Privacy Belts on the Innovation Highway

Maria Grazia Porcedda, Primavera de Filippi

Privacy Belts on the Innovation Highway[1]

Maria Grazia Porcedda
Primavera De Filippi

With this paper, we wish to analyse the supposedly conflicting relationship between privacy/data protection and innovation on the Internet, in the context of cloud computing and big data. On the one hand, we try to untangle the different claims relating to the relationship between privacy/data protection and innovation, along with the regulatory options available to address each of the claims. While some believe that privacy/data protection cannot co-exist with innovation, and others that the former will always prevail over the latter, both seem to lead to the conclusion that online privacy is dead.
However, and on the other hand, we claim that there is a way to reconcile the two by intervening at the level of business practices, physical design & networked infrastructure, and IT systems. We suggest that 'privacy belts' – a feature inspired by the idea of the Internet as a highway of innovation – could be used to regulate the sector in ways that satisfy the varying needs of users, while nonetheless allowing service providers to innovate.

Keywords: big data, cloud computing, data protection, innovation, privacy.

---

[1] *This paper was published in the Proceedings of Internet, Politics, Policy 2012: Big Data, Big Challenges?*, Oxford Internet Institute, University of Oxford, 20-21 Septembre 2012

1. Introduction

In this paper, we would like to take you on an explorative 'trip on the innovation highway': an Internet characterized by creative services such as those based on cloud computing and big data. [2]
Innovation based on users' data raises questions as to the extent to which regulation should determine the degree of informational privacy, or the protection of personal data, of users online. The attempts to offer the highest degree of protection to users online, and users' freedom to enjoy innovative services as they see fit (reflected in the differing views of the authors), seem to clash. In our figurative trip, whose meaning will be unveiled at destination, we question whether there is a dichotomy between innovation online and users' rights to privacy and data protection. In order to explore and elaborate upon all different points of view, we frame the problem as a zero-sum game: while, on the one hand, cloud-based services and big data applications increasingly encroach on the right to privacy and data protection, on the other hand, privacy and data protection laws are said to restrain the operation of many innovative techniques and applications. We unpack the trade-off from all angles, and frame the analysis of the supposedly conflicting relationship between privacy/data protection and innovation in the context of cloud computing and big data from a European Union (EU) regulatory perspective (although we also refer to the United States (US) as major creator of services).

In our opinion, the current economic crisis urges this reflection, since boosting ICT-driven innovation is seen as an important tool to spur growth.[3] Yet, policy-makers acknowledge that innovation cannot be fostered at any cost: the "economic and social benefits of the digital market" (European Commission 2010b) must be sustainable, and this includes ensuring the respect for privacy and data protection.[4] This paper presents the results of our analysis, based on the belief that innovation can, and should, coexist with the safeguard of privacy and data protection, understood as fundamental rights. We present our conclusions building on and adding to existing strategies and tools - such as Privacy by Design (hereafter PbD) and Privacy Enhancing Technologies (hereafter PETs) - through

[2] Big data was the focus of the event for which this paper was drafted, the Internet Politics Policy 2013 event organized by the Oxford Internet Institute.
[3] Indeed, in the European Union (EU), innovation is one of the five pillars of the European Union 2020 Strategy for growth (European Commission 2010a). Innovation is broadly understood as including "both search-driven innovation and innovation in business models, design, branding and services that add value for users (…)." (European Commission, 2010c, 7).
[4] The Digital Agenda is one of the many initiatives (European Commission 2010c) of the European Union 2020 Strategy for growth. See at: http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_en.htm.

the metaphor of 'privacy belts' inspired by the (long-established) idea of the Internet as a highway to innovation.

The article is organized as follows. Section 2 provides a definition of the core concepts and terms used throughout the paper. Section 3 illustrates the perspective whereby privacy and innovation stand in a zero-sum relation: if innovation prevails, privacy is necessarily infringed; alternatively, there can be no room for innovation. Section 4 illustrates the perspective whereby there is no trade-off between privacy and innovation, because innovation will always find new ways to overcome privacy legislation, leaving users with the burden to protect themselves. In section 5, we present our own opposite vision: privacy and innovation can actually co-exist online and should in fact be integrated in such a way as to support (rather than thwart) each other.

2. Definitions of terms

2.1 Privacy and Data Protection

In the EU constitutional landscape, privacy and data protection are two intertwined fundamental rights enshrined in the European Charter of Fundamental Rights.[5] The former protects individuals' private and family life (hence relations), private dwellings and communications via any medium, while the latter safeguards the processing of data carrying information relating to identified or identifiable individuals (i.e. personal data).[6] The boundary between these two rights is, however, blurred. It could be said that privacy strictly relates to the person, her body and surroundings, whereas data protection is concerned with the protection of information relating to a person and parcelled into data. The two overlap whenever the improper handling of personal information affects private life as defined in the copious case law of the European Court of Human Rights; moreover, data protection is a proxy to protect rights such as freedom of thought and religion, expression, and non-discrimination (Poullet and Rouvroy 2009; Rodotà 2009). Many scholars are striving to define the boundaries between these two rights (Gutwirth et al. 2013; Porcedda et al. 2013;) focussing on the 'attributes' or substantive dimensions of fundamental rights may help clarify the

[5] Respectively article 7 and 8 thereof.
[6] A datum could be understood as a vehicle carrying personal information, and as such can be seen as a separate entity from the person it relates to.

differences (Porcedda 2013).[7] Such a task is, however, beyond the scope of this paper.

The conflation of the two rights arises perhaps from the fact that data protection was born out of the right to privacy and is thus far only recognized in the EU, whereas many characteristics relating to data protection are attributed to (informational) privacy elsewhere.[8] In the United States, where many innovative companies are based, there is no right to data protection (despite it being the country of origin of the Code of Fair Information Practices, Gellman 2012); informational privacy is mainly intended as a consumer issue, based on the conception of data as property.[9] Conversely, in the EU, privacy and data protection, underpinned by the universal values of dignity and autonomy, are considered crucial for the free development of individuals in a democratic society (Poullet and Rouvroy 2009).[10] The concern of the legislator is therefore self-explanatory (and with it, the opposition between the EU and the US approaches).

2.2 Innovation: Cloud Computing and Big Data

To date, there is no widely agreed definition of innovation.[11] Here, we refer to innovation as "the introduction or combination of new or pre-existing processes, products or services, with a view to translating them into commercial outcomes." We shall briefly define cloud computing and big data before describing where their innovative value lies.

---

[7] For example, health-related information can be seen both in terms of privacy (physical integrity), and data protection (sensitive data); the two are connected, but are not the same thing. The improper use of health data affects the physical and mental integrity of the individual, as well as one's confidentiality of communications, which are all dimensions of privacy. As for data protection, an improper use of data can impact on procedures relating to information parcelled into data, such as legitimacy and security of the processing, all dimensions of data protection.

[8] This is reflected in the jurisprudence of the Court of Justice of the European Union, as well as the Court of Human Rights, which eschew providing a clear definition of the two rights (Court of Justice of the European Union 2008a, 2008b, 2009).

[9] See Richard A. Posner (1978), "The Economic Theory of Privacy", *Regulation,* Vol. 9, n. 3, pp. 19-26.

[10] The system of protection of (informational) privacy is analysed in various ways in the course of this paper.

[11] Schumpeter describes innovation as "the introduction of new elements or a new combination of old elements in industrial organizations" (Schumpeter, 1934), while Nedis and Bylerin define it as "the ability to take new ideas and translate them into commercial outcomes by using new processes, products or services in a way that is better and faster than the competition" (Nedis and Bylerin in European Commission 2009, 3).

Briefly, cloud computing consists of delivering computing resources, storage capacity and software applications as a service rather than as a product.[12] By analogy with the electrical grid (Kushida et al. 2011), resources in the cloud are dynamically "rented out" to consumers according to real-time demand, so that only actual consumption is paid for. Cloud computing allows for hardware resources and software applications to be added or updated at any moment without users' intervention (Armburst et al. 2009; ENISA 2010; Grossman 2009; Miller 2009; Pallis 2010; Marston 2011). This necessarily implies that users are expropriated of control, with mixed consequences. On the negative side, the internal procedures of the cloud are obscure to most users. On the positive side, users are relieved of configuring their software or setting up their own devices, since everything is taken care of automatically through the cloud platform.

As for big data, the term was first used in science to refer to large data sets requiring the processing capacity of supercomputers (Boyd and Crawford 2011). Today, it essentially refers to the aggregation of massive stacks of data originating from different sources, produced by humans or machines (Lohr 2012). As a general rule, big data can be collected from users, either directly by requesting information to be provided in order to use the platform, or indirectly, by sieving open data or monitoring online users ' preferences and activities (through cookies or more questionable practices such as deep-packet inspection[13]). Data can also be obtained indirectly, by sale or through the provision of services based on the processing of such data, from third parties or data brokers.[14]
Yet, beyond the quantitative element, what distinguishes big data from any other data sets is a crucial qualitative aspect, namely the combination and integration of different types of data into one large set of networked or linked data (Boyd and Crawford 2011). The advantage over processing different data sets separately is the ability to find correlations and infer additional information by aggregating, comparing, or otherwise analysing data combined into a single, large data set.

Although theoretically distinct, in practice, cloud computing technologies and big data are often connected and generally feed into each other. On the one hand, cloud-based services heavily contribute to data proliferation, while also providing

[12] Following a widely accepted definition, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Grance and Mell 2010).
[13] The use of deep packet inspection (DPI) for behavioural advertising could be fraudulent. However, given the complexity of DPI as an enabling technology, the topic is too large to be treated in this paper. See Porcedda et al. (2013).
[14] Data brokers are intermediaries whose assets and goods are the data (Federal Trade Commission 2012).

the necessary computing resources for data processing and analysis to anyone lacking in-house server capacity. On the other hand, big data increases the profitability (to providers), as well as the appeal (to users) of many cloud-based services, in a way that we explain below.

2.3 Where the value lies: information extracted from data

What is valuable about data is not each *datum*, but the information that can be extracted from them at the aggregate level, when processed into meaningful information or data-derivatives representing patterns, thanks to recent developments in data mining and analysis (Philip Russom, 2011).[15] Data analysis tools[16] (and the personal data they process), such as sense-making technologies, allow the extraction of significant value and "make sense of observational space" from what might have previously been considered insignificant user data (Cavoukian and Jonas 2012). Activities such as tagging, correcting, reviewing or linking data together, as well as enhancing data with metadata, contribute to both improving the overall quality of data (Cavoukian and Jonas 2012) and facilitating its subsequent processing and integration.

The databases resulting from such processing are profitable in at least three ways: they can be sold, inform the development of new products and services, and allow generating profits from these services, such as in the case of cloud services. Cloud operators capitalise on the collection, aggregation, integration and processing of data coming from many different sources, for the delivery of a more personalized product (i.e. personalised selection of content, recommendation systems, or customized search algorithms), whose value for the interested consumer is much higher than if they were each offered as a stand-alone service, that evolves according to user's preferences and behaviour (De Filippi and Belli 2012). Clearly, the greater the amount of data collected by or about users, agents, devices and the interaction between them, the more accurate (and hence the more valuable) will be the information that can be derived from it. Companies thereby acquire a better understanding of their user-base, and can thus offer a more personalized service, enabling users to disclose information more easily, in an endless "data cycle".

---

[15] This is, indeed, the reason why certain countries (in the EU, in particular, with the implementation of the European Directive on the protection of databases) have enacted legislation aimed at extending the sphere of intellectual property rights to protect the content of large databases whose production required an important investment. While mere data is actually excluded from the scope of protection, the new regulatory framework introduced a sui-generis right on the extraction or reutilisation of a substantial amount of data (big data).

[16] Data analysis tools abound. For an overview, see at http://www.gmw.rug.nl/~huisman/sna/software.html.

As the economic value of personal data (units and aggregates) increases for innovative cloud service providers, users are encouraged to provide growing amounts of (personal) information: the imperative seems to be that 'if data is valuable, it must be exploited'. With the economic potential of big data becoming increasingly apparent, the industry's[17] demand for data management and analysis is soaring. Large companies such as Oracle, IBM and Microsoft are substantially investing in the development of ever more sophisticated data analysis tools (The Economist 2010).

The conspicuous downside is that users incur the risk of losing control over their personal information (Clarke and Stavensson 2010; ENISA 2010; Gayrel et al 2010; Gellman 2009; Hustinx 2010; Leenes 2011). Furthermore, these practices are likely to infringe upon users' privacy and data protection, especially when online firms rely on business models such as behavioural advertising. (Bryant et al. 2008; Chester 2012; Castelluccia 2012; Article 29 Working Party 2011b).

3. The Privacy vs. innovation trade-off

Many innovative online services provided (apparently) for free can both benefit their users and seriously affect their rights to privacy and data protection. The issue has been widely addressed (Chester 2012; Nissenbaum 2011a and 2011b; OECD 2011; Poullet and Rouvroy 2009; Rodotà 2009; Randal et al. 2008), but opinions of privacy advocates diverge from those of service providers as regards the solution. In this section, we voice the regulatory options addressing the privacy vs. innovation trade-off from two *drastically opposed* perspectives: one claiming that privacy needs to prevail over innovation, the other claiming that innovation will always prevail over privacy. While, in practice, many regulatory solutions will situate themselves on a continuum between these two standpoints, the underlying idea is that innovation cannot harmoniously co-exist with the fundamental rights to privacy and data protection, since one is necessarily harming the other.

3.1 The privacy standpoint

[17] In the EU regulatory framework, these include both Internet Service Providers (ISPs) and Information Society Services (ISSs). However, with a view to simplify the analysis, the term 'service provider' will be used in its generic sense.

The privacy extreme of the dichotomy is that the only way for privacy to be preserved is to rein in, or even "kill" innovation, because the benefits deriving from the use of cloud platforms and the processing of users' big data are outweighed by the ensuing challenges to privacy and data protection principles.[18] Such challenges having been widely analysed elsewhere, we shall focus on one example, namely users' consent,[19] which constitutes, in many instances considered here, the only legitimate ground for the processing of personal data (for other grounds of legitimacy, see art. 7 (a) of Directive 95/46/EC). Indeed, the law requires data controllers and processors to obtain explicit, unambiguous and genuine consent from the data subject, who must be properly informed of the specific purposes of data collection. Hence, both authorization by use (on a take-it-or-leave-it basis) and the mere provision of information (such as a privacy notice hidden at the bottom of a web-page) are not deemed sufficient to meet the legislative requirements of consent (Article 29 Working Party 2011a and 2011b). We return to this point in section 5.

These requirements intend to foster user control from both a procedural dimension (transparency of the data practices) and a temporal dimension (appropriate timing for seeking consent). Yet, in the cloud, both dimensions are undermined in various related ways. Data harvesting practices are usually opaque, i.e. invisible to users, and can only be prevented or minimized by installing appropriate software, such as cookie-blockers and Java-script debuggers (Castelluccia 2012). Users' capability to keep track of how – and by whom – personal data is being processed or collected is further undermined by the myriad of data brokers and intermediaries involved in a variety of data transfers, resulting not only from company transfers and mergers, but also from commercial sales. While such practices are often reported in the (often lengthy and convoluted) privacy policies of many cloud operators, they are, however, generally difficult to understand. Besides, many cloud operators rely on social engineering techniques to encourage users to consensually provide personal information, or to accept data-sharing settings by default (OECD, 2011), without properly informing them of the above-mentioned practices.[20] In addition, consent is often violated indirectly, whenever users using cloud-based social media and participative Web 2.0 platforms publish, sometimes unlawfully (Court of Justice of the European Union, 2003),

[18] On the topic, see Taipale (2005).

[19] Under article 2(h) of Directive 95/46, consent is "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

[20] An example is Facebook's recently added personal information banner, which encourages users to add information about their past and present personal lives to their profiles.

information about third parties - which inevitably provides new material for data harvesters.

These practices can affect various tenets of privacy and data protection (i.e. the right to access, rectification, deletion and redress). Moreover, personalised outputs are obtained through the profiling, or categorisation, by service providers of the user-base, resulting from the secondary processing of big data collected or inferred about them. While supporting several legitimate applications, such as "better market segmentation, permitting an analysis of risks and fraud, or adapting offers to meet demand by the provision of better services […] profiling an individual may result in unjustifiably depriving her or him from accessing certain goods or services and thereby violate the principle of non-discrimination" (Council of Europe 2010).

In the US, where privacy protection is sectoral and piecemeal[21], (Newman 2008), users are often targeted with personalized advertisements and tailored political ads (Leber 2012; Bott 2012). User profiling has also led to exclusion (e.g. from credit and insurance companies) and loss of jobs. Besides, user profiles are sometimes shared with law enforcement agencies, potentially endangering the liberties of individuals whose profiles might suggest criminal behaviours (Vance and Stone 2011; Scheinin 2007).

As of today, the universe of data brokers has become so complex - and their impact so great - that policy makers cannot avoid looking into it anymore (Marked 2012). Yet, according to some, the consequences of innovation are so nefarious for privacy and data protection that one should simply renounce it altogether. This is the "keeping off the Internet" approach.

3.2 The Industry standpoint

Conversely, from an 'extreme' industry perspective, privacy and data protection laws constrain the deployment of innovative services based on the harvesting of personal data, such as many 'social' cloud-based services, which encourage users to disclose personal data and share it with their peers. Indeed, data analysis and integration leading to customization and personalization could not be easily

[21] Unfortunately the analysis of the system of protection of privacy in the United States is beyond the scope of this paper, and thus there is no room to review sectorial laws (such as Electronic Communications Privacy Act, the Children's Online Protection Act, or the Fair Credit Reporting Act), and the role of responsible agencies beyond the work of the Federal Trade Commission. For a comparison of the system of (informational) privacy protection in the EU and the US, see Newman (2008) and Nissenbaum (2011a).

achieved in a stringent data protection regime, which would ultimately prevent users from fully enjoying the potential of their services. Hence, many believe that the overhaul of the data protection framework in the EU (European Commission 2012), and the Federal Trade Commission proposal for a Bill of Privacy Rights in the US (White House 2012) are too stringent and thus likely to harm technological innovation (Chester 2012; Gellman 2012).

In the United States, for instance, the industry strongly criticized the plan to waive the requirement of consent only if the collection of personal data is "consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law" (FTC 2012, 7; Gellman 2012).

In the EU, online service providers are criticizing the proposed Data Protection Regulation (European Commission 2012) on grounds of its unreasonable provisions as to consent, data retention, the right to be forgotten and administrative burdens. First, online service providers lament the burdensome obligation to inform users as to when – and why – data is collected, and the prohibition to process personal data without obtaining the explicit consent from the data subject, in the light of the real-time data collection and the chain of data brokers characterizing data collection; online service providers foresee that constantly asking permission would be a mere annoyance for users.[22] Second, one single intermediary can hardly ensure the proposed limited data retention period, and the 'right to be forgotten' that is the prompt deletion of data upon user's request whenever there are no legitimate reasons for retaining it (Lindsay 2012), given the pace of data transfers and sales. Third, the same applies to the proposed right to data portability, that is, the right to transfer data from one service to another, which promotes interoperability and reduces the odds of lock-in. Finally, online service providers are lamenting the introduction of a mandatory data protection officer, along with the obligation to draft privacy impact assessments, as this would divert investments from innovation.[23]

The Data Protection Regulation is still in a draft form, and thus it is too early to provide a proper assessment here. Yet, (as it currently stands) it is regarded by online service providers as a draconian measure (Blume 2012), which might

[22] Under the proposed Data Protection Regulation, "freely given, specific and informed" consent will no longer be sufficient, consent will also have to be "explicit" and evidenced by "a statement or by a clear affirmative action".

[23] See at http://www.huntonprivacyblog.com/2012/06/articles/uk-ministry-justice-outlines-negotiating-position-european-commissions-proposed-regulation/.

discourage the development of innovative services that would ultimately benefit users through better personalisation and improved functionalities (Laursen 2012).

If privacy and innovation cannot coexist, users must decide whether they prefer privacy without innovation, or innovation without privacy. Online service providers claim that most Internet users prefer the latter, thus announcing the imminent death of online privacy and data protection.

4. Innovating against privacy

For others, the effect of privacy law on innovation is the opposite, and thus there is no trade-off. Stringent privacy and data protection laws constitute a driving force for Internet operators to innovate with new business models and fast-evolving technologies, which the law is unable to keep up with.

4.1 The Industry bypassing the rules

In order to further its interests and maximize its profits, the industry has ultimately to meet (or spur) the demands of the user-base. Yet, increasingly stringent privacy and data protection laws constraining the deployment of personalized services and innovative features might actually encourage the most innovative businesses to bypass, or simply ignore the law, in order to keep serving (or enticing) their user-base. This is particularly relevant in the context of big data, whose value lies in the attribute of 'relationality', that is in 'linked data'.[24] While users might have explicitly agreed to the processing of their personal data by one specific party and for a specific purpose, more comprehensive aggregations of data are likely to require personal data transfers or exchange across different services, potentially resulting in secondary processing that users may have not agreed to (De Filippi and McCarthy 2012).

Consider, for instance, the case of Google, which changed its privacy policy in March 2012 with a view to aggregating personal data from all its services into a single database, so as to build detailed user profiles. Although Google extensively notified its users of the upcoming changes, the new policy has been strongly criticized by privacy advocates and consumer groups, who accused Google of

[24] With Big Data, the added value is obtained by aggregating different types of data extracted from different sources, connecting them together with other pieces of data about the same users, different users, users they are in connection with, or the whole community of users to which they belong.

failing to obtain the proper consent of its user-base, and of purpose creep.[25] Yet, Google's new privacy policy nonetheless came into force – for the sake of clarity, Google claimed – in spite of the European Union's request to delay the implementation, pending further investigations.[26] This led the Article 29 Working Party to subsequently request Google to amend its privacy policy (Pfanner and O'Brien 2012).

In a similar fashion, the outrage and investigations concerning Google Street View's surreptitious collection of personal data can be regarded as an instance of the company's disregard for EU law. A report by the CNIL (2011) demonstrates in fact that the collection of data by Google's city-mapping vehicles was not an inadvertent mistake by a few employees, but was rather a well-orchestrated program, which many people inside the company were perfectly aware of (Streitfeld and O'Brien 2012; Arthur 2012).

Facebook is another company often criticised and taken to court for bypassing data protection/privacy regulations, such as in the recent case of "sponsored stories,"[27] which informed the class action *Fraley v. Facebook, Inc*., (2011). Sponsored stories are automatically generated by an algorithm that infers a user's affinity with a particular good or service – mostly resulting from the use of the "like" button – and consist in advertising such products to one's Facebook's friends by means of a personalized endorsement (i.e. one's name and likeness), paid for by third party companies (advertisers or sellers). Although sponsored stories are explicitly mentioned in Facebook's Terms of Use, such Terms were scattered, complex, contradictory[28] and did not have to be agreed or read by users (who were in any case not notified of such new feature), thus seriously questioning the validity of users' consent (and Facebook's conduct).[29] Following the settlement of the class action, Facebook must allow users to visualize all posts displayed in Sponsored Stories and, eventually, to prevent these stories from being shown any longer.

---

[25] After investigations, the French data protection authority (CNIL) claimed that Google's new privacy policy does not satisfy the requirements of the European Data Protection Directive and should therefore not be implemented without first being amended.

[26] Following CNIL's analysis, EU Justice Commissioner Vivian Reding requested Google to delay the implementation of its new privacy policy in order to investigate whether it was indeed compatible with European law.

[27] http://www.facebook.com/ads/adboard/?type=stories.

[28] While an external Facebook page suggested that the creations of such stories from posts could be prevented, users could not opt out from "sponsored stories" (Fraley v. Facebook, Inc., 2011).

[29] Although the Court endorsed the newsworthiness doctrine argued by Facebook, it rejected Facebook's motion to dismiss under the notion that newsworthy actions used for commercial purposes are subject to liability (Frankel et al. 2012).

This behaviour does not only attach to the usual suspects, *i.e.* Google and Facebook. In 2008, Internet access providers in the UK planned to use the company Phorm to serve behavioural advertisement to users in the United Kingdom based on deep packet inspection, a technique consisting in scanning the payload of the packet, which carries the content of the communication (Mueller 2011). The practice is unlawful in most cases not just under data protection laws, but could be easily seen as such from most countries' constitutional perspective (Berners-Lee 2009). While outcry obliged Phorm to offer opt-out solutions to such type of advertisement (Cellan-Jones 2008), such behaviour revealed a widespread approach to bypassing the rules (as well as the more general issue of deep packet inspection).

Also smartphone applications (apps) often represent means for circumvention. Carnegie Mellon University researchers conducted a study on the data collection practices of 56 of the most common smartphone apps.[30] Surprisingly, some popular apps collected users' geo-location data, their devices' unique identifier and list of contacts in opaque or secret ways. Angry Birds, produced by Rovio Entertainment, is a case in point. Their lengthy privacy policy, which is more of a "disclaimer than a choice" (O'Brien 2012), suggests that if users "want to be certain that no behaviourally targeted advertisements are not displayed to you, please do not use or access the services" (ibid.).

4.2 The industry making the rules: code is law

In some cases, innovation can drastically change the technological landscape, thereby invalidating what previously appeared to be a technologically neutral regulatory framework (Porcedda 2012a).
One of the fundamental characteristics of cloud computing is that service providers acquire complete control over all data (personal or not) directly yielded by users, or indirectly communicated through their uses and behaviours (De Filippi and McCarthy 2011). Indeed, in the cloud, every activity and operation can be monitored, tracked and – most importantly – every user can be identified according to her past, present, and future behaviour. In spite of the advantages it might offer in terms of data availability and accessibility, the cloud has become increasingly immune to the law, since it has rendered obsolete most of the rules relating to data control, transfer and accountability (Bollier 2010; Porcedda 2012).

[30] The study included reactions of users to the data collection practices. http://confabulator.blogspot.it/2012/11/analysis-of-top-10-most-unexpected.html.

The inherently dynamic and evolving character of cloud computing also raises the issue of assessing the limits of data retention and the scope of purpose limitation from a privacy and data protection perspective. Indeed, the elasticity and scalability of the cloud implies a constant re-allocation of resources, which depends on actual needs. As a result, some of the internal operations of the cloud require logging and monitoring users' activities. While this is not a problem *per se* – as log-keeping is considered a good practice for procedural security (article17 of Directive 95/46/EC), sometimes even required by data protection laws (Barcelò 2009)– it is often difficult to draw a clear line between what constitutes legitimate data processing and what does not, without reasoning on the admissibility and limits of practices carried out in the cloud and with big data.

Hence, in many circumstances, rather than following privacy rules, innovative firms, such as Google and Facebook, adopt a 'do-it-first-and-see-what-happens' approach. They set their data practices and related privacy policies independently of the law and wait for people's reaction to determine whether or not they will be accepted. Yet, social media, and social networks in particular, drastically promoted data sharing on the Internet: users are increasingly willing, or enticed, to disclose personal information online – regardless of the extent to which such information can be subsequently accessed or processed by third parties. Given the growing urge to share personal data with friends and acquaintances, users will rarely stop and think about the privacy implications of using a certain infrastructure for communication over another (Cranor et al. 2010).
Although on grounds different from those described in section 3, the argument whereby the law bypassed legislation also leads to the conclusion that "the age of privacy online is over". Users must choose between basic or uninteresting services that comply with the law and innovative services which have no – or little – privacy safeguards. However, as opposed to the former view (according to which privacy law constitutes an obstacle to innovation), advocates of this view see privacy and data protection laws as an actual driver for innovation. Yet, they consider that strong privacy protection will most likely spur bad innovation, encouraging companies to find new ways to bypass the restrictions imposed by the law through the development of new tools that will further endanger the privacy of end-users. The fear is that innovative companies will dictate the terms of use of their services, imposing upon users the acceptance of privacy conditions far less protective than those prescribed by laws.[31]

[31] However, these practices can (sometimes) be blocked by other bodies of law - such as competition law or consumer protection law - which can be used as a means to prevent other companies from following the same trend.

4.3 Users' response to bad innovation

In such circumstances, the only option left to users is to defend themselves by means of specific software and hardware devices designed to counteract attacks to privacy suffered while wandering online. Yet, this is a costly option, clearly applicable only to a minority of tech-savvy and expert users. For all the others, taking part in the innovation feast will mean observing powerlessly the infringement of their rights to privacy and data protection.

5. Privacy and innovation

The increasing data collection and integration linked to cloud computing and big data, as well as the growing phenomenon of users voluntarily making their data publicly available– which is blurring the distinction between public and private information – bring about the need to re-evaluate how privacy and data protection can be safeguarded online. Possible solutions are those offered by the privacy vs. innovation dichotomy or trade-off. If one necessarily impinges on the other, users must eventually decide whether they prefer: (a) maintaining control over personal information at the cost of renouncing to most innovative cloud-based services; or (b) enjoying a (highly) personalized service based on sharing or disclosing a certain degree of personal information, at the cost of jeopardizing one's privacy.

Our view is that the privacy vs. innovation trade-off is a false dichotomy, and that it is possible to enjoy both privacy and innovation at the same time. Indeed, the two might support rather than impinge on each other, in a virtuous circle whereby privacy demand pushes for protective innovation, with the early support of the law, as we argue below. On the one hand, the law could encourage the development of privacy enhancing technologies (PETs) designed to safeguard users' fundamental right to privacy, without negatively affecting the quality of the service provided (European Commission 2007). On the other, it could foster the incorporation at an early stage of privacy into the design and operation of computer systems and networks such as cloud computing and big data systems. This is the idea behind the seven principles of "privacy by design"[32] (Cavoukian; EDPS 2010), which are a strong answer to the privacy/innovation trade-off, provided these principles do not become an empty checklist for regulatory compliance (Diaz et al. 2011).

[32] The seven principles are available at: http://privacybydesign.ca/about/principles/.

To work properly, privacy by design has to be applied to three distinct but interrelated business fields: (1) accountable business practice, (2) physical design and networked infrastructure and (3) IT systems.[33]

5.1 First step to accountability: transparency of business practices

Rather than a lack of care for privacy from the part of users, a pivotal problem of privacy and innovation (particularly in cloud computing and big data), is users' unawareness of the (obscure) practices relating to the use of personal data provided to innovative services, which undermines businesses' accountability. In other words, users are generally not aware that many of the services they use, albeit apparently free, are paid for with a different type of currency: the provision of personal data. Users are not paying for the product – they are the product being sold.

The first step to address most online privacy concerns is to require cloud/ big data operators to provide *proper information* to their users, as mandated by the regulatory framework on consent and as a basis of accountability. There is, of course, an inherent conflict of interests for big data and cloud computing service operators. Indeed, if their goal is to collect as much personal data as possible, transparency could eventually harm their interests, by creating a more privacy-aware user-base, which might, in certain cases, oppose these practices. The result is epitomized in simple 'notice and consent', the obscure and ineffectual privacy policies hidden on the services' website that conceal the power imbalances between users and service providers. Hence, following Nissenbaum's reasoning (2011a), we suggest to abandon the principle of 'notice and consent' in favour of a two-step approach.

First, service providers should offer clear and short, but nonetheless complete notices, written in layman's terms (akin to those offered in open source services[34]), which users cannot skip and necessarily have to accept at the time of starting to use the service. Such notices should include links to easily understandable, detailed and objective information relating to the data practices of the service providers. Borrowing from the idea of 'contextual privacy' proposed by Nissenbaum (2010a) and the FTC (2012),[35] such notices would ideally be

---

[33] Ibid.

[34] That is, software released under a specific licenses stipulating that the source code of the software must always be made available to the public.

[35] Nissenbaum suggests that privacy 'online' should be read through the lens of privacy 'offline', by following a contextual approach. In fact, 'code is law' only to a certain extent; it is like gravity, and the rest is up to us. Therefore, online contexts corresponding to the offline ones should be regulated similarly; otherwise, offline proxies should be found for new online contexts, suggesting regulatory paths (Nissenbaum 2011b).

drafted by a multi-stakeholder group composed of regulators, private actors and members of civil society involved in a particular field of business (i.e. the music industry, the film industry, or social networks etc.).
Second, those who are reaping the benefits of the processing of personal data (whether it is the service providers or the States in which they operate) should provide proper education in order to help users understand the risks of improper data processing practices. For instance, an often neglected, yet important issue concerns the security of cloud-based services and its interconnectedness with privacy (Friedman et al. 2012; Porcedda 2012b). The media increasingly report cloud-related data breaches (a recent example of cloud's failure can be found at Honan 2012), without necessarily emphasizing that this might lead to privacy infringements (Porcedda 2012b).[36]

5.2 Offering choice: Privacy-compliant technical infrastructure

It goes without saying that proper information has to be complemented by an appropriate technical infrastructure. Only if provided with the right information and the proper technical tools can users have the final say as regards the precise level of privacy they aspire to. In the context of cloud computing, this means offering multiple and meaningful privacy settings which protect users' personal data by default and a series of tools allowing users to escape from profiling or monitoring practices (e.g. opt-in as opposed to opt-out, track-me-not choices, etc.). Privacy settings should be positioned to the highest by default.

Yet, we also believe that experienced users (who are aware of the risks and content to agree to the rules of the cloud operator) should have the freedom to choose the service they prefer. While they should not be surreptitiously redirected from the safe to the unsafe platform, it should be nonetheless easy for users to enjoy the benefits of a service with the lowest privacy settings – if they so wish.
In other words, privacy settings should be easy to change (reduce); moreover, choosing the parameters should be akin to allowing individuals to negotiate the terms of service (Nissenbaum 2011b). Instead of current practices based on opting-out from data collection, we advocate a strictly opt-in approach to data collection and processing. Borrowing from Nissenbaum's proposal for "expressive choice", we suggest that every cloud platform implement privacy by design by automatically triggering the applicability of "reasonable expectations of privacy" (or claims to having one's privacy and data protection respected),

[36] The security of personal data is an essential component of data protection (laws) leading to online privacy, and is a consumer's prerogative for any online service (Hopkins 2012; Porcedda 2012b).

transforming consent into a means preventing circumvention of users' choice (Nissembaum, 2011b). Other noticeable initiatives are protocols for portability of informed consent, relating in particular to research in health, and institutional technology assessment as a substitute for consent when individuals have practically no contractual power (Porcedda 2013).

5.3 Building privacy belts into IT systems

If users' devices are completely exposed to potential offenders, all efforts to protect users' safety and security through proper information and technical infrastructure will be diminished. Hence, in order to safeguard privacy, users' devices need to be endowed with built-in protective features, such as firewalls, anti-viruses/spyware, content encryption (at least for sensitive data) and protective internet settings, which should be turned on by default, and very easy to use (De Filippi and Bourcier 2011; Porcedda 2012b).

Coming back to the title of our paper and our figurative journey, this is akin to producing cars with built-in safety belts and airbags to ensure drivers' safety in case of accidents. Some decades ago, many cars did not have safety belts, and only some offered them as optional, despite the fact that such feature could have avoided severe injuries or even deaths – particularly in connection with the front passenger's seat, hence called "death seat".[37] Yet, as more companies started offering cars with safety belts as a feature, they eventually became a standard, which is now required by law (Bilton 2012). The same analogy could be drawn in the case of privacy and data protection. Indeed, several companies are now offering alternative services or devices that respect users' privacy (i.e. data vaults). We expect and hope this trend to continue, as privacy and data protection are progressively being regarded as a socially desirable and useful means to foster competition in the market for cloud services. If drivers do not want to wear safety belts, they do so at their own risk; such should be the case for users wearing 'privacy belts'.

Some could argue, based on case law concerning the relationship between privacy and the obligation to wear safety belts (European Court of Human Rights, 1979 and 1993), that this is not the case. In the judgment *X vs. Belgium* (1979), the European Commission of Human Rights rejected an application concerning the alleged violation of private life resulting from a fine for not wearing safety belts *rationae materiae*, as the contested fact was outside the scope of article 8 ECHR. In fact, the Commission noted that the imposition to wear safety belts intended "to

[37] The development of this analogy was inspired by a fruitful conversation with Professor Richard Jones (University of Edinburgh), to whom we are therefore indebted.

protect the public from various dangers and as a consequence protect society against the harm".[38] A similar conclusion was reached in the case *Schmautzer vs. Austria* (1993) on the same grounds.

Nowak (2005) contested such conclusions, arguing that harming oneself is a dimension of privacy as "self-determination" (the Commission declined to interpret the expression 'private life'). We agree with this view, as we believe that customers should not have the burden to protect themselves – rather, they should make a conscious and well-informed effort for putting themselves at risk.

Such argument is compelling if one observes that major online service providers (i.e. Google, Amazon, Microsoft and Apple) that dominate the market for online services are increasingly leveraging their dominance into complementary markets, through the sale of non-interoperable user devices (i.e. Amazon's Kindle, Apple's Ipod and Ipad, Microsoft's Zune, etc.) whose functionalities are, to a large degree, dictated by service providers themselves. This creates a situation of oligopoly, as users are left with little choice concerning the service or the device they use, and absolutely no chance to negotiate the terms and conditions of the selected services. The regulator should swiftly address such landscape to counter distortion of the incentives and competition.

We think that the right to privacy should be regarded as informational self-determination – a fundamental right that should be protected *by default* to preserve the public interest, but that encompasses the choice to renounce protection, provided it constitutes a free and informed choice, with full understanding of all possible related consequences. Hence, we believe that the law should impose the provision of 'privacy belts' (computer privacy and security settings) that should be worn by default (in terms of service's privacy settings) because of the value inherent in the privacy (life) of the users (drivers). As a general rule, users should have a claim to privacy protection, and – in case of an adverse event – they should be eligible for damages. Yet, if users decide not to 'wear' privacy belts (i.e. to change their own security/privacy settings), their claims to privacy would change, akin to losing the insurance privileges in case of

[38] The European Commission of Human Rights further argued, "This for example is the position with regard to the safety appliances…and numerous other measures of individual or collective protection adopted in the public interest. The compulsory wearing of safety belts by the drivers and passengers of motor-vehicles, the effectiveness of which is proved by numerous authoritative statistics, is a measure of this type. In the Commission's opinion they in no way affect a person's "private life", however broadly this expression is interpreted" (1979, p. 258), which in fact the Commission declined to do.

an accident (i.e. no claim for compensation), or incurring a fine (i.e. being held liable).

6. Conclusion

We have now reached the final destination of our road trip on the innovation highway, which we hope was helpful to readers to clarify the intricacies of the relationship between privacy and innovation in the context of cloud computing and big data. We presented the perspectives of those who believe that there is an inherent conflict between privacy and innovation, which can only be resolved by one taking over the other. On the one hand, privacy-minded but inexperienced users may eventually give up enjoying the benefits of innovative services in order to avoid excessively exposing themselves – since protection is currently only available to those possessing the proper know-how and adequate devices. On the other hand, service and device providers are either struggling to keep minimal legal guarantees as regards privacy and data protection, or simply decide to ignore them (e.g. with a 'do-it-first-and-see-what-happens' approach), responding to the attempts at increasing protection by circumventing the law with innovative tools. In both cases, privacy is bound to lose; but so is *bad* innovation. We believe that the dichotomy between privacy and innovation is false, and that privacy laws may actually foster *good* innovation through the creation of innovative services which can provide a personalized and customized experience to their users (if they wish so) but only insofar as the degree of privacy is customizable (with simple settings ranging from the highest to the lowest) and is backed up with appropriate technological measures to enforce those settings (as illustrated in section five).[39]

To us, informational privacy and data protection are not dead; their focus might, however, need to be adjusted to the online environment, by putting particular emphasis on the notion of choice concerning the collection and processing of personal data, including the disclosure thereof, provided a number of caveats are respected. The user must properly understand the impact of sharing information with one service or another, must be fully endowed with all necessary tools to protect or remove protection, and be well informed of the alternatives - that is, the user *has alternatives*, and this is where the law must come into place.

---

[39] For instance, Cavoukian and Jonas (2012) have recently demonstrated how privacy can be embedded in sense-making technologies, which are used in the context of big data, based on the following steps: 1) full attribution; 2) data tethering; 3) analytics on anonymized data; 4) tamper-resistant audit logs; 5) false negative favouring method; 6) self-correction false positives; 7) information transfer accounting.

We insist on the notion of 'alternatives'. The idea of 'privacy belts' on the 'innovation highway' came to us as a wider metaphor (which might draw interesting parallels between the evolution of road safety and security and the recent developments in privacy and data protection laws). We thought that the current situation online resembles that of a panoramic road (innovation) depicted by road signs (information notices) as fun and safe. Yet, when one starts driving (surfing) on it, one discovers that it is a bumpy road without guardrails (insecurity of the Internet and services), infested by aggressive merchants (advertisers) and thieves (cyber-criminals), and that to drive on it one needs an armoured car (device). While one user may be aware of the conditions of the road, prepared to drive on it and enjoy it, another user may be inexperienced and lacking the appropriate vehicle (with some correspondences with the beliefs of the flesh and bone writers). We thought that for each destination there should be two roads: one safe, if dull, the other fun, if risky. Road signs should appropriately signal the conditions of the road and the vehicle needed to enjoy the experience; all vehicles should have embedded safety add-ons to make driving safer.
Likewise, the legislator should mandate the provision of information, and impose embedded safety/security standards upon the producers of devices. As for the services, the law should provide for minimum standards of privacy/data protection (opt-in, track-me-not, highest standard by default, *ex ante* technology assessment), akin to providing two alternatives for the same services, respecting the choices and preferences of different kind of users. The rest should be left to a truly competitive market, where there is as much symmetric information as is humanly possible. At the time of writing the Prism program, i.e. the processing of big data partly collected from cloud-based services by the US National Security Agency, has been unveiled. A whole different paper would have to be written about the use of big data generated from cloud computing by law enforcement agents. Yet, the revelations have sparked the demand for services that ensure higher privacy and data protection.[40]

While most of our policy recommendations draw on previous concepts and techniques (such as PbD, PETs, etc.) that have been developed and elaborated over the past twenty years, our contribution to the state of the art lies in the proposed implementation of these tools. Indeed, while they have received strong support from the public, and have been, thus far, endorsed by several institutions and policy makers, most of these concepts actually failed to be implemented or adopted in practice. We are, nonetheless, convinced that those principles are key to the establishment of a trusted online environment, where users do not have to feel their rights being threatened by innovative services. It is, in our view,

[40] See at http://uk.reuters.com/article/2013/06/17/uk-cloud-europe-spying-idUKBRE95G0FM20130617.

extremely important – in these challenging times of big data and cloud computing - to support and reiterate these principles, even though they might need to be slightly revisited to comply with emerging online practices and evolving user's preferences or behaviours. To us, past failures should not be regarded as a defeat, but rather as an experience to learn from, so as to elaborate (by means of trial and errors) a smart approach that is more likely to succeed in today's online environment. We proposed a possible approach to reconcile online privacy and innovation in ways that do not excessively hinder the interests of online operators or end-users.

By relying on the concepts of information notices (akin to 'proper road signs'), alternative services ('safe/risky roads for the same destination') and 'privacy belts', we have (hopefully) shown that it is possible to address online privacy concerns by fostering innovative business models that give users the choice to step up or surrender their privacy for the sake of a more personalized service, if (and only if) a number of important caveats are respected. Yet, further research in the field is needed: this is only the beginning of a long journey.

7. References

Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Konwinski Andrew, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia. 2009. "Above the Clouds: A Berkeley View of Cloud Computing." University of California, Berkeley Technical Report # UCB/EECS-2009-28.

Arthur, Charles. 2012. "Google's problem is that it now believes itself above others – even governments." *The Guardian*, May 1. http://www.guardian.co.uk/technology/2012/may/01/google-street-view-data-fcc?INTCMP=ILCNETTXT3487.

Article 29 Data Protection Working Party. 2012. "Opinion 05/2012 on Cloud Computing". (WP 196), Brussels.

Article 29 Data Protection Working Party. 2011a. "Opinion 15/2011 on the Definition of Consent." (WP 187), Brussels.

Article 29 Data Protection Working Party. 2011b. "Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising." (WP 188), Brussels.

Barcelo, Rosa. 2009. "EU: Revision of the ePrivacy Directive." *Computer Law Review International* 5: 129 – 160.

Berners-Lee, Tim 2009. No Snooping. www.w3.org/DesignIssues/NoSnooping.html

Bilton, Nick. 2012. "Disruptions: And the Privacy Gaps Just Keep On Coming." *The New York Times*, February 19 http://bits.blogs.nytimes.com/2012/02/19/disruptions-and-the-privacy-gaps-just-keep-on-coming/?ref=technology.

Blume, Peter. 2012. "Will it be a better world? The proposed EU Data Protection Regulation." Oxford Journals: Oxford University Press.

Bollier, David (Rapporteur). 2010. "The Promise and Peril of Big Data." The Aspen Institute, Communications and Society Program, Washington DC.

Bott, Ed. 2012. "Is Facebook damaging your reputation with sneaky political posts?" *Zdnet.com*, July, 12. http://www.zdnet.com/is-facebook-damaging-your-reputation-with-sneaky-political-posts-7000000828/.

Bowker, Geoffrey C. 2005. "Memory Practices in the Sciences." MIT Press: Cambridge, Massachusetts.

Boyd, Dana and Kate Crawford. 2011. "Six Provocations for Big Data." Paper presented at the Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" (September 21, 2011).

Bradshaw, Simon, Christopher Millard and Ian Walden. 2010. "Contracts for Clouds: A Comparative Analysis of Terms and Conditions for Cloud Computing Services." Queen Mary School of Law Legal Studies Research Paper n. 63/201.

Bryant, Randal E., Randy H. Katz and Edward D. Lazowska. 2008. Big-Data Computing: Creating revolutionary breakthroughs in commerce, science, and society.

Castelluccia, Claude. 2012. "Behavioural Tracking on the Internet: A Technical Perspective." In *European Data Protection: In Good Health? Eds. Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet*. Springer, 21-34.

Cavoukian, Ann, and Jeff Jonas. 2012. "Privacy in the Age of Big Data." http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf.

Cavoukian, Ann. "Privacy by Design. The Seven Foundational Principles." http://privacybydesign.ca/about/principles/

Cellan-Jones, Rory (2008). Web creator rejects net tracking. *BBC News*, March 17. http://news.bbc.co.uk/2/hi/technology/7299875.stm

Charter of Fundamental Rights of the European Union. OJ C 364, 18.12.2000, 1–22.

Chester, Jeff. 2012. "Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the "Big Data" Era." In *European Data Protection: In Good Health?* Eds. Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet. Springer, 53-78.

Clarke, Roger, and Dan Stavensson. 2010. "Privacy and Consumers Risks in Cloud Computing." *Computer Law and Security Review,* 26 (4): 391-397.

Commission Nationale de l'Informatique et des Libertés (CNIL). 2011. "Google Street View: CNIL pronounces a fine of 100,000 Euros."<http://www.cnil.fr/english/news-and-events/news/article/google-street-view-cnil-pronounces-a-fine-of-100000-euros/>.

Communication from the Commission. 2010d. "A Comprehensive Approach on Personal Data Protection in the European Union." COM (2010) 609 final.

Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). OJ C 83, 30.3.2010.

Council of Europe. 2010. Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling. CM/Rec(2010) 13.

Court of Justice of the European Union. 2003. Case C-101/01 Criminal Proceedings against Bodil Lindqvist. Judgement of November 6th.

Court of Justice of the European Union. 2008. Case C-73/07, Tietosuojavaltuutettu v. SatakunnanMarkkinapörssiOy, SatamediaOy, Judgement of December 16.

Court of Justice of the European Union. 2008. Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, Judgment of January 29.

Court of Justice of the European Union. 2010. Joined Cases Volker und Markus Schecke GbR (C.92/09) and Hartmut Eifert (C.93/09), Judgment of the Court (Grand Chamber) 9 November 2010

Cranor, Lorrie Faith, Joseph Reagle and Mark S. Ackerman. 2010. "Beyond Concern: Understanding Net Users' Attitudes about Online Privacy." In *The Internet Upheaval raising questions seeking answers in communications policy*, eds. Ingo Vogeslang and Benjamin M. Compaine.

De Filippi, Primavera and Luca Belli. 2012. "The Law of the Cloud v. the Law of the Land: Challenges and Opportunities for Innovation." *European Journal of Law and Technology*, 3 (2).

De Filippi, Primavera and Smari McCarthy. 2011. "Cloud Computing: Legal Issues in Centralised Architectures", *Proceedings of the VII International Conference on Internet, Law and Politics.* Barcelona.

De Filippi, Primavera and Danièle Bourcier. 2011. "Cloud Computing: New Research Perspectives for Computer & Law", in *Proceedings of the 13th International Conference of Artificial Intelligence & Law*, eds. Casanovas, Ugo Pagallo, Palmirani, Giovanni Sartor. Springer.

De Filippi, Primavera and Smari McCarthy. 2012. "Cloud Computing and Data Sovereignty." European Journal of Law and Technology, 3 (2).

Diaz, Claudia, Seda Gu¨rses and Carmela Troncoso. 2011. "Engineering Privacy by Design." K.U. Leuven/IBBT, ESAT/SCD-COSIC. <http://homes.esat.kuleuven.be/~cdiaz/>.

Diffie, Withfield, and Susan Landau. 2008. "Internet Eavesdropping: A Brave New World of Wiretapping." *Scientific American Magazine*.

European Commission. 2007. Communication "Promoting Data Protection b Privacy Enhancing Technology (PETs)." COM (2007) 228 final.

European Commission. 2009. Communication "Reviewing Community innovation policy in a changing world." COM (2009) 442 final.

European Commission. 2010a. Communication "Europe 2020. A strategy for smart, sustainable and inclusive growth." COM (2010) 2020 final.

European Commission. 2010b. "A Digital Agenda for Europe." COM (2010) 245 final/2.

European Commission. 2010c. Communication "Europe 2020. Flagship Initiative Innovation Union" COM (2010) 546 final, SEC(2010) 1161.

European Commission. 2012. "Proposal for a Regulation 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). COM (2012) 11 final.

European Court of Human Rights. 1979. Application No. 8707/79, X. vs. Belgium, European Commission of Human Rights, Decision of Admissibility, December 13th.

European Court of Human Rights. 1993. Application No. 15523/89, SCHMAUTZER vs. Austria, European Commission of Human Rights, Decision of Admissibility, May 10th.

European Data Protection Supervisor (EDPS). 2010. "Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (Opinion on Privacy By Design)." OJ C 280, 16.10.2010, 1–15.

European Network and Information Security Agency (ENISA). 2009. "Cloud Computing, Benefits, Risks and Recommendations for Information Security."

European Parliament and Council. 1995. *Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. OJ L 281, 23.11.1995, p. 31-50.

Federal Trade Commission. 2012. Recommendations for Businesses and Policymakers. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

Fraley v. Facebook, Inc. 2001. U.S. District Court, Northern District of California (San Jose). No. 11-CV-01726-LHK, 2011 WL 6303898. Dec. 16th.

Frankel, Simon J., Laura Brookover and Stephen Satterfield. 2012. "Famous for Fifteen People: Celebrity, Newsworthiness, and Fraley v. Facebook." *Stanford Law Review* 64 (82).

Friedman, Allan F. and Darrell M. West. 2010. "Privacy and Security in Cloud Computing." *Issues in Technology Innovation*, 3.

Gayrel, Claire, Jacques Gérard, Jean-Philippe Moniy, Yves Poullet and Jean-Marc Van Gyseghem. 2010. "Cloud Computing and its Implications on Data Protection." Paper for the Council of Europe's project on Cloud Computing. Namur: Centre de Recherche Informatique et Droit. <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf>.

Gellman, Robert. 2009. "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing." Paper prepared for the World Privacy Forum.

Gellman, Robert. 2012. "Fair Information Practices: a Basic History." http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

Grance, Tim and Peter Mell. 2009. "The NIST Definition of Cloud Computing." Version 15, <http://csrc.nist.gov/groups/SNS/cloud-computing/>.

Grossman, R. L. 2009. "The Case for Cloud Computing". *IT Professional*, 11 (2): pp. 23-27.

Gutwirth, Serge, Gloria Gonzàles Fuster, Ivan Sz´ekely and Erik Uszkiewicz. 2013. "Discussion paper on legal approaches to security, privacy and personal data protection". PRISMS Project, Deliverable 5.1.

Honan, Mat. 2012. "How Apple and Amazon Security Flaws Led to My Epic Hacking." *Wired*, August, 6. http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/.

Hopkins, Nick. 2012. "Cyber security should be promoted with hard-hitting ad campaign, says Labour." *The Guardian*. May 15. http://www.guardian.co.uk/technology/2012/may/15/cyber-security-ad-campaign-labour.

Hustinx, Peter. 2010. "Data Protection and Cloud Computing under EU Law." Speech delivered at the Third European Cyber Security Awareness Day, Brussels.

Kushida, Kenji, Jonathan Murray and John Zysman. 2011. "Diffusing the Fog: Cloud Computing and Implications for Public Policy." University of California, Berkeley, BRIE Working Paper # 197.

Laursen, Lucas. 2012. "Privacy Laws Turn Europe into Economic Laboratory." *MIT Technology Review*, June 20, http://www.technologyreview.com/news/428051/privacy-laws-turn-europe-into-economic-laboratory/.

Leber, Jessica. 2012. Campaigns to Track Voters with "Political Cookies". *MIT Technology Review*, June 27. http://www.technologyreview.com/news/428347/campaigns-to-track-voters-with-political-cookies/.

Leenes, Ronald. 2010. "Who Controls the Cloud?" *Revista de Internet, Derecho y Politica,* 11.

Lindsay, David. 2012. The Emerging Right to be Forgotten in Data Protection Law: Some Conceptual and Legal Problems. *Proceedings of IDP VIII Conference*: 420-438.

Lohr, Steve. 2012. "The Age of Big Data." *The New York Times*, February 18, https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?_r=1&ref=technology.

Markey, Ed (Congressman). 2012. "Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information." July, 24. http://markey.house.gov/press-release/bipartisan-group-lawmakers-query-data-brokers-about-practices-involving-consumers%E2%80%99

Marston, Sean, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang and Anand Galsasi. 2011. "Cloud Computing - The business perspective." *Decision Support Systems*, 51 (1): 176-189.

Miller, Michael. 2009. Cloud Computing: Web-Based Applications that change the way you work and collaborate online. Indianapolis: Que Publishing.

Moses, Asher. 2010. "'Petulant' Conroy accuses Google of 'single greatest privacy breach'." *The Sidney Morning Herald*, May 25. <http://www.smh.com.au/technology/technology-news/petulant-conroy-accuses-google-of-single-greatest-privacy-breach-20100525-w937.html>.

Mueller, Milton (2011). DPI technology from the standpoint of internet governance studies: an introduction. Syracuse university school of information studies. http://deeppacket.info.

Newman, Abraham L. 2008. “Protectors of Privacy. Regulating Personal Data in the Global Economy. Ithaca: Cornell University Press.

Nissenbaum, Helen. 2011a. “A contextual approach to Privacy Online.” *Daedalus, the Journal of the American Academy of Arts and Sciences,* 140 (4). http://www.nyu.edu/projects/nissenbaum/.

Nissenbaum, Helen. 2011b. “From Pre-emption to Circumvention: If Technology Regulates Why Do We Need Regulation (and Vice Versa)?” *Berkeley Technology Law Journal* 26 (3).

Nowak, Manfred. 2005. CCPR Commentary, 2nd edition (N.P. Engel). Chapter on Article 17, pp.377-405.

O’Brien, Kevin J. (2012). Data-Gathering via Apps Presents a Gray Legal Area. October 28. https://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personal-data.html

Organization for Economic Co-operation and Development. 2011. “30 years after: the OECD Privacy Guidelines.”

Pallis, G. 2010. "Cloud Computing: The New Frontier of Internet Computing". *Internet Computing, IEEE*, 14 (5): 70-73.

Pfanner, Eric and Kevin J. O’Brien. 2012. “Europe Presses Google to Change Privacy Policy.” New York Times, October 16th 2012.

Porcedda, Maria Grazia. (2013). “Paper establishing classification of technologies on the basis of their intrusiveness into fundamental rights.” Deliverable 2.4, SURVEILLE Project. Florence: European University Institute (forthcoming).

Porcedda, Maria Grazia, Mathias Vermeulen and Martin Scheinin (2013). "Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy." Deliverable 3.2, SurPRISE Project. Florence: European University Institute. Available at: http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE_D3.2_Report-on-regulatory-frameworks-concerning-privacy-for-final-formatting_v094.pdf

Porcedda, Maria Grazia. 2012a. “Law Enforcement Access to Data in the Cloud: is the Data Protection Legal Framework up to the task?” In *European Data Protection: In Good Health?* Eds. Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet. Springer, 203-232.

Porcedda, Maria Grazia. 2012b. “Reviving Privacy: the Opportunity of Cyber-security.” *Proceedings of IDP VIII Conference*: 485-506.

Poullet, Yves and Antoinette Rouvroy. 2009. “The right to informational self-determination and the value of self-development. Reassessing the importance of

privacy for democracy." In *Reinventing Data Protection?* Eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Sjaak Nouwt and Cécile de Terwangne. Springer. http://works.bepress.com/antoinette_rouvroy/7

Rodotà, Stefano. 2009. "Data Protection as a Fundamental Right." In *Reinventing Data Protection?* Eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Sjaak Nouwt and Cécile de Terwangne. Springer.

Russom, Philip. 2011. Big Data Analytics, TDWI best practices report.

Scheinin, Martin. 2007. Implementation of General Assembly Resolution 60/251 of 15 March 2006 entitled "Human Rights Council". Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin. General Assembly. A/HRC/4/26, January 29.

Streitfeld, David and Kevin J. O'Brien. 2012. "Google Privacy Inquiries get little cooperation." *The New York Times*, May 22. <http://www.nytimes.com/2012/05/23/technology/google-privacy-inquiries-get-little-cooperation.html?_r=1&hp&pagewanted=all>.

Taipale, Kim A. (2004). "Technology, Security And Privacy: The Fear Of Frankenstein, The Mythology of Privacy and The Lessons of King Ludd", *Yale Journal of Law and Technology,* 123 (7).

The Economist. 2012. "Data, data everywhere". February 25. http://www.economist.com/node/15557443

Vance, Ashlee and Brad Stone. 2011. "The Company that sees everything." *Bloomberg BusinessWeek*, November 28- December 4.

White House. 2012. "Consumer Data Privacy in a Networked World. A framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.