border data flows on the Internet, it was found that there are four fundamental principles that should govern such a regulation. First, it was concluded that the regulation of cross-border data flows on the Internet must be the same as the regulation of other forms of cross-border data flows. The second fundamental principle made clear that, in relation to data exports by organisations, or otherwise systematic export, the regulation of cross-border data flows on the Internet should take "border control" as its starting point, with export only allowed where specific requirements are met. Third, in relation to data exports by individuals, the regulation of cross-border data flows on the Internet should take the form of abuse regulation. Finally, the fourth fundamental principle clarified that the regulation of cross-border data flows on the Internet should ensure that the exporter remains accountable.


European
University
Institute
European University Press