Privacy Belts on the Innovation Highway

Primavera De Filippi (PhD, CERSA, CNRS)
&
Maria Grazia Porcedda (LL.M., EUI)

Paper prepared for the Conference "Internet, Politics, Policy 2012"
Oxford Internet Institute,
September 21-22 2012
(policy track)

Abstract

With this paper, we wish to take you on a road trip on the 'innovation highway' - a rough metaphor we propose to analyse the supposedly conflicting relationship between privacy/data protection and innovation in the context of cloud computing and big data.
We think that, today, innovative services based on cloud computing technologies and big data can be compared to roads, described as stunning and entertaining, but also dangerous (unsafe and unsecure), filled with bandits or street vendors eager to attack unprepared drivers travelling along the way.
The preferences of two imaginary travellers, Alice and Bob, will help us untangle the different claims relating to the relationship between privacy/data protection and innovation: some believe that one cannot co-exist with the other, others that the latter will always prevail over the former.
We claim, however, that there is a way to combine the two. Whether you are an inexperienced driver with an unsafe vehicle (Bob), or an experienced driver looking for an exciting drive through a panoramic road (Alice), you should be able to reach the same destination without losing control over your personal data or putting your privacy at risk.
We suggest that 'privacy belts', and a number of other road metaphors, 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. Introduction

In this paper, we would like to take you on a road trip on the innovation highway. Our imaginary travellers, Alice and Bob, want to reach the same destination, but have different driving skills and preferences. Alice is an expert driver and likes panoramic roads. Bob does not drive confidently, and prefers less exciting but safer roads. Yet, in the current context, the final destination can only be reached in one way: through a private road, which is depicted as a beautiful, fun and safe place. Checkpoints are located at the entrance and at the exit of that road, in order to monitor and record the traffic, along with a large number of remote-control cameras. The road is stunning, as it overlooks the sea, but there are neither guardrails nor asphalt and the terrain is bumpy; an off-road vehicle is necessary to drive through it. The road is fun and interesting, as you can get to know many people along the way; yet some are bandits eager to rob you, others are vendors in disguise, who will not let you go until you have bought some of their merchandise. To escape them, you need to drive fast, and possibly have an armoured vehicle. Yet, not all vehicles are apt to this task; some do not even have safety belts or airbags.

Alice adores this road. She enjoys the beautiful landscape and she hardly gets bothered by the myriad of thieves, bandits or merchants populating the road, since her vehicle is well protected. Bob does not have an adequate vehicle and does not feel safe on that road. He thus decides to stay home, but nonetheless complains to the authorities requesting the construction of a new road. He also advocates for raising the minimum standards of road safety, thereby making the panoramic road unavailable to the public - an option that would make Alice deeply unhappy.

Authorities' opinions as to the possible solution differ. Some believe Bob's desire for safety is incompatible with Alice's preference for adventure. If the two cannot be satisfied, either Bob has to give up travelling, or Alice has to give up adventure. A first option is to preserve the status quo (thus favouring Alice's over Bob's) by keeping the panoramic road in its current state and letting road owners dictate the conditions for usage. A second option (favouring Bob's over Alice's preferences) is to impose conditions and safety standards, which have to be met by every road owner. Yet, road owners argue that, since drivers keep coming on dangerous roads, they are actually happy with the service and would not be prepared to incur the costs arising from additional safety standards. Consequently, some members of the authorities fear that road owners will be tempted to circumvent legislation and/or surreptitiously build new streets by their own standards. Thus, regardless of the safety rules, drivers willing to shield themselves from dangers and annoyances will be forced to defend themselves by their own means (i.e. by travelling in off-road, armoured cars).

This metaphor is used to roughly illustrate the current struggle between privacy and innovation in an Internet dominated by cloud computing and big data. In our metaphor, the road is the technical infrastructure of innovative businesses based on cloud computing and big data, and directions are the information provided to the user as regards the characteristics of those services and businesses. On the Internet, entry or exit checkpoints are implemented either by the service providers asking for authentication or directly by the government. The vehicles are users' devices (computers, smartphones, tablets, consoles, etc.), whereas bandits are the cyber-criminals robbing drivers of their data, and vendors are the service providers and advertisers trying to sell their products. Finally, safety and security standards are the equivalents of privacy and data protection (regulations). Following this analogy, we encounter a similar dilemma as the one illustrated before. On the one hand, new services, technologies, and software applications based on cloud computing and big data increasingly encroach on the right to privacy and data protection. On the other hand, privacy and data protection laws could restrain the operation of many innovative techniques and applications.

Our objective is to analyse the (supposedly) conflicting relationship between privacy, data protection and innovation in cloud computing and big data from a European Union (EU) regulatory perspective, in order to determine whether they can co-exist on the Internet. Discussing this topic is both timely and relevant from a policy perspective, especially now that boosting ICT-driven innovation is seen as an important tool to foster growth. Indeed, in the European Union (EU), innovation is one of the five pillars of the European Union 2020 Strategy for growth (European Commission 2010a), a document that sparked several initiatives[1] (European Commission 2010c), such as the 'Digital Agenda for Europe' (European Commission 2010b), which is specifically aimed at reaping the "sustainable economic and social benefits of the digital market" while boosting innovation and fostering citizens' trust in the digital market by ensuring the respect for privacy and data protection.

The interaction between privacy, data protection and innovation will be analysed throughout the paper by means of our road metaphor, which we hope will help clarify our argument (although we are conscious that the metaphor has its limits, and can be improved). Bob and Alice's contrasting needs represent the dilemma we intend to untangle, and the authority's options represent our different lines of analysis. Section 3 illustrates the view of those who believe that privacy and innovation stand in a zero-sum game: if privacy wins, there can be no innovation; alternatively, if innovation prevails, there can be no room for privacy. Section 4 illustrates the view of those who believe that innovation will always find new ways to overcome privacy law, leaving to users the burden to protect themselves.

[1] See at: http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_en.htm.

As opposed to these two views, we believe instead that privacy and innovation can co-exist and be integrated, as illustrated in section 5. To discover how, we invite you to join us on a road trip on the innovation highway.

2. Definitions of terms

Before analysing the different regulatory solutions to solve Bob's and Alice's struggle, we should first clarify some of the concepts used in this paper.

2.1 Privacy and Data Protection[2]

In the context of EU law, privacy and data protection are two intertwined fundamental rights enshrined in the European Charter of Fundamental Rights.[3] The former protects individuals' private and family life, home and communications, while the latter safeguards 'information relating to identified or identifiable individuals' processed for specified purposes; in other words, it relates to the use of data carrying information relating to individuals.[4] Hence, privacy has a 'bodily or physical' dimension lacking in data protection, but data protection is a proxy to protect rights such a freedom of thought and religion, expression, and non-discrimination. (Poullet and Rouvroy 2009; Rodotà 2009).
Yet, the boundary between these two rights is blurred and the two overlap whenever the improper handling of personal information affects informational privacy (roughly, communications or private life). Such confusion arises perhaps from the fact that data protection was born out of privacy and is EU-specific, whereas many characteristics relating to data protection are attributed to (informational) privacy elsewhere.[5] In particular, in the United States, where

[2] In our analogy, privacy and data protection refer to the security and safety of the drivers. As such, they concern both the vehicles (the devices used) and the services offered (the quality and 'policing' of the road). In the following sections, the enforcement of these two rights will be contrasted with the ability of Internet service providers (ISPs) to use personal data as 'raw material' to offer increasingly personalized or customizable products or services, in other words to innovate, with cloud computing technologies and big data.

[3] The Charter of Fundamental Rights of the European Union introduced a distinction between the fundamental right to privacy (Article 7) and the fundamental right to the protection of personal data (Article 8). The latter has been subsequently recognized by the European Court of Justice, in the Satamedia and Promusicae Cases (Court of Justice of the European Union 2008a and 2008b).

[4] A datum ould be understood as a vehicle carrying personal information, and as such can be seen as a separate entity from the person it relates to.

[5] This is reflected in the jurisprudence of the Court of Justice of the European Union, which has only recently acknowledged the right to data protection as defined in the Charter in the cases Satamedia and Promusicae, but seems still uncertain as to the content of the right.

many innovative companies are based, there is no right to data protection (despite it being the country of origin of the Fair Information Principles, Gellman 2012) and informational privacy is mainly intended as a consumer issue, based on the conception of data as property. 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 - and citizens - in a democratic society (Poullet and Rouvroy 2009). 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[6]

There is no widely agreed definition of innovation. The term has been variously described as "the introduction of new elements or a new combination of old elements in industrial organizations" (Schumpeter, 1934), or "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) In the EU, innovation is broadly understood as including "both research-driven innovation and innovation in business models, design, branding and services that add value for users (…)." (European Comission, 2010c, 7) For the purpose of this paper, innovation will refer to pioneering the introduction in research and organizational practices of new processes, products or services, or the combination of existing ones into new results, with a view to translating them into commercial outcomes, with specific focus on cloud computing technologies and big data. The EU is indeed heavily relying on cloud computing and big data to boost competition and innovation.
In a few words, Cloud Computing can be described as a new business model based on delivering computing resources, storage capacity and software applications as a service rather than as a product.[7] By analogy with the electrical grid (Kushida et al. 2011), resources in the Cloud are dynamically provided to consumers according to real-time demand. Instead of being purchased, the necessary hardware and software applications are actually rented by the clients,

[6] In our metaphor, innovative services based on big data and cloud computing represent the infrastructure or the highway where users 'circulate', with the corresponding services they offer to their drivers. In this context, an important element is the quality of the infrastructure, as well as the availability of alternative infrastructures. Yet, innovation also applies to the users' devices (vehicles), as we will clarify later on.

[7] According to the United States National Institute of Science and Technology (NIST) 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).

who pay for the actual consumption only. This greatly reduces the upfront investments of online businesses or start-ups, while simultaneously minimizing the risks and the impact of any potential failure. One of the strongest appeals of the Cloud is that it allows hardware resources to be added and software applications to be updated at any moment without requiring any kind of intervention from users (Armburst et al. 2009; ENISA 2010; Grossman 2009; Miller 2009; Pallis 2010; Marston 2011). While this naturally implies that the internal procedure of the cloud are obscure to users, it also means that users can benefit from a more customized and personalized service, based on the data collected (or inferred) about them (De Filippi and Belli 2012). Users are thus encouraged to provide an increasing amount of information to online operators, thereby incurring the risk of losing control over their personal data (Clarke and Stavensson 2010; ENISA 2010; Gayrel et al 2010; Gellman 2009; Hustinx 2010; Leenes 2011).

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, the term refers to the aggregation of massive stacks of data originating from different sources, produced by humans or machines (Lohr 2012). While the quantitative element is a necessary defining criterion, it is not sufficient as such. Indeed, what distinguishes Big data from any data sets is a qualitative aspect, namely the combination and the integration of different types of data into one large set of networked or linked data (Boyd and Crawford 2011). As elegantly stated by Geoffrey Bowker, "raw data is both an oxymoron and a bad idea; to the contrary, data should be cooked with care." (Bowker 2005, 183-184). The advantage over processing different data sets separately is that it becomes possible to find correlations and infer additional information by aggregating, comparing, or otherwise analysing data combined into one single large data set.[8]

With the economic potential of Big data becoming increasingly apparent, the industry's 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 tools for improved data collection, aggregation, and analysis (The Economist 2010). A variety of new technologies are being developed to further exploit the value of Big data, namely sense-making

[8] Every day, massive quantities of data are used, reused, integrated, aggregated and processed in such a way as to bring new benefits to users, advertisers, and, naturally, Internet service providers. Data analytics can help users access information more efficiently, it can help advertisers better identify their target and their marketing strategies, and - most importantly for the purpose of this paper - it can be used by large service providers to better understand their user-base and learn from every single user interaction so as to provide a more personalized service to each individual user. For a more detailed overview of the various opportunities offered by Big Data, see the TDWI best practices report on "Big Data Analytics" by Philip Russom, 2011.

technologies which are able to find new data and organize it together in order to "make sense of observational space." (Cavoukian and Jonas 2012).
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 the necessary computing resources for data processing and analysis to anyone lacking in-house server capacity. On the other hand, Big data increases the attractiveness of many cloud-based services by allowing the delivery of a more personalized service that automatically evolves according to each user's preferences. The combination of Cloud computing technologies and Big data can thus be regarded as an innovative business strategy which is slowly becoming pervasive on the Internet network.

2.3 Where the value lies: information extracted from data[9]

Data analysis techniques (and the personal data they process) are not only used to develop new products and services, they have also become a major way to monetize those services. Nowadays, data is being produced ubiquitously, and in large amounts, by social networks, mobile technologies, RFID, the Internet of things, and increasingly also by web communities. As a general rule, data can be collected from users, either directly by requesting information to be provided in order to use the platform, or indirectly, by monitoring user's preferences and activities (through cookies or more illicit practices). Data can also be obtained indirectly from third parties or data brokers.[10]
For most companies, the imperative seems to be that 'if data is valuable, it must be exploited'. Yet, data is not valuable as such, it is the information that can be extracted from that data which is valuable. In an information-driven society, characterized by information overflow, data is useless unless processed into meaningful information or data-derivatives representing patterns at the aggregate level. Recent developments in data mining and analysis have shown that it is possible to extract significant value from what might have previously been considered insignificant user data. Contemporary data-analysis techniques are

[9] In our metaphor, value lays in the relationship that subsists between drivers and road-owners. While the former can benefit from a faster path to a specific destination, or from a beautiful panorama along the way, the latter needs to provide accurate road directions in order to help drivers find their way. Road owners can also extract value from their drivers, either by making them pay a toll to enter the road, or by means of collateral services offered on the road (e.g. gas stations, drive-ins), sometimes connected with illegal practices (e.g. street vendors, bandits, thieves).
[10] Data brokers are intermediaries whose assets and goods are the data (Federal Trade Commission 2012).

based on non-structured data, collected in real-time, organized and linked together in order to obtain an exponential volume of "meaningful" data.
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 and facilitating its subsequent processing and integration. 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 thus acquire a better understanding of their users, a broader overview of their preferences and characteristics, and a wider knowledge base from which to derive information to offer a more personalized service to each and every user (including behavioural advertising), or build new services, thus extracting considerable value. The conspicuous downside is that these practices are likely to infringe upon privacy and data protection regulation, especially when online firms rely on advertising-based business models, (Bryant et al. 2008; Chester 2012; Castelluccia 2012; Article 29 Working Party 2011b).
The goal of our road trip is to show how it is possible to combine the corporate interests of innovative service providers - who are trying to extract value from personal (big) data - and the interests of users – receiving certain services - in a way that protects their fundamental rights to privacy and data protection.

3. The Privacy vs. innovation trade-off

Innovative online services based on the features described above seriously challenge the basic tenets of privacy and data protection. While users are likely to benefit from a more personalized service - apparently offered for free - they should nevertheless be aware of the risks that such service entails. Indeed, as soon as information is turned into currency, privacy is put at risk. The problem has been widely discussed in the literature (Chester 2012; Nissenbaum 2011a and 2011b; OECD 2011; Poullet and Rouvroy 2009; Rodotà 2009; Randal et al. 2008), with divergent opinions as regards the solution.
Coming back to our metaphor, there is an obvious clash between the interests of road owners (acting in order to maximize their profits), the interests of Alice (who wants to have fun on a beautiful panoramic road) and these interests of Bob (who merely wants to reach his final destination safely). Authorities must intervene in order to establish a trade-off between these divergent interests. In this section, we provide an overview of the idea that Bob and Alice's preferences are incompatible: innovation cannot harmoniously co-exist with the fundamental rights to privacy or data protection, since one is necessarily harming the other.

3.1 The privacy standpoint: kill innovation or die

According to a certain number of privacy-minded people, the only way for privacy to be preserved is to limit or "kill" innovation; the benefits deriving from the use of cloud computing platforms and the processing of user data into big data are outweighed by the challenges to privacy and data protection that these services can bring.

One of these challenges is related to a data subject's consent, i.e. "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." (article 2(h) for the Directive 95/46). In many instances considered here, consent is the only legitimate ground for the processing of personal data (art 7 (a) of Directive 95/46), provided that all the criteria of its definition (which have been the subject of precise interpretation) have been respected (Article 29 Working Party 2011a and 2011b). The law requires data collectors (controllers and processors) to obtain explicit, unambiguous and genuine consent of users after they have been directly informed about the specific purposes of data collection. This means that both authorization by use (on a take-it-or-leave-it basis), as well as the mere provision of information (for instance, in the form of a privacy notice hidden at the bottom of the page) are not deemed to meet the legislative requirements of consent (Article 29 Working Party 2011b). The requirements of consent are meant to bring the data subject to a situation of control; this implies both a procedural dimension (transparency of the data practices) and a temporal dimension (appropriate timing for seeking consent) (Article 29 Working Party 2011a).

However, the dimensions of consent are undermined in a number of interconnected ways in the cloud. Data processing practices are usually opaque, i.e. invisible to users' view, and can only be prevented or minimized by installing appropriate software, such as that blocking cookies, beacons and javascript add-ons (Castelluccia 2012). The ability of users to keep track of how their personal data is being processed or collected - and by whom - is considerably jeopardized by the practice of data transfers, not only in the case of company purchases and mergers, but also - and most importantly - in the case of commercial sales, which often includes a myriad of data brokers and intermediaries. While these practices are often reported in the privacy policies of many cloud operators, they are however generally hidden and difficult to understand. As of today, the universe of data brokers has become so complex - and their impact so important - that policy makers cannot avoid looking into it anymore (Marked 2012). Besides, certain cloud operators use social engineering to encourage users to consensually provide personal information, without however properly informing them of the above-

mentioned practices.[11] Social engineering based on behavioural economics also leads users to accept data-sharing settings by default (OECD, 2011). In addition, consent is often violated indirectly, by users using cloud-based social media and participative Web 2.0 platforms to publish information about third parties, which, albeit unlawfully (i.e. the famous case of Lindqvist), inevitably provides free material for data harvesters.[12] Most of these practices have repercussions on other tenets of privacy and data protection, such as the right to access, rectification, deletion and redress. In the context of cloud computing, the use of big data for secondary processing and profiling is amongst the most threatening for privacy and data protection. While it allows service providers to offer a more desirable product with high customization and personalization, categorizing users as a result of collected or inferred information also allows providers to discriminate amongst customers according to the category in which they have fallen - a practice which can have significantly negative impacts on users' rights. As the Council of Europe has recognized in recitals 9 and 10 of the Recommendation on online profiling: "profiling may be in the legitimate interests of both the person who uses it and the person to whom it is applied, such as by leading to better market segmentation, permitting an analysis of risks and fraud, or adapting offers to meet demand by the provision of better services; [however] 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 United States, where privacy protections are less stringent, Internet users are often targeted with discriminatory advertisements, including tailored political ads, (Leber 2012; Bott 2012). In addition to discrimination, profiling might also lead to exclusion (e.g. from credits and insurance) and losses of jobs. Some have argued that many junk mortgages that led to the 2008 economic crisis had actually been sold online, as a result of behavioural advertising (Chester 2012). Finally, data can sometimes be shared with law enforcement agencies, potentially restricting the liberties of individuals whose profiles suggest criminal behaviours (Vance and Stone 2011; Scheinin 2007).

According to this view, the consequences of innovation are so nefarious for privacy and data protection, that one should renounce it altogether. This is the "keeping off the internet" approach, which, in our metaphor, corresponds to Bob's decision of quitting travelling altogether, due to insurmountable concerns in terms

[11] 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.

[12] Finally, the requirement of consent can also be violated - in extreme cases - by data breaches (due to either internal or external factors), which are becoming increasingly common in the context of cloud computing (as a notable example, see the double Sony case in 2011).

of safety (e.g. the bad state of road, the weak vehicle, etc.) and security (e.g. bandits, thieves, etc.).

3.2 The Industry standpoint: kill privacy or die

Conversely, from an industry perspective, the enforcement of privacy laws constrains the deployment of innovative services based on the harvesting of personal data for customization and value extraction. This is the case of many 'social', cloud-based services, where users are encouraged to disclose personal data in order to share it with their peers. Similarly, data analysis and integration leading to new services based on customization and personalization could not be easily achieved in a stringent data protection regime, ultimately preventing users from enjoying in full the potential of those services.

Hence, many believe that the overhaul of the EU data protection framework pursuant to article 16 of the Lisbon Treaty (European Commission 2012), as well as the proposal of a Bill of Privacy Rights made in the US (White House 2012), as formulated by the Federal Trade Commission, are too stringent and thus likely to harm technological innovation (Chester 2012; Gellman 2012).

In the United States, the industry criticized the proposed plan of the Federal Trade Commission to waive the requirement of consent for only five categories of data collections, "that are 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, the situation has become even more drastic with the proposed Data Protection Regulation (European Commission 2012), which broadens the scope of application of a variety of obligations imposed on the operations of ISPs. To begin with, it obliges all ISPs to inform users as to what data is being collected and for what purpose, as well as to obtain explicit consent for the processing of personal data.[13] The problem is that explicit consent is difficult to obtain in real-time data collection, or in subsequent data transfers, at least under current business structure, and continuously asking for user consent is portrayed as a mere annoyance to the user. As for data retention, the proposed Regulation stipulates that collected data should only be retained for a limited period of time, and should be promptly deleted upon user's request. The latter is referred to as the 'right to be forgotten',[14] which is criticized on the grounds that data in the clouds are often

[13] 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"

[14] After having been heavily debated in the past few years, the European Commission's proposal to create a new privacy right - the "right to be forgotten" - has eventually been codified as part of

transferred from one place to another, and from one company to another, thus making it difficult for one single intermediary to ensure the effective deletion of the data. The Regulation also recognizes a right to data portability, according to which users should be entitled to transfer data from one service to another in order to promote interoperability and reduce the risks of user lock-in. Finally, a few operators are lamenting the introduction of a mandatory data protection officer, coming along with the obligation to draft privacy impact assessments.[15]

Although it will not come into effect before 2014 (and it may undergo substantial changes until then), the Data Protection Regulation as it currently stands is regarded as a draconian measure by several ISPs operating in the realm of cloud computing (Blume 2012). According to many online operators, these provisions are likely to discourage the development of innovative services that would ultimately benefit society. Indeed, aggregating data collected from different services could eventually increase the perceived value of each of those services, enhanced with additional customization and improved functionalities (Laursen 2012).

If privacy and innovation cannot coexist, users need to decide whether they prefer privacy without innovation, or innovation without privacy. Supporters of this view claim that users prefer to enjoy the benefits that cloud-based services and big data provide, thus announcing the imminent death of online privacy and data protection. In our metaphor, this corresponds to "eliminating" safety and road regulations, or at least opposing the raising of the minimum security standards that every road owner and vehicle producer has to respect.

4. Innovating against privacy

For others, the effect of privacy law on innovation is the opposite. To the extent that law is unable to keep up with fast-evolving technologies, stringent privacy/ data protection laws can be regarded as a driving force for Internet operators to innovate with new mechanisms that are likely to further violate the privacy of users. The reason is that technology and innovative business models can essentially redefine privacy rules faster than the law can adapt. In out metaphor, this is the position of those believing that Alice will always win and Bob will thus have to learn how to protect himself.

---

the new Data Protection Regulation, allowing users to request the deletion of their personal data whenever there are no legitimate reasons for retaining it (Lindsay 2012).

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

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. However, if legislation is too strict, the industry will be unable to satisfy both the provision of the law and the emerging needs of users. Considering the growing complexity and severity of the legal framework as regards privacy and data protection, the industry is ever more tempted to drive and serve the demands of users with the development of innovative tools and techniques. Although policy-makers try to regulate personal data processing practices, i.e. their collection and use by corporations and businesses, those rules are often bypassed, or simply ignored by most innovative firms. This is particularly relevant in the case of Big data. As explained above, the power of Big Data is not only related to the quantity of data available; it is also - and mainly - related to the 'relationality' of such 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. While users might have explicitly agreed to the processing of their personal data by one specific party and for one or more specific purposes, such a comprehensive aggregation of data is likely to require personal data transfers or exchange across different services, i.e. secondary processing that users may have not agreed to (De Filippi and McCarthy, 2012).

Consider, for instance, the case of Google, whose new privacy policy proposes to aggregate personal data from all Google services into one single database, so as to be able to build a more detailed profile of every one of its users. Although Google extensively notified its users of the upcoming changes, the new policy has been strongly criticized by several privacy advocates and consumer groups - who accused Google of violating data protection laws by extending the purpose of the collection and processing of personal data without having properly obtained the consent of its user-base.[16] In spite of the European Union's request to delay the implementation awaiting further investigation,[17] Google's new privacy policy nonetheless came into force - on the grounds that users would otherwise be confused as to the actual policy of Google.

The recent outrage and investigations concerning Google Street View's surreptitious collection of personal data such as email addresses, passwords, IP

[16] After investigation, 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.

[17] 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 incompatible with European law.

addresses etc. (CNIL 2011), is also easily explained in this light. The related report published at the end of April demonstrates that the collection of such data by Google's vehicles mapping different cities' streets was not due to the decision of a single employee acting in his own capacity; rather, it was a well-orchestrated program, which many people inside the company were aware of (Streitfeld and O'Brien 2012; Arthur 2012).
Another company often criticized for bypassing data protection regulations is Facebook, which has recently been accused of further infringing privacy rights by turning users' comments into "sponsored stories"[18], paid for by the company whose products are being unknowingly endorsed by the user community. These stories are automatically generated by an algorithm inferring users' affinity with one particular good or service (mostly as a result of the "like" button) and re-proposing these products with personalized advertisement to the Facebook's friends of each user. Although users consent to this practice by agreeing to Facebook's Terms of Service, the length and complexity of these terms is likely to impair the validity of such consent. Besides, while they can limit the extent to which their posts can be turned into sponsored stories, users are however not granted the ability to completely opt-out from the program.[19]

4.2 The industry making the rules: code is law.

In other cases, innovative technologies are so radical as to completely change the technological landscape, thereby invalidating what previously appeared to be a technologically neutral regulatory framework (Porcedda 2012a).
Indeed, one of the fundamental characteristics of Cloud Computing is that it requires all data to be exported from a personal device into the Cloud. Even if users do not expressly provide information about themselves, every piece of information that is uploaded into the Cloud becomes available to the service provider(s), who acquire complete control over the data, its uses and its movements. (De Filippi and McCarthy 2011). In the Cloud, each activity can be monitored, each operation performed can be tracked and, most importantly, each user can be identified according to its past, present, and future behaviour. In spite of the advantages the cloud might offer in terms of data availability and accessibility, cloud operators can ultimately bypass the law (Bollier 2010), since

[18] http://www.facebook.com/ads/adboard/?type=stories
[19] Following the settlement of a class action lawsuit against Facebook's use of users' names and images into sponsored stories (Fraley et al v. Facebook, Inc.), Facebook must allow users to visualize all posts displayed in Sponsored Stories and to prevent these stories from being shown any longer.

most of the rules relating to data control, accountability and data transfers have become obsolete in the cloud.

Cloud computing technologies also deprecated rules on consent and purpose limitation - i.e. collection exclusively for a specific, explicit and lawful purpose - enshrined in EU law (but not only). Indeed, the elasticity and scalability of the Cloud implies a constant re-allocation of resources, which ultimately depends on the activities and needs of users. Hence, logging and monitoring user activities is often necessary for the internal operations of the Cloud. This is usually not a problem per se, since logging and monitoring is actually considered good practice for procedural security (i.e. article17 of Directive 95/46/EC) - and sometimes even required by data protection laws (Barcelò 2009). The problem is that it is often difficult to draw a clear line between what constitutes legitimate data processing and what does not. The inherently dynamic and evolving character of Cloud Computing raises therefore the issue of assessing the limits of data retention and the scope of purpose limitation from a privacy and data protection perspective.

In short, it can be observed that, 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 create their privacy policies independently of the law and wait for society's reaction to see whether or not they will be accepted by the masses. Social media, and social networks in particular, drastically influenced the approach of 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 to think about the privacy implications of using a certain infrastructure for communication (social networks, web-based mail and the like) over another (Cranor et al. 2010)

Although on different grounds, the arguments described in this section lead to the same conclusions of those described in the previous one, namely that "the age of online privacy is over". Users are left with limited choice between an innovative service without privacy and no service at all. Yet, as opposed to the former view (according to which privacy laws constitute an obstacle to innovation), this view considers privacy regulations as an actual motor for innovation to the extent that they spur companies to find new solutions bypassing the restrictions imposed by the law. Advocates of this view consider that strong privacy protection will most likely encourage bad innovation. They claim that, as an attempt to protect the fundamental rights of users, or to limit the damages that they might incur in the Cloud, privacy laws have the unintended effect of contributing to the development of new tools or techniques designed to further endanger the privacy of end-users. Regardless of the words of the law, the fear is that innovative companies will

ultimately dictate the terms and conditions according to which their services can or cannot be used, often imposing users to accept privacy conditions that go far beyond those prescribed by data protection laws.[20]
Back to our metaphorical model, this vision considers that road operators will always be able to impose their own rules to anyone driving on their roads. This basically condemns Bob to driving on a road whose minimum safety standards are ultimately established by the road operators rather than by the law. As long as there are people like Alice who value this road and are willing to use it in spite of its dangerous drawbacks, there will be no incentive for the road operators to make the road safer by maintaining the asphalt, constructing rail guards, or chasing the bandits or street vendors harassing the drivers along the way.

4.3 Users' response to bad innovation

In such circumstances, the only option left to users is to defend themselves by their own means, e.g. using privacy-protecting software and hardware devices to protect against any attack to their privacy encountered while wandering online. In our metaphor, this is like using an armoured vehicle with black windows to go on the road to avoid bandits and merchants, as well having all necessary features in the car (safety belts and airbags), to speed up safely if needed. Yet, this a time-consuming option, clearly applicable to a minority of tech-savvy or expert users. For all those like Bob, taking part in the innovation feast will mean observing powerlessly the infringement of their privacy.

5. Privacy and innovation

The emerging trend towards the collection and integration of data linked to cloud computing and big data may demand a re-evaluation of how privacy and data protection can be achieved on the Internet. As more and more data is being voluntarily made available by the users to the public, the boundaries between personal information and public information are becoming increasingly blurred, with relevant consequences for privacy. The problem with the privacy vs. innovation dichotomy is that it can easily induce people to think that there is a trade-off between the two. 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

[20] 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.

(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 it is possible to enjoy both privacy and innovation at the same time. Indeed, the two might actually work together, supporting rather than impinging on each other. The law could in fact push innovation in the right direction, by encouraging on the one hand 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 of privacy at an early stage into the design and operation of computer systems and networks, especially those in risky areas such as Cloud Computing and Big data systems. This is the idea behind the seven principles of "privacy by design"[21] (Cavoukian; EDPS 2010), which may actually constitute an answer to most of the problems discussed about, provided these principles do not become an empty checklist for regulatory compliance (Diaz et al. 2011). To work properly, privacy by design has to be applied to three distinct but interrelated fields of a business: (1) accountable business practice, (2) physical design and networked infrastructure and (3) IT systems.[22] These corresponds to the following three levels of our metaphorical model: (1) the directions given to drivers on the road, (2) the actual infrastructure of the roads and (3) the vehicles of the drivers.

5.1 Privacy and data protection directions

The problem with privacy and innovation, in general, and cloud computing in particular, is not that users do not care about their privacy, but rather that they are unaware of the practices and use of personal data provided to these services. In fact, as already noted, the internal operation of cloud and big data services is obscure to most users, who (usually) neither know what happens to the information they explicitly provide, nor are properly informed about the risks of providing such information. In other words, users are generally not aware that many of the services they use, albeit apparently free, are actually paid for with a different type of currency. Although they do not have to provide any financial contribution to use the service, users pay indirectly with the provision of personal data. Users are not paying for the product, because they are in fact the product being sold. Referring to our metaphor, the road directions are sometimes missing or hidden within the vegetation, thus leaving users with an impression of safety

[21] The seven principles are: 1) a proactive or preventative approach; 2) privacy by default; 3) privacy embedded in design; 4) positive sum game; 5) end-to-end security; 6) respect for users; 7) visibility and transparency. Cavoukian, http://privacybydesign.ca/about/principles/.
[22] Ibid.

that will come to an end as soon as they realize that the road is nothing but a dirty road, with a beautiful panorama, but also lots of obstacles and tortuous paths which are extremely dangerous to drive on. Sometimes, the directions are there, but they are misleading the drivers into alternative paths - hidden dark roads where it will be easier for bandits to attack them and for street vendors to approach them - ultimately leaving it up to the drivers to protect themselves.

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. By proper information, we do not mean simple 'notice and consent.' We follow Nissenbaum's reasoning (2011a) that simple 'notice and consent' often translates into obscure and ineffectual privacy policies hidden on the services' website, concealing the power imbalances between users and service providers. Specifically, what we mean by proper information translates into a two-steps approach.

First, service providers should offer clear and short - but complete - notices, written in layman language (such as the ones offered in open source services), 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),[23] such information would ideally be drafted by a multi-stakeholder group composed of regulators, private actors and members of the civil society involved in a particular field of business (i.e. the music industry, the movies industry, or social networks etc.). This is tantamount to providing clear and precise directions for drivers to make informed decisions concerning the path to take: the beautiful, fast, but more dangerous road, or the safe, quiet but dull, road.

Secondly, 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 (Friedman et al. 2012). Cloud-related data breaches are increasingly being reported by the media (a recent example of cloud's failure can be found at Honan 2012), but the association with the privacy of users is often not made explicit, even though they often lead to the

[23] Nissenbaum suggests that privacy 'online' should be read with the lenses of privacy 'offline', by following a contextual approach as it happens in the US. If the situations online correspond with the ones offline, they should be regulated similarly, or otherwise by finding proxies. In fact, according to Nissenbaum, 'code is law' only to a certain extent; it is like gravity, and the rest is up to us (Nissenbaum 2011b).

loss or disclosure of personal information (Porcedda 2012b).[24] In our metaphor, this corresponds to financing public awareness campaigns on safe driving, such as wearing safety belts, discouraging drinking, doping or talking on mobile phones while driving.

5.2 Privacy-compliant roads

It goes without saying that proper information has to be complemented by an appropriate technical infrastructure. Going back to the road metaphor, proper directions are useful, but not sufficient if there is only one road to use, which is both unsafe (e.g. with no asphalt and guardrails) and unsecure (e.g. full with bandits, thieves and vendors in disguise). Proper direction are also useless if it is extremely difficult to reach the safe road, or if the directions thereto can be only found out after having taken another road. 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. Beyond the metaphor, this means offering 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.).

In practice, we believe that there should be many roads (also within the same service): from the entirely safe (and unattractive) one that is requested by Bob, to the unsafe (but very panoramic) one that is so cherished by Alice. Different conditions can be set by different road operators (e.g. the safe road might be subject to a toll, whereas the panoramic road might be - apparently - used for free). Since most users are non-experienced drivers, the safe road should be the default option (i.e. privacy settings should be very high by default).

Yet, users like Alice, who are experienced drivers, aware of the risks and eager to agree to the terms and conditions of the road operators shall have the freedom to take the road they prefer. While the ones who decided to take the safe road should not be redirected to the unsafe road (and in any case, not without a proper disclaimer), it should be nonetheless easy for users to switch from one road to the other when the need arises (i.e. privacy settings should be easy to change). The different roads should be connected to each other and allow users to move back and forth from one road to the other, sometimes taking an intermediary path along the two (this would be akin to allowing individuals to negotiate the terms of service) (Nissenbaum 2011b). As opposed to current data practices based on a policy of opt-out, we advocate for a strictly opt-in approach to data collection and processing. Borrowing from Nissenbaum's (...) proposal for an "expressive

[24] 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).

choice", we suggest that every cloud computing platform implement privacy by design by automatically triggering the applicability of reasonable expectations of privacy, transforming consent into a means preventing circumvention of users' choice (Nissembaum, 2011b).

5.3 Privacy belts

Although innovative cloud services (or the road infrastructure) and users devices or vehicles) are not necessarily offered by the same company, they do nonetheless interact and influence each other. If users' devices are completely exposed to the wrongdoers, all efforts to protect users' safety and security will be diminished. This aspect becomes even more important whenever the devices are offered by the same companies that offer online services (such as Google, Amazon Microsoft and Apple). Hence, in order to ensure the privacy of users, users' devices need to be produced 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 amd Bourcier 2011; Porcedda 2012b). This is akin to producing cars with built-in safety belts and airbags to ensure drivers' safety in case of accidents, as well as the provision of optional features (such as off-road wheels, armour, opaque windows, etc.) providing more intimacy or security.

***

To conclude, we believe that privacy online is not dead, although it might have changed its meaning. Whether it relies on the protection of all personal data (as Bob wants), or some personal data but not others (as Alice wants), it is our view that privacy must respect individual choice concerning the collection and processing of personal data, including the disclosure thereof. In other words, we believe that such choice shall not rest on the public or the private sector, but rather on the consumer - one who is well informed of the alternatives, properly understands the impact of sharing information with one service or another, and is fully endowed with all necessary tools to protect or remove protection.[25]
Hence, the legislator should mandate the provision of information, and impose embedded safety/security standards upon the producers of vehicles producers. As

[25] See the report of the Fair Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, which strongly emphasizes the concept of consumer choice in data protection by stating that, whenever a user provides personal data or information to a third party, that user should be clearly and concisely informed as regards the use of that information, and should always be given the opportunity to decide whether or not to continue the interaction.

for the services, the law should provide for minimum standards of privacy/data protection (opt-in, track-me-not, highest standard by default), and leave the rest to a truly competitive market, where there is as symmetric information as is humanly possible.

6. Conclusion: innovation with 'privacy belts'

We have now reached the final destination of our road trip on the innovation highway. We have travelled with Bob and Alice, two drivers with different interests and skills who triggered a lively regulatory debate. According to some members of the competent authority, Bob and Alice's needs were irreconcilable. Either Bob had to give up travelling due to safety concerns, or Alice had to go without the freedom of driving on the panoramic road. According to others, Alice would always have the means of enjoying new, exciting panoramic roads, regardless of the wording of the law. Indeed, any attempt by the authority to close down unsafe roads would only lead to the opening of new, hidden and unsafe roads. The only alternative left to Bob would be to become an expert driver and procure himself a full-geared vehicle capable of handling those roads. In both cases, Bob would have to give in his desires, unless accepting the risk or investing personal time and resources in improving his safety and security. As a general rule, if there are only few roads, which are all bumpy and rough, and only unsafe vehicles to drive with, informed and skilled users are the only ones who may succeed in safely driving through them; in other words, the burden of safety and security is on users, and not on providers (only a well-informed user can apply the privacy-belts).

Today, privacy and innovation are being dealt with in a similar manner. On the one hand, privacy-minded but inexperienced users may eventually renounce enjoying the benefits of innovative services to avoid excessively exposing themselves, as protection is currently only available to those who possess the proper know-how and the appropriate hardware. On the other hand, service and device providers are either struggling to keep the legal guarantees as low as possible, or simply decide to ignore them with a do-it-first-and-see-what-happens approach, responding to the various attempts to raise the legal protections by circumventing the law with new innovative tools. In both cases, privacy is bound to lose; but so is (bad) innovation.

We believe that privacy laws may 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 of the service is itself customizable with simple privacy settings (ranging from the highest to the lowest) and backed up with the appropriate technological measures to enforce those settings.

Coming back to our metaphor, several years ago, many cars did not have safety belts, and some offered them as an optional, despite the fact that such feature could have avoided severe injuries or even deaths. Yet, as one car company started offering cars with safety belts as a mandatory feature, they eventually became a standard, which is now required by the law (Bilton 2012). The same analogy could be drawn in the case of privacy and data protection. Several companies are progressively emerging to offer alternative services or devices, which strongly focus on the respect of users' privacy and data protection. We expect this trend to continue insofar as privacy is gradually being understood as a socially desirable and useful means to foster competition in the market for cloud-based services.

Cavoukian and Jonas (2012) have recently demonstrated how privacy can be embedded in sensemaking 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.

Privacy laws should be in charge of fostering this change. Customers should not have the burden to protect themselves - rather, they should make a conscious and well-informed effort for putting themselves at risk. If users do not want to wear safety belts, they do it at their own conscious risks. So should be for privacy belts.

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, Berkely Technical Report # UCB/EECS-2009-28.

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.

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.

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

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 # 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/

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/>.

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. 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.

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.

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

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).W COM (2012) 11 final.

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.

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.

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 Interent, 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 Appications 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>.

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

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

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

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

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

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.

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”Hman 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>.

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.