RSCAS 2013/37
Robert Schuman Centre for Advanced Studies
Global Governance Programme-51

Providers' liabilities and the right to be forgotten

Giovanni Sartor

European University Institute
Robert Schuman Centre for Advanced Studies
Global Governance Programme

Providers' liabilities and the right to be forgotten

Giovanni Sartor

EUI Working Paper **RSCAS** 2013/37

ISSN 1028-3625

Printed in Italy, June 2013
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu/RSCAS/Publications/
www.eui.eu
cadmus.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies (RSCAS), created in 1992 and directed by Stefano Bartolini since September 2006, aims to develop inter-disciplinary and comparative research and to promote work on the major issues facing the process of integration and European society.

The Centre is home to a large post-doctoral programme and hosts major research programmes and projects, and a range of working groups and *ad hoc* initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration and the expanding membership of the European Union.

Details of the research of the Centre can be found on:
http://www.eui.eu/RSCAS/Research/

Research publications take the form of Working Papers, Policy Papers, Distinguished Lectures and books. Most of these are also available on the RSCAS website:
http://www.eui.eu/RSCAS/Publications/

The Global Governance Programme at the EUI

The Global Governance Programme (GGP) is research turned into action. It provides a European setting to conduct research at the highest level and promote synergies between the worlds of research and policy-making, to generate ideas and identify creative and innovative solutions to global challenges.

The GGP comprises three core dimensions: research, policy and training. Diverse global governance issues are investigated in *research* strands and projects coordinated by senior scholars, both from the EUI and from other internationally recognized top institutions. The *policy* dimension is developed throughout the programme, but is highlighted in the GGP High-Level Policy Seminars, which bring together policy-makers and academics at the highest level to discuss issues of current global importance.The Academy of Global Governance (AGG) is a unique executive *training* programme where theory and "real world" experience meet. Young executives, policy makers, diplomats, officials, private sector professionals and junior academics, have the opportunity to meet, share views and debate with leading academics, top-level officials, heads of international organisations and senior executives, on topical issues relating to governance.

For more information:
http://globalgovernanceprogramme.eui.eu

Abstract

I address the novelties contained in the “Proposal for a Data Protection Regulation”, recently advanced by the EU Commission, with regard to providers’ liabilities and the right to be forgotten. First I consider how the Proposal regulates the contentious overlap of e-commerce immunities and data protection rules. Then I examine providers’ knowledge that illegal personal information has been uploaded on their platform, and discuss whether such knowledge should terminate providers’ immunity. Finally, I critically assess the right to be forgotten, newly introduced in the Proposal, and the sanctions for its violation.

Keywords

Providers liability, Web-hosting, Data protection, Right to be forgotten.

1. Introduction[*]

As data are moving into the web and over the clouds, hosting is becoming ubiquitous, polymorphous and interconnected.

On the one hand, in the user-generated web, not only we store our web-pages in the servers of host providers, but we produce and distribute content in multiple ways: we upload our texts, our music, our pictures on various on-line repositories, making them available to a world-wide audience; we build our public images on social networks, where we disclose aspects of our personalities, interact with others, advertise our social and work capacities, create and map our relationships; we create blogs where we present our work, tell our stories, present our initiatives; we express our opinions by intervening in forums and commenting on web-pages and blogs.

On the other hand, in the cloud, we keep our data in remote data farms (infrastructure as a service), we access remotely located software programs (software as a service), we use virtual computers emulated by the provider's hardware and software (computing as a service).

Web hosting and cloud hosting have, in principle, different functions, which overlap to some extent with the public-private divide (at least concerning individual, rather than corporate usage): the first enables us to make content accessible to others, while the latter offers a remote substitute for the use of one's personal computer (memory, software, computing power); the first provides us with a public space for sharing and communicating, the second with a remotely accessible private space. When putting or accessing content on the web we exercise the freedom of expression and information as well as economic and political freedoms, while when using the cloud for storing the documents we own and the computer tools we need, we exercise not only our property rights, but also our right to autonomy, work, and to the "security of the person," given that our personal computer space has become in a way our "external mind," where we store our memories and often outcomes and tools of our work.

However, the borderline between what is public and what private is getting increasingly fuzzy and shifting: on the one hand users can restrict their web audiences to particular circles of people, and on the other hand they can instantaneously move content from their private spaces on the cloud into the public web, uploading such content into some web hosting platform, or just linking it to publicly accessible web pages. Thus, to better analyse this new normative scenario, some conceptual analysis may be useful, and in particular the distinction between two dichotomies: private vs. public and personal vs. anonymous.

The private-public distinction opposes privately-kept information and publicly-accessible information. It addresses the scope of distribution of the information, according to the choices of individuals having factual and legal control over such information, in particular by having created the information or at least having selected it. Information is factually private to a person when that person has the factual possibility of restricting access to it, and it is legally private to a person when that person has the legal power of making such access permissible or impermissible. For instance, the present paper is both factually and legally private before I send it to he publisher. In fact since its only embodiment is stored on my computer protected, I can effectively prevent others from accessing it by keeping the computer with me, and moreover I can validly prohibit them from accessing it, on the basis of my property right over the computer. With regard to the legally private information, we may want to distinguish again between information that is legally private on contextual ground and information that is legally private on intrinsic grounds. In the first case the prohibition from accessing/ reproducing the information results from the rights over the embodiment of the information or the

[*] Some parts of this paper have already been published in "International Data Privacy Law" Journal, 2002.

container of such embodiment (such as my property right over the computer), in the second case it results from rights over the information itself (such as copyright or also data protection rights. The information ceases to be factually private when it is distributed to others, so that I loose control over its circulation, it ceases to be legally private in the case of intrinsic privateness, to the extent that I authorise access to it, and allow for its reproduction/distribution.

The private/public distinction overlaps, but is to be distinguished from a different distinction, namely the distinction between personal and anonymous information, the first being the information that concerns an identified identifiable persons. In this regard we have to distinguish two ways in which information can be personal. A piece of information can be intrinsically (or semantically) personal in the sense that the information itself concerns an individual; it can be contextually (or pragmatically) personal in the sense that the context where it appears provides information about individuals. In particular, the very fact that a piece of information having certain content was created or even just collected by an individual provides some clues about what that individual is or may be. Just to give an example, recently an Italian political activist issued a tweet expressing a derogative view of a gay politician using highly vulgar and offensive words. The tweet arguably was public, having been made publicly accessible through the web, but it embodied personal information both with regard to its object (the gay politician) and with regard to its issuer (the activist making the statement), whose impoliteness and homophobia it revealed.

Finally there is a further distinction to be considered, namely, the distinction between neutral and non-neutral information processing. This is relevant when, as in the context of web or cloud hosting, information is uploaded by a user and is processed (and in particular, distributed) in the infrastructure provided by a third party. It seems to me that in this context neutrality for a processing taking place on a third party infrastructure is based on two related conditions: (1) the provision of an infrastructure which is useable for any pieces of information (possibly within constraints pertaining function of the infrastructure, e.g., limitations pertaining to the subject matter of a blog), according to the independent choice by the user; (2) the fact that the processing at issue is directly meant to realise the objectives of the user (in particular, the objective of making this information accessible to the public). Through serving the user's aims (e.g., by facilitating access to the material though indexing), the provider also achieves his own purposes, typically, increasing access to the website, which may lead to revenue from advertisers. However, this result supervenes on the outcome that is aimed at by the user, namely, on the information-sharing functions for the sake of which the user is uploading content on the platform. Neutrality does not cover further activities by the provider, such as using user's information for administrative purposes, or for various commercial interests, such as profiling or providing personalised advertising.

My inquiry is limited to information freely uploaded by users and neutrally processed by providers' platforms. Thus, I shall only address the role of providers as neutral (though self-interested) enablers of the sharing of user generated-information, in the context of web and cloud-hosting. In this context I will critically examine the right to be forgotten considering the impact of the new regulation on users' freedoms, directly or by modifying providers' behavior.

2. The e-commerce immunities

Web-hosting of user-generated information is governed in the EU by the E-Commerce Directive,[1] which exempts providers from liability for hosting illegal content, while maintaining the liability of the users who have uploaded such content. The fundamental justification for these immunities can

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). In the US, similar immunities are provided by US Digital Millennium Copyright Act and the Communication Decency Act.

identified through a simple counterfactual argument, namely, by considering what would happen if providers where held liable, under criminal and civil law, for the illegal information hosted on their platforms: the risk of incurring liabilities would force providers to police the Internet, to engage in filtering out or removing any content for which they may be liable.

In fact, while being unable to filter or remove all illegal information (given the huge amount of data being put on line, still increasing thanks to the development of web and cloud-services), providers would have to be proactive to limit their liabilities. To clean their huge web premises as much as possible from illegal data they would need to interfere with content uploaded by their tenants (users having generated the information): providers could reduce false negatives (the distribution of illegal information) only by increasing false positives (the removal of legal information). Thus providers liability would lead to "collateral censorship" (Balkin, 2008), which would on the one hand undermine users freedom and on the other hand involve high costs, to the detriment of current business models (free user access supported by advertising), and of the usage of the Internet.[2]

Through the regulation of providers' immunities (and the limitations of such immunities), the conflict of multiple valuable interests and rights is somehow balanced: third parties' interests in preventing the distribution of certain data (interests concerning intellectual property, reputation, privacy, hate speech, etc.), users' interests in distributing information (freedom of speech and expression, political and social participation, artistic freedom, economic freedom), users' interests in accessing information (such as participation in knowledge and culture), economic interests of providers (and their market freedoms), public interests (preventing illegal activities, promoting creativity, innovation, access to knowledge and economic progress). In the E-Commerce Directive this balance is stuck by Articles 14 (hosting) and 15 (no general obligation to monitor).

According to Article 14, providers are immune when

- they have no actual knowledge of illegal material, or
- upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to the information.[3]
- Moreover, according to Article 15, member states may not impose general obligations on providers
- to monitor the information
- to actively to seek facts or circumstances indicating illegal activity.[4]

Here I shall not provide an overall analysis of providers' immunities but I shall limit myself to considering how such immunities bear upon data protection with regard to user-generated content.

---

2 There exists a vast literature on providers' immunities. See among others: Lichtman and Posner (2006), Lemley (2007), Hylton (2007), Grimmelmann (2009a). For European law, a detailed analysis can be found in Spindler, Riccio, and Van der Perre (2006). On social network, see also Grimmelmann (2009b).

3 Article 14 (1): "Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."

4 Article 15: "1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

It is dubious whether the e-commerce immunities also apply to data protection, which is governed by the Data Protection Directive[5] and its national implementations.[6] National judges and data protection authorities have adopted different approaches,[7] and even recent EU documents directly addressing data protection with regard to user-generated content (such as Article 29 Working Party's Opinion 5/2009 on online social networking) seem wary of making reference to the E-Commerce Directive. This view may be supported by a literal reading of Article 1 (5), of the E-Commerce directive, according to which the E-Commerce Directive does not apply to issues covered by the Data Protection Directive.[8]

Failure to apply the e-commerce immunities to data protection might lead to what we may call "data protection exceptionalism": while the immunities would cover any other liability for user-generated content – from infringements of intellectual property, to defamation, hate speech, incitement to crime, etc. – they would not apply to user-generated violations of data protection. According to this view, whether the provider would be considered liable or not when hosting third parties' private data would only depend on data protection law: we have to rely only on the Data Protection Directive (and its implementations) to construct the regulation of web-hosting with regard to the illegal processing of user-generated personal information.

I believe that data protection exceptionalism should be rejected: even the existing law allows us to conclude that, contrary to the literal reading of Article 1 (5) of the E-Commerce Directive, the e-commerce exemption applies horizontally, covering any kind of illegal content, including illegally uploaded personal data. We can achieve this outcome through a restrictive interpretation of Article 1 (5), namely, by arguing that this article refers to the Data Protection Directive only the "questions relating to information society services covered by Directives 95/46/EC", which do not include providers' immunities with regard to user-generated data. In other terms, the E-Commerce Directive defers to data-protection law for the specification of what processings of personal data are illegal, while giving providers immunity for all illegal processings taking place on their platform (including those processings that are illegal because of violations of data protection law).

However, certain limitations of the liability of host providers could also be obtained independently of the E-Commerce Directive, on the basis of an appropriate interpretation of provisions in the Data Protection Directive. First of all, Article 3 excludes from the Data Protection Directive the use of personal-data in merely "purely personal or household activity." Thus, as long as the users' activity,

---

5 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).

6 The Data Protection Directive is complemented by the Directive on privacy and electronic communications (Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector), recasting Directive 97/66/EC.

7 For instance the e-commerce immunities are not even mentioned in the recent Italian judgement where three Google executives where condemned as a consequence of the distribution of a video containing sensitive personal data over YouTube (case Google-Vividown, decided by the Tribunal of Milan on 24 February 2010, sentenza n. 1972/2010). For a critical analysis, see Sartor and Viola de Azevedo Cunha (2010). For a review on cases web hosting and data protection, see Viola de Azevedo Cunha, Marin, and Sartor (2012).

8 Article 1 (5): "This Directive does not apply to ... questions relating to information society services covered by Directives 95/46/EC and 97/66/EC." This idea is developed in recital 14: "The protection of individuals with regard to the processing of personal data is solely governed by 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 and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries."

supported by the providers' infrastructure, can be considered purely personal, no issue of data protection emerges. This would be the case when the user stores her information on the cloud making such information inaccessible to others, or also when the information is accessible only to a restricted circle of people. Secondly, the Data Protection Directive provides for the distinction between two addressees of the data protection rules, the controller and the processor, the first deciding what data to process, for what purposes, the second implementing the choices of the first.[9] It is not clear how responsibilities for illegal processing are shared by the controller and the processor. We could limit the liability of the provider by assuming that when engaging in a neutral activity with regard to user-generated data, the provider only acts as a processor, and by arguing the a processor has no general obligation to monitor or check the inputs he receives from the controller, both with regard to the uploaded data, and to the ways in which this data are neutrally processed in the provider's platform. This understanding of the controller-processor relationships would allow us to map the provider-user distinction in the E-Commerce Directive into the controller/processor distinction in the Data Protection Directive.

3. Knowledge of illegality and on-line censorship

After having argued for the application of the e-commerce immunities also to user-generated data violating data protection, we need to consider how such immunities should be understood in order to best balance all interests at stake, namely, the interests of possible victims (data subjects), but also the interest of on-line speakers (uploaders), listeners (downloaders), and providers (enablers).

In particular, we have to examine the provision of Article 14 (1), of the E-Commerce Directive, according to which a provider is immune only as long as he "has no actual knowledge of illegal material, or upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."

Knowledge of the illegality of a certain piece of data involves 2 aspects:

1. the factual knowledge that the piece is hosted on the provider's server;
2. the legal knowledge that the piece violates the law.

To examine the interpretive issues emerging from this provision we need to focus on the concept of knowledge. According to the most common understanding of this concept, we have knowledge when we believe something that it true, which means that the concept of knowledge includes at least two elements: belief and truth.[10] A person knows that *p* is the case when both of the following hold: (a) the person believes that *p* is the case and (b) *p* is indeed the case. Thus for the provider to know that he is hosting illegal materials both of the following must hold: (a) the provider believes that he is hosting illegal materials and (b) the provider is in fact hosting illegal materials. Our interpretive problem pertains to (a), namely, we need to examine what it means for the provider to believe that he is hosting illegal materials.

---

[9] Data Protection Directive, Article 2 (1): "(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; (e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."

[10] For the idea of knowledge as true belief, see recently Goldman (1999, ch. 1). According to other authors, for having knowledge, also justification is needed (a true belief held without a plausible ground would not constitute knowledge), as argued by Plato in the dialogues *Meno* and *Theaetetus*. Therefore only true and justified belief would provide knowledge. Others have argued that this is not yet sufficient to obtain knowledge (following the seminal contribution by Gettier, 1963), and have provided additional conditions. This important philosophical debate, however, is not very relevant for our purpose since all those conceptions include at least the elements we have mentioned, namely, belief and truth.

One possible answer follows from assuming that a true factual belief is enough. According to this perspective (which corresponds to the principle according to which ignorance of the law is no excuse, "ignorantia legis non excusat"), the provider would lose his immunity, and thus be obliged to remove or make inaccessible a piece of data (a text, a picture, a photo, a movie) from his platform whenever he has the true belief that the piece is on the platform, and the piece happens to be illegal (even though the provider does not believe that the piece is illegal). So considering our notion of knowledge as true belief, for the obligation of the provider to be triggered, all of the following should hold, under this interpretation: (a1) the provider believes that a certain piece is on the platform, (b1) the piece is indeed on the platform, (b2) the piece is illegal.

According to the second perspective, the provider would be obliged to remove the piece only when he knows that both the piece is on platform and it is illegal. Thus all of the following should hold, under this second interpretation: (a1) the provider believes that a certain piece is on the platform, (a2) the provider believes that the piece is illegal, (b1) the piece is on the platform, and (b2) the piece is illegal.

Note the difference: according to the first interpretation, for the obligation to take down to be triggered one element is missing, namely, (a2), the provider's belief that the hosted content is illegal: the provider would be obliged to take down also material he considers to be legal (or more probably so, or possibly so), under threat of being liable in case his judgment were considered to be wrong by the competent authority.

Thus, the first interpretation puts the provider in a difficult situation, and would presumably lead to collateral censorship. We have to distinguish here different epistemic conditions, depending on the nature of the illegal content. In some cases the only difficulty consists in knowing whether a certain piece of content is on the platform. Once this knowledge is achieved, establishing whether the piece is illegal is straightforward. This may be the case, for instance, when a right-holder complains about a copyright violation consisting in mere duplication of a registered work (though it may be doubtful whether the right holder has consented to the publication, or whether the use of the work may be considered as fair use, or fall into a copyright exception). More often, however, assessing illegality is much more difficult: even if the provider knows that a certain material is on his platform, he may remain in doubt (and thus fail to form a precise belief) concerning the illegality of such a material. This is the case in particular when competing constitutional rights are involved: consider for instance how it may be difficult to assess whether copyright has been infringed in the creation of a new work inspired by a previous one (intellectual property v. freedom of expression or artistic freedom), or whether by making statements about a person, her data protection rights are infringed (data protection v. freedom of expression).

In such cases, in fact, we may even wonder whether there are objective standards conclusively determining whether the material is legal or illegal, or whether this qualification depends upon a discretional decision by the judge. But this would take us into the legal theory debate on the objectivity of legal knowledge and on the determinacy of the law, i.e., on whether there is only one right answer to each legal issue or whether the law may sometimes be incomplete or undetermined, and whether such an answer, even if it exists, is accessible to a legal reasoner endowed with non-superhuman skills. Without going into that debate, I assume that we have the cognitive skills that allow as to answer such question in many cases, though with degrees of doubt. It may also be argued what is here at issue is not so much the truth of the proposition that a certain content is legal or illegal, but the forecast that the competent authority will consider the content to be legal or illegal, a forecast that we often can (and do indeed) make, though with degrees of doubt.

In situations of legal uncertainty, making the provider liable for hosting illegal information would provide him with a strong incentive to remove any piece of material on whose legality he has even a small doubt; even when a piece appears to be more probably legal, the expected potential loss would

outweigh the marginal benefit the provider derives from keeping that particular piece on line (alongside with all other materials in the platform).

To clarify the point, let us suppose that the provider is able to assess the probability $p(i_d)$ of the illegality i_d of certain piece of data *d*. Let us also assume that in case the piece is really illegal and it is not removed, the provider will have to pay a compensation c_d, while if the piece remains on line, the provider will gain a benefit b_d (the expected additional advertising revenue to be obtained consequent to accesses to the piece of data *d*). Given this arrangement, if the provider leaves the piece on line, his expected loss is $c_d * p(i_d)$, while his expected gain is b_d. So, the expected outcome (gain minus loss) is $b_d - (c_d * p(i_d))$. If he decides to take off the piece, the outcome is 0, no gain and no loss. Clearly, the provider will leave the material on line only when

$$b_d - (c_d * p(i_d)) \geq 0$$

Assuming for instance that the compensation to be paid is 100, while the gain to be obtained by leaving the material on line is 1 (usually the marginal gain a provider can obtain by making one additional piece available is quite low), we have that, for the provider to keep the material on line it must be that:

$$1 - (100 * p(i_d)) \geq 0$$

This will hold only in the few cases when that the probability of illegality $(p(i_d))$ is less (or equal) to 1%. In all other cases, the provider will prefer to take down the information to prevent potential losses.

One possible way out of this perplexity would consist in relying on the provider's assessment of the illegality of the content. This could be obtained by conditioning liability also on some degree of certainly in legal knowledge,[11] namely, in making the provider liable only when he has the belief the he is hosting illegal user-generated content. Such a belief will only exist when the provider in good faith accepts that both certain content is on its platform, and that the content is more probably illegal rather than legal.

Let us assume that the provider has to assess the legality of a set of pieces of data $S = L \cup I$, where *L* is the set of the legal pieces and *I* is the set of the illegal ones. The set *S* may be, for instance, the set of pieces he is requested to take down by the data subject.

Any mistake (taking down legal material or letting online illegal material) will have a social cost. Let c_l be the average social cost of taking down a legal piece *l* and c_i the average cost of letting an illegal piece *i* on line. Then the objective is to minimise the following social cost (the expression $|X|$ indicates the cardinality of a set *X*, namely, the number of its elements):

$$c_l * |L_{out}| + c_i * |I_{in}|$$

where L_{out} is the set of legal pieces that are taken out and I_{in} is the set of the of illegal pieces which are left in.

To simplify the calculations lets us assume that the two kinds of mistakes (keeping illegal data on line on line and taking out legal data) have on average the same cost, so that the objective becomes minimising the following sum

$$|L_{out}| + |I_{in}|$$

Let us assume that the provider can only state whether a piece of information is more probably illegal or more probably legal, and then when making such evaluation he does better than chance. In other words we assume that when the provider says that a piece of information is more probably legal (illegal) there is a chance higher than 50% that it is legal (illegal). For simplicity's sake, let us also assume that the number of legal and illegal pieces in *S* is the same: $|L| = |I|$. Then we get a better

[11] I assume that belief and knowledge can come in degrees, even though I cannot enter here a discussion on the matter, see Haack (1993) and Goldman (1999).

outcome (a lower value for $|L_{out}| + |I_{in}|$) by authorising the provider to let on line all content he believes in good faith to be more probably legal (assuming that the he acts accordingly), rather that telling him to take down all materials he is requested to take down. We also get a better outcome in this way than by making the provider liable for every illegal material he leaves on line, a choice which, as we have seen would lead him to take down all risky materials.

Assume for instance that the provider's judgement on legality or illegality is correct in the 60% of cases. Then the number of mistakes will be $(|L| + |I|) * 0.4)$. Given the assumption that $|L| = |I|$, this is $2L * 0.4 = L * 0.8$, which is inferior to $|L|$, the number of mistakes we will obtain if the provider were to take out all materials he is asked to remove (including pieces legally on line), for fear of undergoing liability in case he were mistaken.

The model here proposed can be developed by considering the possibility that a more serious damage is caused by leaving the data on line then by removing it (or vice versa), and by considering the different prior probabilities that the data are legal rather an illegal (see also the next footnote). This, however, seems to make legal enforcement very difficult. How can we assess the existence of the illegality belief in the provider's mind? A proxy for that, however can be given by the "objective" possibility of achieving a sufficient degree of certainty in such an assessment with a reasonable effort, under the given circumstances. So, the provider's belief in the illegality (of a content he knows to be in his platform) should be excluded when a reasonable person, under such circumstances, could still possibly doubt that the content might be legal.

The legality-judgment by the provider could also be substituted with a mechanism that invites the parties (the data subject and the uploader) to make their legality-assessments, and which induces such assessments to be sufficiently reliable. This could be obtained, for instance, by adopting a notice and takedown procedure such as that introduced by the US Digital Millennium Copyright Act with regard to copyright infringements. According to the DMCA, the uploader who considers that his rights are infringed sends a notice to the provider, who takes down the material and informs the uploader; if the uploader replies with a counter notice (claiming that the uploaded material is legitimate), then the provider will put the material back, unless the right-holder starts a lawsuit. The actions by the right-holder and the uploader signal the probability that the material is legal or illegal: the notice signals the probability that it is illegal (according to the judgment of the right holder), but the counter notice signals that it may on the contrary be legal (according to the uploader), and the decision to sue by the right-holder, again signals the probability that it is illegal (according to more serious evaluation, which involves the cost of starting the lawsuit).

For instance, assume that before the lawsuit there is a very small chance that a randomly taken piece of material is illegal (e.g., 1%). Assume also that the probability that a piece is illegal goes up to 50%, in case that the right holder sends notice of a data protection violation, and that the provider has a 60% chance of judging correctly when requested to determine whether a piece is legal or illegal. Under these assumptions, with regard to those pieces that are claimed to be illegal by the right-holder, we get a better outcome by relying on the provider's judgment, rather than by taking down (or leaving on line) all such pieces.

However, assume that a counter notice by the uploader signals that there is an 80% chances the data is legal (only those who have good grounds would react to the notice). Then it is better than the provider does not exercise his judgment with regard to the counter-noticed pieces, but leaves all materials on line. Were he to apply his judgement (which is correct in the 60% of the cases), he would make things worse: the materials he would wrongly discard would exceed the materials he would rightly preserve. On the contrary, the fact that there is no counter notice may signal that the material is probably illegal, so that it is better to take it down, regardless of the provider's judgment. And so on.

Additionally (or alternatively), we may introduce a judgment on illegality (a presumptive judgment, subject to judicial review) by a body that is better placed and more competent than the provider, i.e., in particular, by a data protection supervisor. Under such arrangements the provider

should enjoy the immunity as long as he, when reached by a notice of a data-protection violation, informs both the uploader and the data protection authority and follows the indications from that authority.

4. Providers' liability in the new regulation and the right to be forgotten

Let us now address the changes that the new EU Proposal for a Data Protection Regulation[12] introduces with regard to providers' liability. First of all, we need to ask ourselves whether all doubts concerning privacy-exceptionalism (i.e., the idea that commerce immunities do not apply to data protection) have been removed. This seems indeed to be the case, according to the clear statement of Article 2 (3), according to which the Regulation "shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive." Thus it seems that the immunities also apply to data protection, their general coverage not being limited by the Regulation.

A possible residual uncertainty may arise in connection with Article 88 of the Regulation, according to which references to the Data Protection Directive "shall be construed as references to this Regulation." In fact, such references also include the above-mentioned Article 1 (5) (a) of the E-Commerce Directive, which should therefore be read as: "Art. 1, par. 5: This Directive does not apply to ... questions relating to information society services covered by Data Protection Regulation." Thus, on the one hand the Regulation is without prejudice to the application of the E-Commerce Directive (whose immunities should therefore cover also user-generated data involving data protection violations), and on the other hand the E-Commerce Directive does not apply to questions covered by the Data Protection Regulation. A clarification on this regard would be welcome, even though the issue may be addressed through interpretation, namely, arguing as above that the Data Protection Directive establishes what processings are illegal, while the Directive exonerates the providers for certain illegal processings taking place on their platforms (including those being illegal for violating data protection law).

Moving down to specify previsions, we need to consider certain rights of data subjects, which entail corresponding obligations of data controllers. Whether such obligations apply to providers neutrally processing user-generated data depends on whether such providers, when exercising this activity, can be considered as controllers.

If providers were controllers, they would be charged with very burdensome tasks. For instance, according to Article 14, they would be required to chase any person mentioned in a blog, social network, or forum, to inform that person that data about him or her is on the platform and to provide him or her with any "information needed to guarantee fair processing."[13] There is a limitation to this

---

[12] COM(2012) 11/4 Draft Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). For a precise analysis of the Regulation, see Kuner (2012). See also De Hert and Papakonstantinou (2012).

[13] Article 14 (1): "Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer; (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (c) the period for which the personal data will be stored; (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data; (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (f) the recipients or categories of recipients of the personal data; (g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission; (h) any further

requirement, namely the provision of Article 14 (5) (b), according to which the controller is exonerated from such an obligation when "data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort," but it remains to be established when an effort may be considered "disproportionate", a concept that invites highly discretional evaluations by data protection authorities and judges.

Article 17 (1) grants data subjects the "right to be forgotten and to erasure," namely, the power to obtain "from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data."[14] The definition of this right, as it has been observed (Rosen, 2012) fails to distinguish two kinds of user-generated personal information:

1. information about the data subject that she has put on a provider's platform
2. information about the data subject that other users have put on a provider's platform.

It seems to me that case (1) is uncontroversial: a data subject should have the right to eliminate all personal information she has chosen to upload on the provider's platforms. More generally, I think that the very idea of neutral processings of user-generated data (processings meant to satisfy users aims) entails that users should be given in principle the possibility of withdrawing any data they have uploaded (users should maintain full ownership of all data they upload). This aspect is particularly addressed by Art. 18, which introduces a right to portability, understood as the right to "The data subject shall have the right to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject." Above we have distinguished between data that are semantically personal, since they consist of information about the data subject (such as her photo, or a description of some of her life events), and data that are contextually personal, since the data is about other things, but they appear to have been collected or authored by the data subject. Art. 18 may indeed raise the issue of whether also the latter data are covered. To give an example, according to this article, has a person who uploaded various pictures on Facebook, only the right to have back the pictures about her, in an appropriate format, or this right extends to pictures of other people uploaded by the same person?

Going back to art. 17, we need to observe that the controversial aspect of the right to be forgotten concerns case (2), namely whether a data subject should have the power of ordering the provider to erase content about herself uploaded by other users (who could have created such content, or have obtained it by reproducing or modifying content originally published by the data subject). Since the obligation to comply with such orders only concerns controllers, the decisive point seems to be whether the provider could be considered a controller or only a processor with regard to such personal data. For instance, we may ask whether Wikipedia is a controller or a processor with regard to personal data published by Wikipedians on Wikipedia's pages.

Let us first assume that the provider only is a processor with regard to user-generated data (concerning an identifiable third party), while the user having uploaded such that data is their only controller. In this case the data subject wishing her personal data to be erased according to 17 (1), should request the user to take down the data he has uploaded. The user should then consider whether to take the data down or whether to leave them on the platform, facing the risk of a lawsuit. The

(Contd.)

information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected."

[14] Article 17 (1): "The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons."

concerned data subject could also request the provider to take down the data, but in this case, given that the provider only is a processor, the data subject could not rely on art. 17 (1). The data subject's request could only be based on the e-commerce regulation, according to which a provider becomes liable when he knows that he is hosting illegal data (which would raise the issue of knowledge of illegality we discussed above).

Let us now assume, on the contrary, that also providers (besides users) are considered as controllers with regard to user-generated data concerning third parties. Then a provider would have the obligation to take down from his platform the content uploaded by any users, whenever the provider is requested by the concerned data subjects, according to Article 17 (1). This would mean that providers would become law enforcers for data protection, exercising this power-duty against their users, who would be deprived of the possibility to object and resist. If a provider-controller would fail to take down privacy-infringing content, not only will the provider have to compensate the damage, but he will also be subject to a severe sanction (art. 77), as we shall see in the next section. Under such conditions providers seems to have no choice but to remove any content has a non-null chance of being considered illegal, without paying attention to any objections. It seems to me that this second way of understanding Article 17 (1) could involve a serious infringement of fundamental rights of Internet users, and in particular, an unacceptable limitation of freedom of expression.

Let us now consider Article 17 (2), according to which the controller who has made personal data publicly available has the obligation to "take all reasonable steps, including technical measures, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data."[15] We need to address the case where personal data, originally uploaded in a provider's platforms, have been reproduced and copies of such data have been made accessible over the Internet in the platforms of other providers (or in the servers of individual users). We distinguish again the two possible qualifications of the original provider, namely, as a processor or as a controller.

Let us first assume that the user who has uploaded other people's personal data is the only controller of such data, while the host provider is their processor. Then the obligation to contact every third party who is processing the data would only fall upon the user. To meet the request by the data subject, the user would have to contact anybody possesses copies of the uploaded data (both users-controllers and providers-processors), and inform them of the erasure request. This would put a serious burden on the user (even though only reasonable steps are required). In particular, the user would be forced to engage in a search over the whole Internet even when the data subject had initially given her consent to the publication of the data (e.g., to the publication of a photo) and has then changed her mind. In many cases, it may not be clear what is meant by the "data the publication of which the controller is responsible". Assume for instance that in a blog some comments were posted concerning a person (e.g., observations about a public persons' financial problems or sentimental affairs), and that similar comments are later published elsewhere on the Internet (in blogs, forums, etc.). Do these other comments contain the same data as published in the original post? Is this the case also when the same information was obtained from other sources and expressed in different ways?

Let us now assume that also the host provider is a controller with regard to other people's personal data uploaded by a user. The provider should then contact all entities hosting copies on the data and inform them of the data subject's request. This information would then trigger for all other providers (who would also be controllers of anything they host) the obligations to take down the data, according to 17 (1). Under this interpretation, thus, the request by the data subject will start a global chase for

[15] Art. 17 (2): "Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication."

any instance of the data, involving all providers hosting total or partial copies of such data. All providers would have to interfere with the choices of their users, removing data uploaded by the latter or making such data inaccessible. The erasure order would not only concern copies of the data, but also links to them, which would require search providers to interfere with their methods for indexing and searching.[16]

It seems to me that under both interpretations the implementation of the right to be forgotten is likely to cause uncertainties and costs, and endanger freedom of expression. The second interpretation (viewing the host provider as a controller) is likely to cause a most serious threat to freedom of expression: the request to take down the data would spread virally over Internet, bringing with it the obligation to "clean" any server from the unwanted information or links to it, an obligation whose violation is severely punished as we shall see.

A further critical aspect of the proposed regulation of the right to be forgotten is the insufficient breadth and strength of the exceptions provided for the obligation to remove data. Such exceptions are mentioned in Article 80, according to which "Member States shall provide for exemptions or derogations ... for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression."

First of all, we may wonder whether the "reconciliation" of data protection and freedom of expression should be completely delegated to national legislations, even though freedom of expression is a most important fundamental right, recognised in Article 11 of the European Charter of Fundamental right as the "freedom to hold opinions and to receive and impart information."
Secondly, it seem that the exceptions to the right to be forgotten (the right to have information erased) are very narrowly framed, as concerning "solely" journalistic purposes and artistic or literary expression.

For instance, the notion of "journalistic purposes" could be understood as only applying to materials published by registered journalists, or in registered journals. This would allow unrestricted censorship of the emerging citizens' journalism (publication of information and opinion by non-professional people in blogs, forums, etc.). Non qualified individuals or organisation (such as Weakileaks) would be obliged to take down any information that, while addressing social or political or social matters, mentions individual persons.[17] If the notion of journalism were limited to information on recent events, activities aimed at informing people about the past (e.g., inputting information on a Wikipedia page concerning past political scandals) would similarly become illegal as soon as people are called with their names. Thus it seems that exceptions covering "solely" journalistic and artistic/literary may fail to cover the full extent of the "right to impart information," as established on the UN Human Rights Declaration, the European Convention of Human Rights and the EU Charter of Fundamental Rights. It is true that the case law of the European Court of Human Right (see particularly the Steel and Morris v. UK judgment of 2005) may support a broad conception of "journalistic purposes," but the distinction between journalism and other manifestations of freedom of expression remains highly controversial.

In section 83 of the Regulation, there is an also an exception to the obligation to forget, with regard to data published by "bodies" conducting "historical, statistical and scientific research," when the publication of such data is "necessary to present research findings." Again, consider a passage in a Wikipedia-page mentioning individuals involved in a past event (e.g. a political scandal, a crime, etc.). We may wonder whether an individual having contributed the page is a "body" and whether the re-publication of other people's research outcomes would count "presenting research findings." Some

[16] On how interventions on search methods may have a negative impact on Internet freedoms, see Lemley, Levine, and Post (2011).

[17] On citizens' journalism on the Internet, see for instance Benkler (2011).

cases of this kind have been addressed in different ways in different jurisdictions, according to how such jurisdiction understand the need to balance data protection and freedom of expression. I am not putting into question that a proportionality based approach may be needed to address such issues, but the Regulation seems to go beyond that, ordering censorship whenever the strict grounds for an exceptions based on journalism or historical research are not available.

5. Is this really a right to be forgotten?

In the previous paragraph we have considered the right provided for in art. 17 in its general term, as a right to be forgotten and erasure'', i.e., as a general a power to obtain removal of one's data, on a set of different grounds. With the term of "right to be forgotten'' or more exactly "right to oblivion" a more specific idea is usually conveyed. This is the idea that information which was originally legitimately distributed may have to be removed at a subsequent time, on social and moral grounds that should find a technical but also a legal response (see in particular Mayer-Schoenberger 2009). In this section I shall consider how the passage of time can impact on data protection, addressing the right to be oblivion strictly understood.

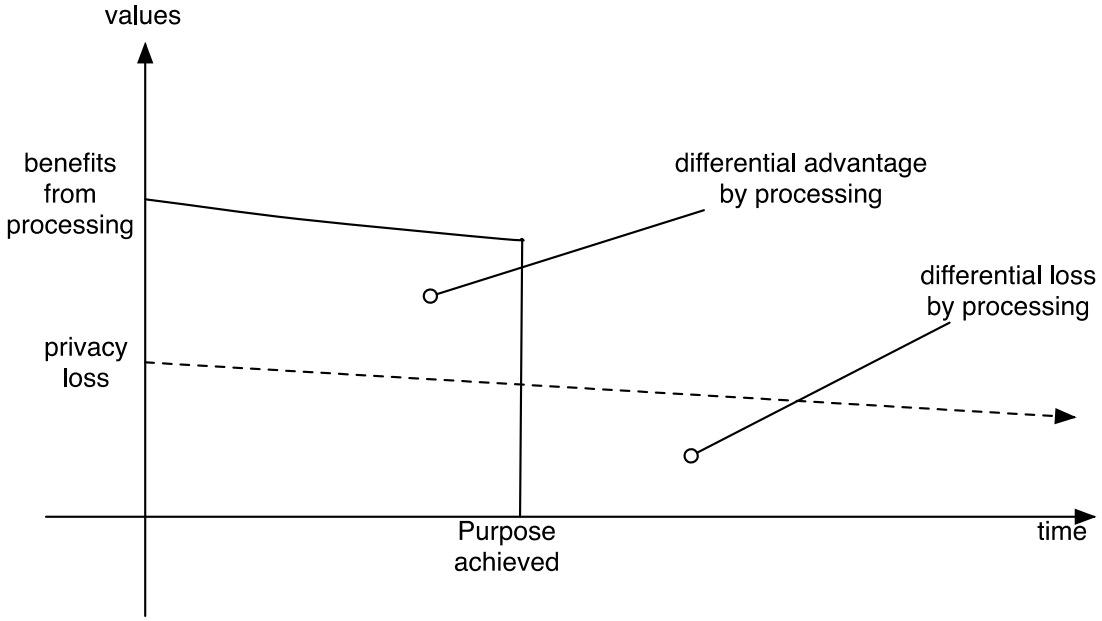
The basic idea is that the passage of time may have an impact on the legality of information that is distributed on line. This may happen either because the data-subject has changed her mind about the distribution of the information who was legitimate only on the basis of her (revocable) consent, or because the constellation of interests has changed so that what could be legitimately distributed at a certain point in time (regardless of the data-subject's consent) can no longer be distributed at a later time.

Let us first focus on the second aspect. The ground for this change in the legal discipline of the same piece of information consists in time's impact on the interests and values at stake: on the one hand the data subject's privacy interest (not to have the data distributed without his or her consent) and on the other hand the existing data processing interests (the interests in distributing and accessing the information, such as freedom of speech and freedom of information). A specific reference to such a balance can be found in art. 6 (e) of the new regulation, according to which processing is allowed when it "is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." We shall now consider whether and how this balance may change over time, involving a change in the legitimacy of data processing.

Let us first address the case when the processing has been completed at a certain point in time, since its purpose has been fully achieved. In such a case there is arguably no utility in continuing to process the data. Once the goals have been achieved, there is no benefit in further processing the data, so that processing should stop. The pattern characterises such a situation is presented in Figure 1. The horizontal axis represents the passage of time, from the initial moment when the processing started (time 0). The vertical axis represent the impact of processing on the interests at stake, on the one hand the benefit with regard to the processing interests (pertaining, for instance to security, or public health, of to the implementation of a contract) and the loss in privacy, on the other hand. Even when all conditions for legitimate processing are satisfied, a loss in privacy takes place, which is, however outweighed by the benefit to the goal that are served by legitimate processing. Note that this representation assumes that both impacts are represented in the same scale of importance, so that they are comparable (on comparing impacts on different rights and values, see Sartor 2010, 2013), an assumption which follows from the very idea of a proportionality assessment (though proportionality also involves a further aspect, namely the idea of necessity, i.e., the non-availability of a less infringing way to achieve the processing interests).

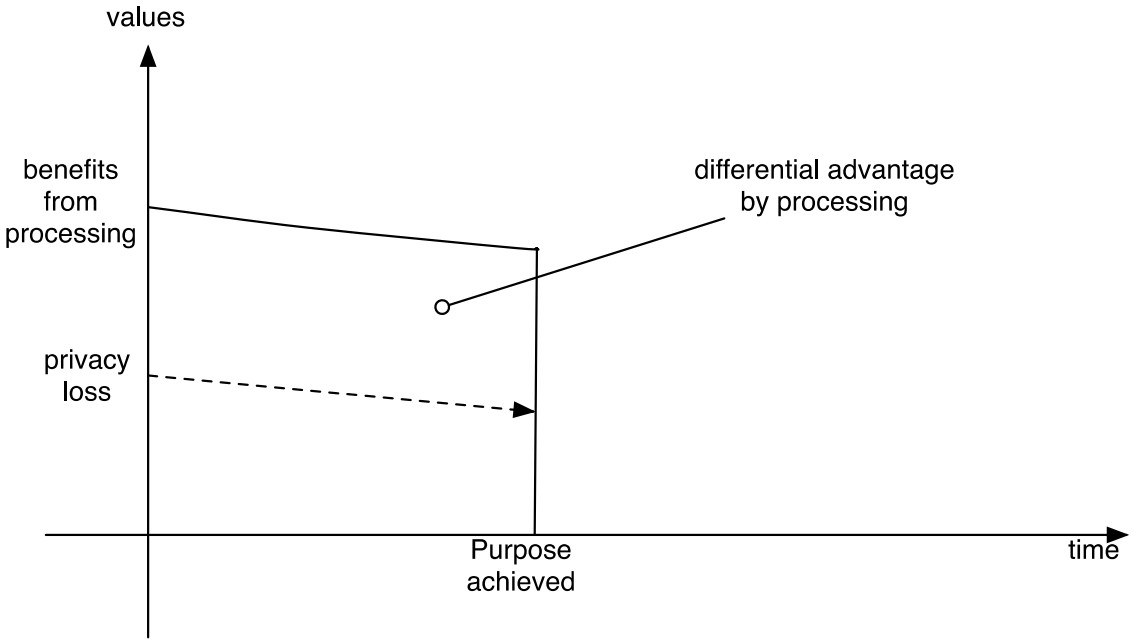
More precisely, the trade-off involved in the processing, namely the net outcome we obtain by subtracting the loss in privacy to the benefit of processing is positive up to the time when the goal is achieved, then it becomes negative since the loss in privacy is not compensated with regard to the achievement of other (legitimate) goals.

Figure 1



After that point there is no utility in continuing processing the data, only damage to privacy. Clearly, under this framework, a better overall result would be achieved by stopping processing (and deleting the data) after the goal is achieved, as shown in Figure 2.

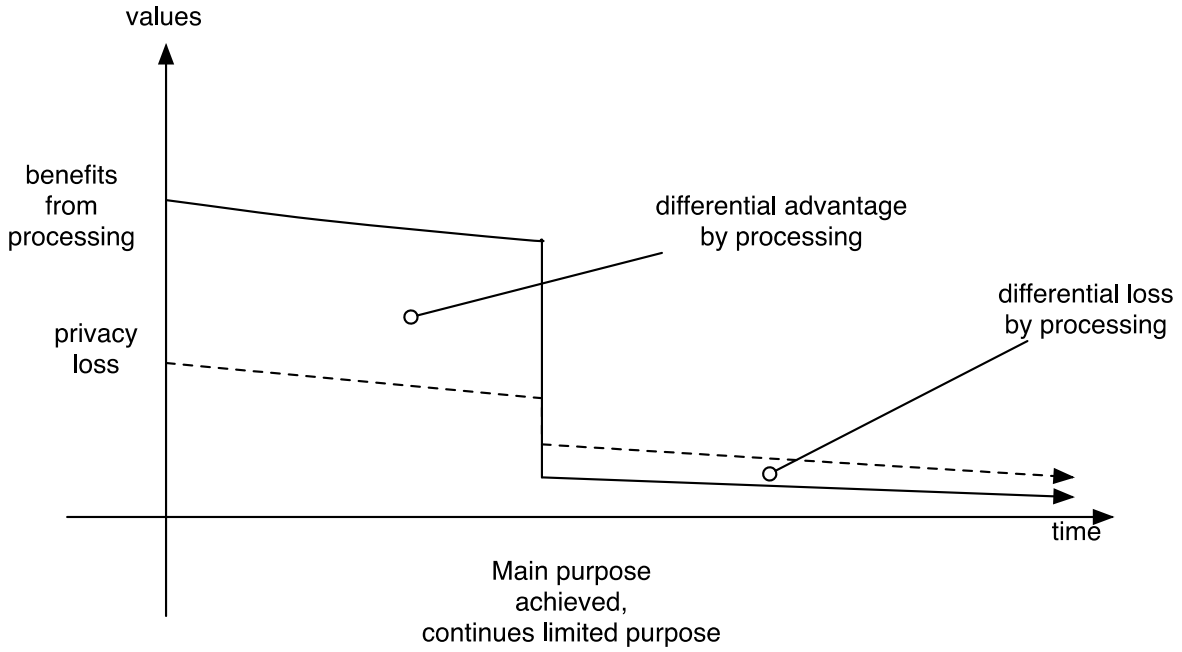
Figure 2



A different result is shown in the Figure 3 where we see that after the main purpose of processing is terminated there may still be minor purposes to be achieve, whose achievement may be combined with

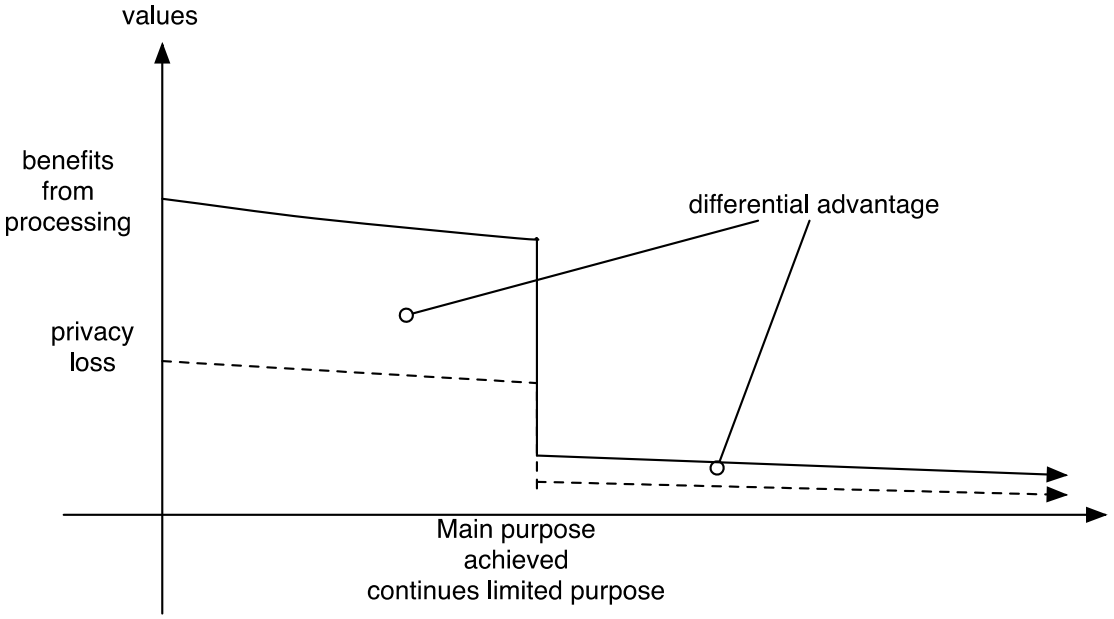
measures which reduce the damage to privacy, having regard to that particular usage. Consider for instance the case when data about a dependant or a client may be need to be kept separately as a poof of the transaction, to be accessed only when an issue emerges. This particular kind of processing could involve a smaller detriment, which is even inferior to minor advantage that is brought about by the continuation of the processing, after the end of the primary usage of the data. Then the processing should continue even after the achievement of the main goal.

Figure 3



Note that it is not always the case that the minor advantage obtained by a reduced processing justifies the continuation of a minor limitation to privacy is the case, and not necessary. It may be that the minor advantage provided by the limited usage is outweighed by the remaining loss to privacy, as indicated in Figure 4. In such a case, processing should be completely terminated as soon as the purpose is achieved.

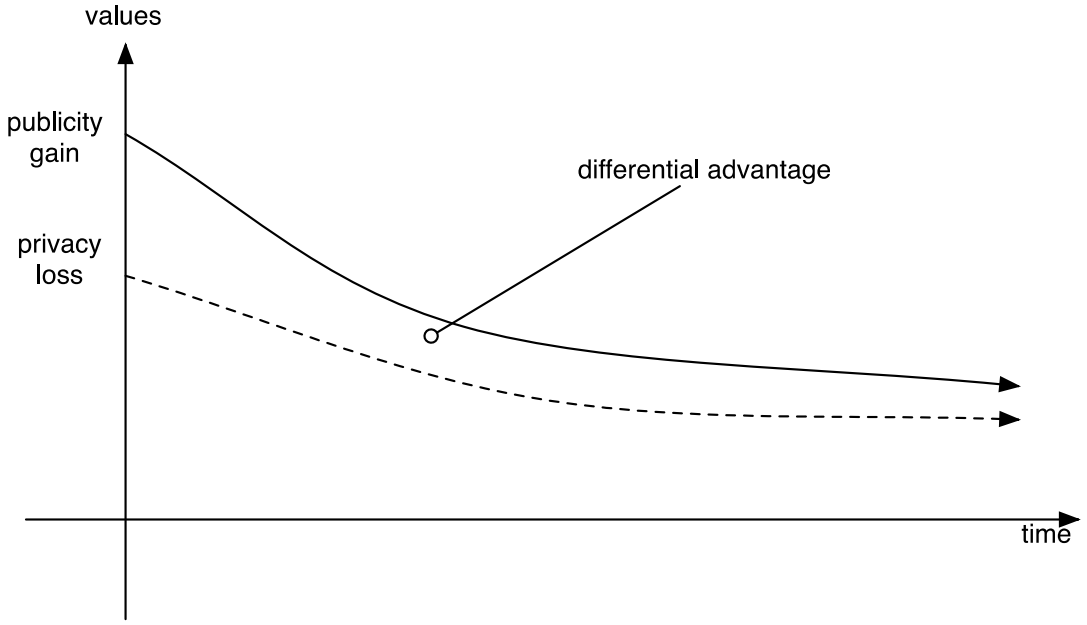
Figure 4



It is also possible that the continued conservation of the data would still contribute to the original main purpose, though to an extent that it diminished through the passing of time. As typical examples of this phenomenon, consider data collected through cameras on the street for security purposes, or information that is distributed on-line for journalistic purposes (even by street journalists). With regard to this kind of information we may consider different configurations of the interests at stake, always assuming that, as time goes by, processing has a continuously decreasing impact both in on the processing interests and on the privacy interests of the data subject. The latter decrease seems to be usually (though not always) present, under the reasonable assumption that we are generally less interested in old facts, give less importance to them (in particular as signals of what a person is now). Moreover we assume that the decrease rate of the impact on the processing interests is larger than the decrease rate of the impact on privacy interests.

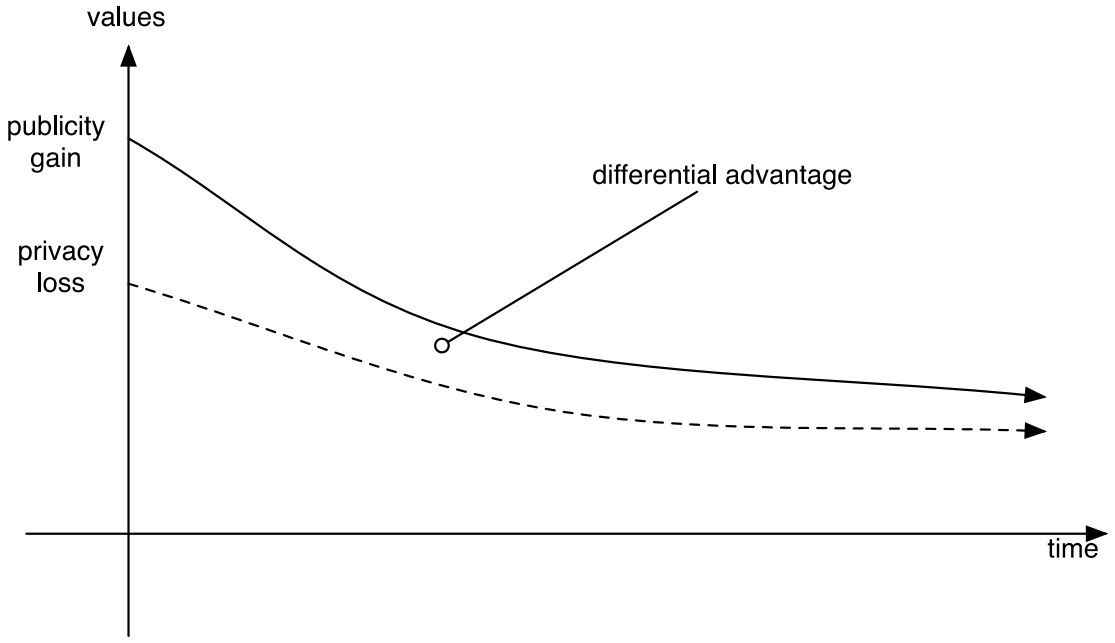
The first, and easiest case to be considered is when the loss with regard to privacy overrides the advantage of distributing the information from the very beginning. Consider for instance the publication of data concerning health or sexual preferences of a person, when this is much significant to his or her social role. Or consider taking and maintaining information from cameras located in toilets, changing rooms or even meeting rooms where no particular security issues are present. In such a case, as shown in Figure 5, the loss to privacy is at no time compensated by gain in freedom of expression/information. Therefore processing should be always forbidden.

Figure 5



The situation is completely overturned in the scenario represented below, where instead there is a social interest in a certain piece of information being distributed and accessed, which always outweighs the privacy interest of the data-subject. As an example, consider personal information (even health information) concerning a person having an important public role, information that is relevant to that role. In such a case the time-induced reduction in the impacts on both freedom of expression/communication and privacy interests does not change the relative importance of the two: the first always outweighs the latter. Thus in such a case processing (and in particular distribution) should always be allowed regardless of the passage of time.

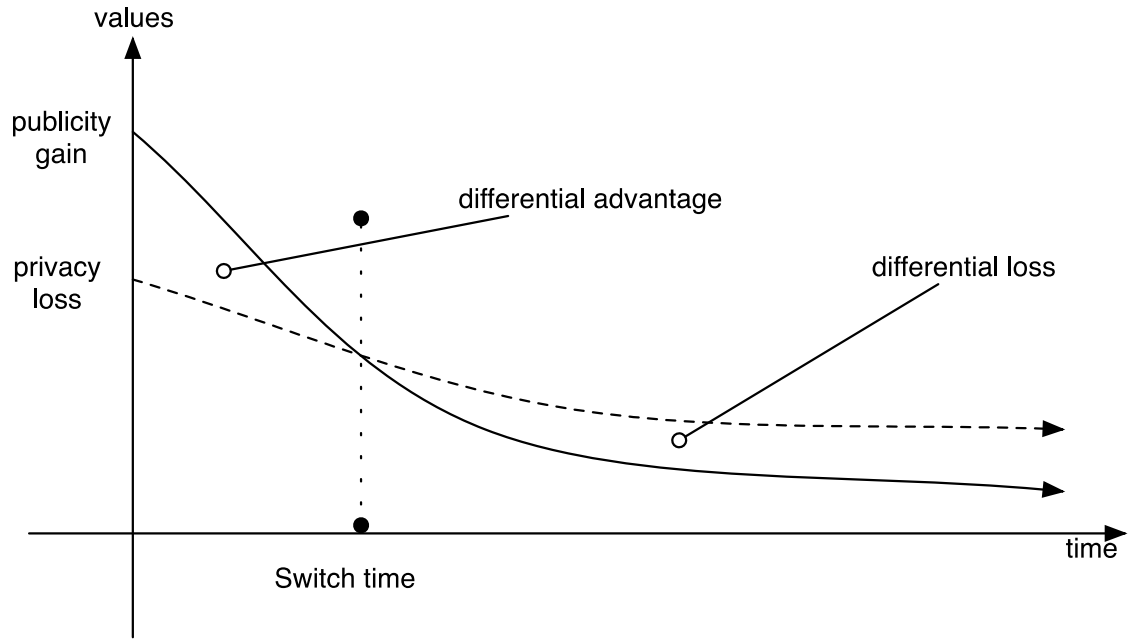
Figure 6



Thus, even though both the importance of the news is (slowly) diminishing it should remain accessible to everybody (processing interests remain asymptotically superior to the privacy interest). This is the case, in particular for people having an important public role and in particular, for those having a paradigmatic significance with regard to the role they play.

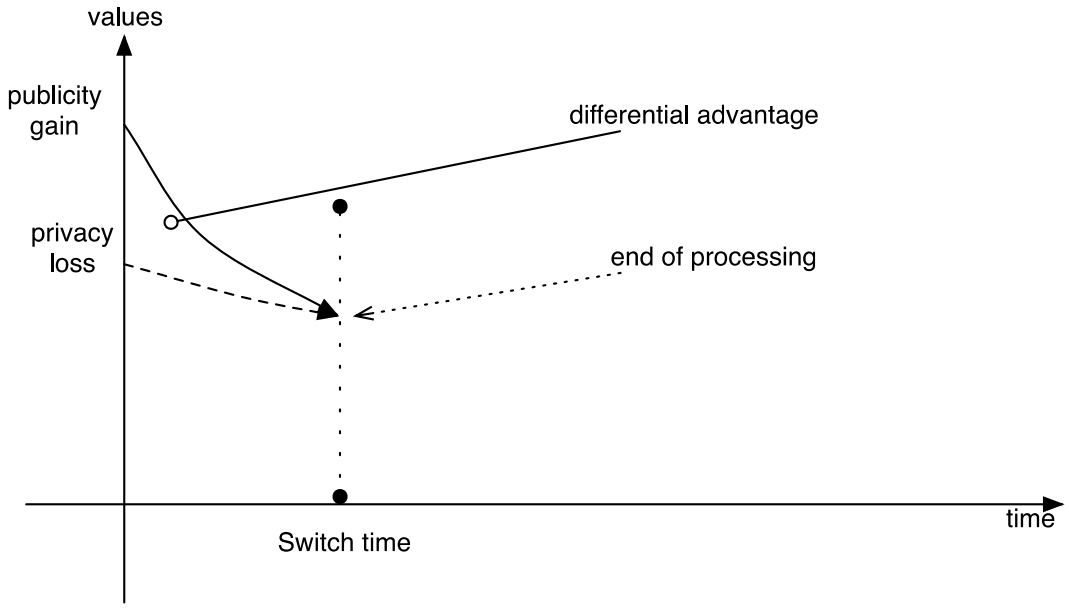
Now let us consider the case directly concerns the right to be forgotten (to oblivion). This is the situation where up to a certain point in time the processing interests prevail, and after that point in time privacy takes the lead. As typical examples consider the situation where certain information is most relevant to the public for a short time after its publication and then loses most its general interest, but continues to have a negative impact on the privacy interest of the concerned person. For instance consider the situation where certain information relevant to security (e.g. information taken from cameras on shops and streets) loses most of its significance after a short time (since arguably the effects of crimes usually can be immediately detected, so that investigation can be performed a short time after the crime was committed) while continuing to have a negative impact on the privacy of the persons whose images are stored. In such a cases, usually both impacts on freedom of expression and on privacy would decrease as time goes by, but the diminution of the impact on freedom of expression would proceed at a steeper pace, so that while at the beginning the benefit would outweigh the loss, at a certain point in time there is a change: the loss in privacy outweighs the benefit in freedom of expression/security. This is the point in time where arguably, the data should be forgotten: In such a case the maximization of the useful result is obtained by switching from processing to not processing the data.

Figure 7



By stopping processing at switch time, a better overall result is indeed obtained: we maintain the differential advantage obtained before switch time without incurring the differential loss we would suffer after that time.

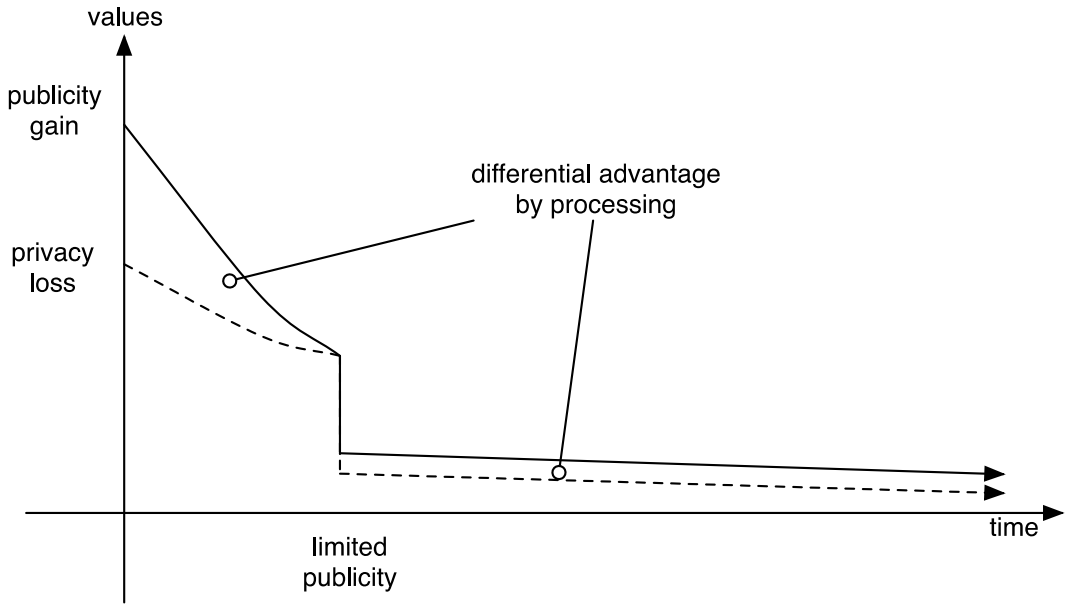
Figure 8



A different solution is also possible, namely, to change the kind of processing at the switch time. Typically this may happen by ensuring that the stored data is processed in particular ways, making it less easily usable and accessible. For instance, a number of judicial decisions have recognized that newspapers are not required to delete articles containing old personal information. On the contrary, it may be sufficient to store old articles in separate archives, so that they are no longer accessible through general searches on the web,

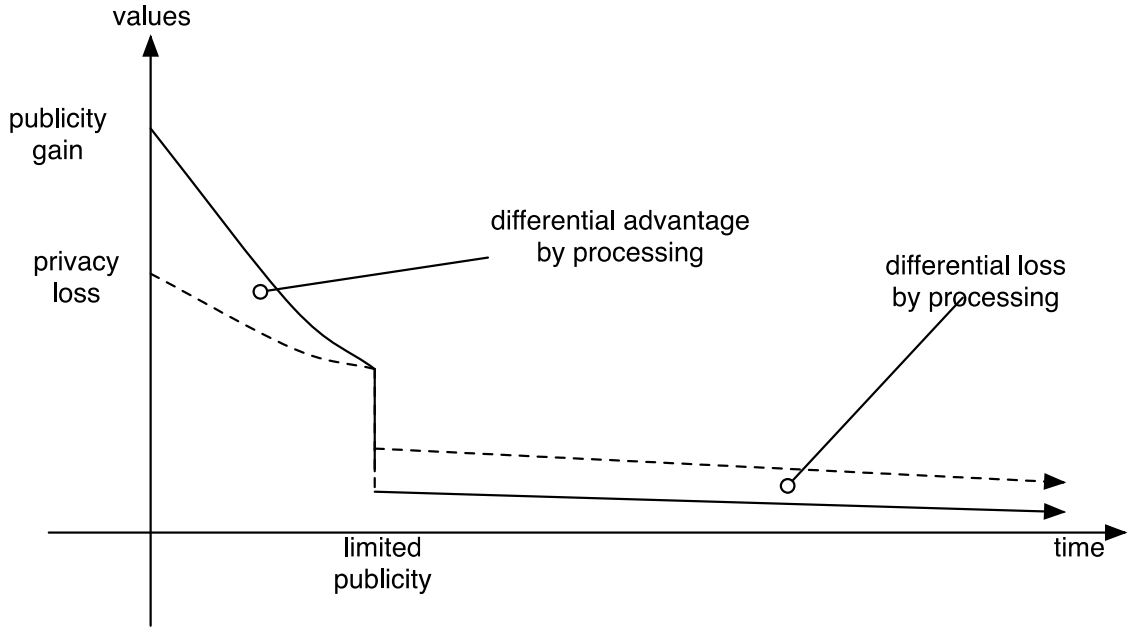
Such limitations to the processing of personal data impose some burdens on users wanting to access the information, but they limit the damage to privacy, so that the overall result may still be positive, even after the switch time. Consider for instance the solution in Figure 9 below. The total benefit is higher than in **Error! Reference source not found.**, since also the differential advantage obtained through the reduced processing after the switch-time can be added to benefit obtained before that time. Thus, the optimal outcome is obtained by having a limited processing with an inferior privacy loss, rather than in erasing the information. When privacy opposes freedom of information, we may indeed often have a right to (partial) concealment minor accessibility, rather than a right to erasure. Such a partial concealment can be obtained in different ways, typically by putting the data in repositories to which only certain categories of people have access (e.g., journalists) or which in any case are not accessible through general searches on the web.

Figure 9



Obviously, this assumes that the differential advantage still is higher than the privacy loss resulting from this different use. Were this not the case, even the limited processing should be stopped (or rather it should not even begin). Consider for instance the case for a continued storage of data collected though street cameras, under particular safeguards (e.g. in encrypted form, with key accessible only to the police). It may be argued that the limited utility of such data still does not justify the ensuing infringement to privacy. The situation is depicted in the following Figure 10, which shows that under such conditions is would be better to terminate any processing, past the switch time.

Figure 10



So the conclusion of our analysis is that indeed there are instances where a right to be forgotten, or more exactly the right to the oblivion of certain information, should be recognized. These are the cases where processing interests outweigh privacy interests up to a certain point, after which the first are

outweighed by the latter. Obviously, the relative importance of privacy against other interests, and in particular interests in freedom of speech and access to information may be measured in different ways in different legal systems. In particular, as it is well know, the US is more on the side of freedom of speech (and also of commercial interests) while in Europe information privacy is more valued. Consequently, the same situation (e.g., the provision on a Wikipedia page of the name of two criminals, some time after the crime) may be considered differently in the two legal systems: in the US approach the benefit to freedom of speech and information may outweigh the loss in privacy, while in some European state the opposite may hold.

6. Sanctions for those who do not forget

The need to give due consideration to a right to oblivion or right to concealment (limited access) under the circumstance above described needs to be connected to specific measures addressed to the parties at issue. As we argued above, such measures would be appropriate when they would minimize the impacts of mistakes, including among mistakes both the continuation of processing that should be stopped (since the loss in privacy interests outweighs the benefit to the processing interests) and the termination of processing that should be continued (since the processing interests outweigh the privacy interests). We need to consider whether the sanctions provided for the right to be forgotten in the proposed General Data Protection Regulation are likely to achieve this outcome, i.e., whether the parties involved, namely, the data uploader, the provider and the data subject are given the right incentives with regard to minimising mistakes

I considered above the problems involved in determining whether processing is legitimate, and have considered how it may be difficult to anticipate what the authoritative assessment may be, and how such a difficulty my lead to self- or collateral censorship, given one's inability of anticipating the legal evaluation effect of one's action. It seems that such a difficulty may be even greater when the right to be forgotten is at issue, since even when there is an agreement on the existence of such a right with regard to a certain kind of information, there may be disagreement on when and how the switch point is reached where privacy interests outweigh processing interests.

An additional reason for indulging in self- and collateral censorship, in the case of the right to be forgotten is provided by the special sanction for the violation of this right. According to Article 79 (5) (a) anyone who violates the right to be forgotten[18] would be subject to the sanction of Article 79 (5), namely "a fine up to 500 000 EUR, or in case of an enterprise up to 1% of its annual worldwide turnover". In addition the violator would have to compensate the damage suffered by the data subject, according to Article 77 (1).[19]

Assuming that individual uploaders would be viewed as controllers, the provision in Article 79 (5), threatening such a high penalty for the refusal to take down illegal information would probably induce uploaders to capitulate to any request to remove information unwanted by the concerned data subject, whenever there is even a minimal risk that the information will be considered to be illegal. This would entail a serious impairment to freedom of expression. Uploaders would face the choice between yielding to the request, or risking the penalty in case they were unable to satisfy the authorities that (a) they had posted the data "solely for journalistic purposes or the purpose of artistic or literary expression," and (b) in the particular case freedom of expression should prevail over data protection,

[18] Article 79 (5) (a): "Anyone who, intentionally or negligently ...does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17."

[19] Article 77 (1): "Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered."

according to the proportionality assessment we have described. In fact for the party who would like to distribute the information, the removal request modifies the equation: before the request, the uploader had to consider only the chance of having to pay a compensation in comparison of the advantages (personal or public) involved in distributing the information; now he has to face the chance of paying a compensation plus the chance of being punished against the advantages of distributing the information. It appears that the sanction introduces a there is a severe risk of over-deterrence.

Let us also assume that in case a piece remains on line after the request to be removed, the uploader will have to pay a compensation c_d plus a fine f_d, while if the piece remains on line the user will gain a benefit b_d (including both the individual gain obtained by the user by leaving the piece on line, and the motivational influence on his or her of the social outcome so obtained). As above let $p(i_d)$ be the probability that the piece will be considered to be illegal. Given this arrangement, if the user leaves the piece on line, his or her expected loss is $(c_d + f_d) * p(i_d)$, while the expected gain is b_d. So, the expected outcome (gain minus loss) is $b_d - (c_d + f_d) * p(i_d))$. If the uploader decides to take off the piece, the outcome is 0, no gain and no loss. Clearly, the user will leave the material on line only when $b_d - (c_d + f_d) * p(i_d)) \geq 0$. Then the higher the sanction, the lower the probability of illegality that justifies taking down the material. For instance assume that the sanction is 10 times the damage which would be caused by distributing the information in case it were illegal and that such damage is equal to the benefit (1) the user will obtain by keeping the information on line. Then the users would be motivated to keep the information on line only when $1 - (1 + 10) * p(i_d) \geq 0$, i.e., when $p(i_d) \leq \frac{1}{11}$, i.e., when the user believes that there is than a 1/10 chance that the material is illegal.

If additionally also providers were viewed as controllers, then according to 17 (1) the data subject could asks the host provider to remove allegedly infringing data uploaded by individual users. In case the data were not removed, the provider would face not only civil liability, but also, the sanction of Article 79 (5). To avoid risking the sanction, providers would have to engage in censorship whenever they receive a request to erase personal data. In fact, given that the utility the providers obtain from maintaining a particular piece of information on line is usually much lower than the utility the uploader obtains, providers would most often be motivated to take down the information.

For instance assume that as above the sanction is 10 times the damage which would be caused by distributing the information in case it were illegal and that such damage 100 times higher than the benefit which the provider will obtain by keeping the information on line. Then the provider would be motivated to keep the information on line, after the take down request, only when $1/100 - (1 + 10) * p(i_d) \geq 0$, i.e., when $p(i_d) \leq \frac{1}{1100}$, i.e., when the provider believes that there is than a 1/110 chance that the material is illegal.

To illustrate the dramatic effects this might have, consider the application of the right to be forgotten to Wikipedia: all propositions including persons' names would have to be deleted under request by the concerned data subjects. Thus every data subject mentioned in Wikipedia's pages could compel Wikipedia to selectively clean their pages from every statement he or she does not like. To prevent such censorial excesses, I think that providers should be should be exempted at least from the administrative sanctions when maintaining on line illegal content while believing in good faith that such content is (possibly) legal.

On the contrary, if providers were considered only as processors, they would not be subject to the administrative sanctions for not complying with the right to be forgotten, which apparently apply only to controllers. Under this interpretation, providers would only run the risk of having to compensate the damage according to Article 77 (1), which is complemented by the provision of 77 (3), which excludes liability "if the controller or the processor proves that they are not responsible for the event giving rise to the damage."

7. Conclusion

It seems to me that the Regulation provides for a significant progress on data protection with regard to user-generated data. While enhancing the protection of data subjects, the regulation puts on-line freedom of speech on a safer ground, by clarifying that providers' immunities introduced by the E-Commerce Directive also apply to data protection. However, I think that an adequate discipline for the hosting of user-generated data, which pays due attention to on-line freedom of speech, would require some modifications.

First of all it should be clarified that providers are not data controllers, when they neutrally process user-generated data. Under such conditions, users-uploaders should considered to be the only controllers.

Moreover, providers should not be liable for keeping data on line when they believe in good faith that the data might be legal, and no competent authority has yet ordered the removal. This could be complemented by designing a notice and take down procedure where also uploaders are given the chance to express their view, and data protection authorities have the power to express a binding (though presumptive, being subject to judicial review) assessment of illegality.

Finally, the sanctions for the violation of the right to be forgotten should be reconsidered with regard to both providers and individual users. In particular, the administrative sanction of Article 79 (5) should be limited to cases where the injunction of a data protection authority is disregarded, since the threat of such a serious punishment, under conditions of uncertainty, is likely to have a chilling effect on freedom of speech, forcing providers into collateral censorship.

References

Balkin, J. M. (2008). The future of free expression in a digital age. *Pepperdine Law Review 36*, 101–18.

Benkler, Y. (2011). A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate. *Harvard Civil Rights-Civil Liberties Law Review*.

De Hert, P. and V. Papakostantinou (2012). The proposed data protection regulation replacing directive 95/46/EC: A sound system for the protection of individuals. *Computer law and security review 28*, 130–42.

Gettier, E. (1963). Is justified true belief knowledge? *Analysis 23*, 121–3.

Goldman, A. (1999). *Knowledge in the Social Word*. Oxford: Oxford University Press.

Grimmelmann, J. (2009a). The Google dilemma. *New York School Law Review*, 939–50.

Grimmelmann, J. (2009b). Saving Facebook. *Iowa Law Review 94*, 1137.

Haack, S. (1993). *Evidence and Inquiry*. Oxford: Blackwell.

Hylton, K. N. (2007). Property rules, liability rules and immunity: An application to cyberspace. *Boston University Law Review 87*, 1–39.

Kuner, C. (2012). The European Commission's proposed Data Protection Regulation: A Copernican revolution in European data protection law. *Privacy and Security Law Report, 11*, 1–15.

Lemley, M., D. S. Levine, and D. G. Post (2011). Don't break the Internet. *Stanford Law Review Online 64*, 34.38.

Lemley, M. A. (2007). Rationalizing Internet safe harbors. *Journal on Telecommunication and High Technology Law 6*, 101–19.

Lichtman, D. and E. A. Posner (2006). Holding Internet service providers accountable. *Sup. Ct. Econ. Rev. 14*, 221.

Mayer-Schoenberger, V. (2009). Delete: The Virtue of Forgetting in the Digital Age. Princeton University Pres

Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online 6w*.

Sartor, G. and M. Viola de Azevedo Cunha (2010). The Italian Google-case: Privacy, freedom of speech and responsibility of providers for user-generated contents. *International Journal of Law and Information Technology*, 1–23.

Sartor, G. (2010). Doing justice to rights and values: teleological reasoning and proportionality. Artificial Intelligence and Law, 18:175–215.

Sartor, G. (2013). The logic of proportionality: Reasoning with non-numerical magnitudes. German Law Journal. Forthcoming.

Spindler, G., G. M. Riccio, and A. Van der Perre (2006). Study on the liability of Internet intermediaries. Markt/2006/09/E. Service Contract ETD/2006/Im/E2/69.

Viola de Azevedo Cunha, M., L. Marin, and G. Sartor (2012). Peer-to-peer privacy violations and ISP liability: Data protection in the user-generated web. *International Data Privacy Law*, 1–18.

Authors contacts:

Giovanni Sartor

European University Institute of Florence

Villa Schifanoia

Via Boccaccio 121

50133 Florence (FI)

Italy

Email: Sartor Giovanni <giovanni.sartor@gmail.com>