icondia
personality matters

Privacy is dead; Long Live Privacy: Cloud Computing, Big Data, and Privacy

Dr Angela Adrian
Southern Cross University

And

Chris Buyvid
IT Manager, Johnson & Johnson

Abstract: The internet is an intrinsic part of our daily life. No longer do we go online to work, play or purchase; we are now in a world where everyone and everything simply is online. Cloud computing is the standard operating process, communications system and underlying infrastructure of the internet. These technological developments have produced incursions into the private space of people, with serious impacts on privacy for the individual, communities, and society. This is of paradigm-shifting significance to the law as it changes the way in which information is managed, especially where personal data processing is concerned. This poses the question: Does privacy still matter? This paper will address the privacy concerns intrinsic to both big data and cloud computing.

Keywords: Cloud computing, privacy, internet, big data

1 Introduction

The internet has become such an intrinsic part of our daily life that it is almost impossible to turn it off. No longer do we go online just for work, play or purchase; we are now in a world where everyone and everything simply is online all the time. Even when we are not actively 'surfing the net', our devices – from smart phones, to cars, to our home thermostats – can be online and collecting data when we are asleep and even if we are not home. When we are nowhere near a computer there are CCTVs, traffic sensors, and ATMs that can track our daily lives. And when we overindulge in Social Media by posting our status and pictures – Liking this and Tweeting that – it poses the question: Does privacy still matter? If so, how does it matter, why does it matters, and has the way it matters, in fact, changed over time?

Much of this activity is collected as data, a lot of data, so much so we call it big data. Should the upswing of big data mean that privacy must not matter as much as it used to? After all, look at all the information that people are sharing. Look at all of the good ways in which it is being used. Facebook allows a billion people in the world to share all kinds of personal information about themselves.

The amount of data in our world has been exploding, and analyzing large data sets—so-called big data—will become a key basis of competition, underpinning new waves of productivity growth, innovation, and consumer surplus, according to research by MGI and McKinsey's Business Technology Office (2012). Leaders in every sector will have to grapple with the implications of big data, not just a few data-oriented managers. The increasing volume and detail of information captured by enterprises, the rise of multimedia, social media, and the Internet of Things fuels exponential growth in data for the foreseeable future.

Today, commercial wireless signals already cover more of the world's population than the electrical grid, (Meeker, 2011) and the number of connected devices around the globe is expected to hit anywhere from 50 billion to a staggering one trillion in the next five years (Littleson, 2011). The sheer enormity of digital information that now connects us is mind-blowing. Cisco estimates that by 2015, the amount of data crossing the Internet every 5 minutes will be equivalent to the total size of all

movies ever made, and that annual Internet traffic will reach a zettabyte[1] – roughly 200 times the total size of all words ever spoken by humans (Cisco, 2012).
Transmitting, storing, and quickly accessing to process all this data has given rise to Cloud Computing. Built on top of the Internet, cloud computing addresses a key need by providing the efficient infrastructure necessary to support an agile and global market. This market is expected to grow at anywhere from 20% - 30% per year over the next several years, with Gartner predicting a $149 billion market by 2014 (Deloitte, 2012).

These technological developments have produced incursions into the private space of people, with serious impacts on privacy for the individual, communities, and society. In turn, businesses and organizations are beholden to regulations and industry standards for protecting privacy. This is of paradigm-shifting significance to the law as it changes the way in which information is managed, especially where personal data processing is concerned. This paper will address the privacy concerns intrinsic to both big data and cloud computing.

2 What do these concepts mean?

2.1 Big Data

Companies are awash with data, some generated by their customers or systems, some by third parties. Everyday IBM (2012) creates 2.5 quintillion bytes of data. In fact, 90% of the data in the world today has been created in the last two years alone (Ibid). This data comes from everywhere: from sensors used to gather climate information, posts to social media sites, digital pictures and videos posted online, transaction records of online purchases, and from cell phone GPS signals to name a few. The data comes in both structured and unstructured forms: those banking and online purchases are structured whereas videos and blogs are unstructured. Big data is the confluence of a number of technology trends: big transaction data, big interaction data, big data processing, growth of processing power and more sophisticated analytic techniques, and the pervasiveness of the Internet and data sharing through public and private clouds. Big data is therefore not just about the volume of data, spooky Big Brother or privacy, it is about gaining new insights and delivering business and service benefits, and one of the key challenges is reconciling the benefits with the legitimate concerns of individuals concerning access to, and use of, their personal information. And the challenge will become even greater as organizations gain the tools to tie unstructured data to structured data as the Internet becomes dominated by machine-to-machine applications (where devices communicate without conscious action by humans). This data is big data.

Big data, thus, refers to datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyse. This definition is intentionally subjective and incorporates a moving definition of how big a dataset needs to be in order to be considered big data. That is, big data will not be defined in terms of being larger than a certain number of terabytes. As technology advances over time, the size of datasets that qualify as big data will also increase. This definition will also vary by sector, depending on what kinds of software tools are commonly available and what sizes of datasets are common in a particular industry (McKinsey Global Institute, 2011)

Big data spans three dimensions: Variety, Velocity and Volume (IBM, 2012).

- **Variety** – Big data extends beyond structured data, including unstructured data of all varieties: text, audio, video, click streams, log files and more.
- **Velocity** – Often time-sensitive, big data must be used as it is streaming in to the enterprise in order to maximize its value to the business.
- **Volume** – Big data comes in one size: large. Enterprises are awash with data, easily amassing terabytes and even petabytes of information.

2.2 Cloud Computing

[1] 1 zettabyte = 10^{21} bytes or 1 billion terabyte

Originally dominated by North American users, the internet has grown and spread all over the world. In 2011 there were over 2 billion of internet users worldwide. The largest population of internet users is currently located in Asia (44%), followed by Europe (22.7%), North America (13%), Latin America (10.3%), Africa (5.7%), the Middle East (3.3%) and Australia (1%) (Miniwatts, 2011). This internationalization of the internet has had a tremendous impact on global trade and international law, as internet businesses have created a new international marketplace for goods and services. The Internet allows businesses to expand to global markets and directly interact with customers in ways impossible before. As computing becomes more pervasive, the opportunities for the smallest businesses expand. Business can now be transacted at the speed of thought (Gates, 1999). The digital nervous system that Bill Gates envisioned is blossoming as cloud computing.

Cloud computing is the ability to access highly scalable computing resources through the Internet without the upfront investment in computer equipment, software, infrastructure, etc. Massive computing capability is available to many users by economy of scales of sharing costs. Cloud computing has been defined as the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typically the Internet) (NIST, 2012). Computing clouds provide computation, software, data access, and storage resources without requiring cloud users to know the location and other details of the computing infrastructure. End users access cloud based applications through a web browser or a light weight desktop or mobile app while the business software and data are stored on servers at a remote location. At the foundation of cloud computing is the broader concept of infrastructure convergence (or Converged Infrastructure) and shared services. Rather than purchasing servers, software, data-centre space or network equipment, clients instead buy those resources as a fully outsourced service.

2.3 Privacy

Altman (1977) conceptualised privacy as the 'selective control of access to the self' regulated as dialectic and dynamic processes that include multi-mechanistic optimising behaviours. He regarded privacy as a boundary regulation process. The ability of information technology to disrupt or destabilise the regulation of these boundaries is a key issue in privacy management. "Through the establishment of a civil society each individual is protected by the whole of the community, thereby which each individual should be granted with the same rights and obligations and the same chance to develop. This relates in particular to the use of freedom via the social contract, which secures the self-determination of all individuals." (Weber & Weber, 2009)

The right to privacy has also been seen primarily as a human or social right arising from the nature of the relationship between the individual and society. This view derives from the empiricist and liberal philosophy of thinkers such as Hobbes and Locke, though others argue that privacy is too complex a concept to be reduced to a singular conception. Just as the Eskimo or Inuit have 50 words for 'snow', there are an equal number of ways to identify privacy. Most attempt to understand privacy through a core characteristic or common denominator that links disparate ideas under a single classification of 'privacy', especially when creating law and policy involving privacy depends upon a particular characterization of what privacy is. Privacy comes in many flavours and it is the plurality of different privacy concepts that do not share any one element but bear a resemblance to one another. (Solove, 2011) Privacy is acknowledged as a human right, under Article 12 of the Universal Declaration of Human Rights (1948), and Article 17 of the International Covenant on Civil and Political Rights (1976), both use the same form of words: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." It is not however the only approach possible. De Boni and Prigmore (2001), for example, have shown how it is possible to give a solid theoretical foundation to the right to privacy from the point of view of an idealistic, neo-Hegelian philosophy, seeing privacy not as a "human right" proceeding society but as the logical consequence of the Hegelian idea of free will. The important consequence of these definitions of privacy as an interest is that privacy has to be balanced against many other, often competing, interests.

It must balance the interests of the individuals themselves, of other individuals, of groups and of society as a whole. This balancing process is political in nature, involving the exercise of power deriving from authority, markets or any other available source (Clarke, 1999). Most privacy laws today focus on protecting the individual from the collection of what is considered private data. But these laws often overlook protecting the individual from how their non-private data is collected and processed, and ultimately used while denying the individual the ability to decide for himself how the information is used. The individual pieces of personal information may not be private, but the aggregation and analysis of that information can be used to make decisions about the person.

The privacy notion that will be considered in this paper relates to the right of self-determination. In other words, privacy is the right of individuals to 'know what is known about them', be aware of stored information about them, control how that information is communicated and prevent its abuse. Moreover, it refers to more than just confidentiality of information. Every individual should have the right to control his or her own data, whether private, public or professional. Without knowledge of the physical location of the server or how the processing of personal data is configured, end-users of cloud services could be jeopardizing their privacy.

2.4 Facebook

There are a billion people in the world who are sharing all kinds of personal information about themselves. How can Facebook be such a success if privacy still matters? It is necessary to look closely at Facebook and the Facebook story to answer this question. Six years ago, Microsoft invested $240 million in Facebook without any idea that Facebook would ever have a billion users. At the time, Facebook was not even the most popular social network on the planet. It definitely was not the first. The first was probably a service called Friendster. It was not even the second. The second was a social network called MySpace. In fact, six years ago, MySpace had 100 million users, Facebook had only 24 million. In this industry it is very unusual for one company to be the first to reach 100 million users and to have four times the market share of its next closest competitor and not go on to be the prevalent and most popular service (Smith, 2012).

What happened? What happened over the last six years? Why has MySpace declined? Why does it have fewer users now than six years ago? What caused the Facebook explosion? How did Facebook go from 24 million users to a billion? But the real question is why did it happen?
It is a facet that was captured well by one of the leading books about what happened, David Kirkpatrick's (2011) book, *The Facebook Effect*, when he addressed why this happened. On MySpace, the default setting was that you could see anybody's profile. Or to put it another way, the default setting was anybody could see your profile as well. But on TheFacebook, and initially it was called TheFacebook, the default allowed you only to see profiles of others at your school or those that had explicitly accepted you as a friend. A degree of privacy was built in at Facebook by default in a way that was simply not the case at MySpace. Although at MySpace you could change the settings, the default was that you shared your information with the world. At Facebook by default, you shared information only with people in your network and the people that you decided to make your friend.

At first the scarcity factor of Facebook made it highly desirable. Supply was short and demand was high – you were special to have a Facebook account and people would have to "Friend" you to network. But as social networking grows, our appetite has grown ravenous for instant social gratification. Twitter is an open social system and was designed from the start to allow people to follow those they were interested in without the bureaucracy of Facebook. This is why you do not have to send a friend request you simply follow the person. This simple balance of supply equals demand in Twitter's design is a big factor of its success.

2.5 Twitter

Twitter is the fastest growing amongst the top social networking sites in 2012. By its sixth birthday in March 2013, Twitter had more than 200 million active users creating over 400 million Tweets each day. (Twitter, 2013) With Twitter search you can find people with similar interests and then follow the people that are actively tweeting about the subjects you are interested in.

While Facebook is about social friendships, Twitter is about staying informed on the here and now. Topics and trending conversations are constantly changing. Twitter allows people to follow important topics, people, and conversations that are relevant or interesting to them. You will find that Twitter users, hashtags and general conversations change quickly and update throughout the day. The latest trends, hottest topics and most vibrant news garner the most Tweets.

Twitter conceived the hashtag to promote communication, and now corporations are learning to harness its power. Business benefit from using social media tools to engage the audience in current events and news as well as to build ongoing social relationships with followers. Personal data, not just tweets and posts, is being harvested and resold by large consumer data companies.

Social media sites sell their amassed customer data to data aggregators, which collate and mine the data, and then in turn sell it to consumer data companies that can take your tweets, posts and website activities, combine it with your personal information, and turn it into a behavioural pattern dossier to be sold to a company that wants you to buy its product.

A consumer data company that works with catalog and retail companies, said that it may use information about social media users' "names, ages, genders, hometown locations, languages, and a numbers of social connections (e.g., friends or followers)." The company also works with information about "user interactions," like what people tweet, post, share, recommend, or "like." These companies obtain information from third parties that specialize in collecting social network data. (Beckett, 2012)

Social media users want the benefits of easy and free networking, and are willing to quickly agree to the Terms of Use to join in. Most understand that some of their data is publically available, and know social sites must generate revenue – so they are willing to put up with ads that come with the free social site. When users are in control of their own data, they feel empowered. This is why Amazon users are apt to buy book recommended by Amazon. "Users of social media want to share with friends, not enable the sale of their personal information to data miners." Massachusetts Rep. Edward J. Markey told ProPublica in an e-mailed statement (Ibid).

Companies loose consumer trust when operating in the shadows with the data. Most users have no clue that a comment they made on a blog is being added to a database for some unknown use. Companies mine social media data to build dossiers on users. Social sites collect and resell user information – not just what users post, but web sites visited, interests, screen names, professional history, and how many friends or followers.

It is not just the votes of consumers in their adoption of Facebook that tells us that privacy matters to people; privacy matters to consumers. Recently, Pew Research found that 56% of consumers had decided not to complete an online purchase because of concerns about sharing personal information with the seller that they were going to do business with. They also found that 30% of consumers had uninstalled an app from their smart phone because of concerns about the way that app dealt with their personal information (Madden, 2012). Together, this tells an important story. It tells us that people care about privacy. Not only that, but people are thinking about privacy in new ways.

This is not a new phenomenon. The history of technology is a history of societal change. Typically one sees a pattern. The pattern starts with an invention and then the increasing adoption of new technology. That is followed by a second step in the process which involves new consumer needs and new consumer views about what to do with respect to the technology. And finally, what all of this means for laws and for regulation and for public policy.

3 Cloud Computing, Big Data and Privacy Paradigm

There is as yet no single, commonly-agreed definition of ‘cloud computing’. The United States National Institute of Standards and Technology has defined it as follows: ‘Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction’ (NIST, 2012). Under this definition, the cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models. The three cloud service delivery models are: Application/Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three classic cloud service models have different divisions of responsibility with respect to personal data protection. The risks and benefits associated with each model will also differ, and need to be determined on a case-by-case basis and in relation to the nature of the cloud services in question (ITU-T Technology Watch Report, 2009).

SaaS enables the consumer to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a client interface such as a web browser. With the SaaS model, the consumer has little or no influence how input data is processed, but should be able to have confidence in the cloud provider’s responsibility and compliance or can control which input he gives to a SaaS. First of all he can avoid giving sensitive data to a SaaS. Secondly, he might be able to ‘secure’ the sensitive data before it is inputted to the SaaS; for example, by encrypting the information (ENISA, 2009). However, if the individual encrypts the information, then that information is isolated and can no longer be processed. One is only storing information and not using it.

PaaS provides tools, supported by a cloud provider, that enable developers to deploy applications. On the one hand, a big responsibility lies with the developer to use best practices and privacy-friendly tools. On the other hand, the developer has to rely on the trustworthiness of the underlying PaaS (Ibid). IaaS provides the consumer with computing resources to run software. An IaaS provider will typically take responsibility for securing the data centres, network and systems, and will take steps to ensure that its employees and operational procedures comply with applicable laws and regulations. However, since an IaaS provider may have little application-level knowledge, it will be difficult for that provider to ensure data-level compliance, such as geographic restriction of data transfers. In this case, the responsibility lies with the cloud user to maintain compliance controls (Ibid).

3.1 Big Data: application

Mark Graham (2012) has levelled broad critiques at Chris Anderson’s (2012) assertion that big data will spell the end of theory: focusing in particular on the notion that big data will always need to be contextualized in their social, economic and political contexts. Even as companies invest eight- and nine-figure sums to derive insight from information streaming in from suppliers and customers, less than 40% of employees have sufficiently mature processes and skills to do so. To overcome this insight deficit, ‘big data’, no matter how comprehensive or well analyzed, needs to be complemented by ‘big judgment’, according to an article in the Harvard Business Review (Shah, et al, 2012).

Much in the same line, it has been pointed out that the decisions based on the analysis of Big Data are inevitably “informed by the world as it was in the past, or, at best, as it currently is.” (Anderson, 2012) Fed by a large number of data on past experiences, algorithms can predict future development if the future is similar to the past. If the systems dynamics of the future change, the past can say little about the future. For this, it would be necessary to have a thorough understanding of the systems dynamic, which implies theory (Ohm, 2012).

As a response to this critique it has been suggested to combine Big Data approaches with computer simulations, such as agent-based models, for example (Boyd, 2010). Those are increasingly getting better in predicting the outcome of social complexities of even unknown future scenarios through computer simulations that are based on a collection of mutually interdependent algorithms. In addition, use of multivariate methods that probe for the latent structure of the data, such as Factor Analysis and Cluster Analysis, have proven useful as analytic approaches that go well beyond the bi-variate approaches (cross-tabs) typically employed with smaller data sets.

3.2 Social Media & Privacy

We are becoming familiar with the adage: 'if you are not paying for the product, you are the product'. Most social networking sites require users to accept the Terms of Use policy before using the site. The common thread to these policies from free social media sites is the provider may share the user's data and, importantly data about the user, to third parties with little restraint. Social Media by its nature is viral and with near ubiquitous presence, its use is an all or nothing proposition – the user agrees to share all or be excluded from the network entirely. For those who can decipher the Privacy Agreement often discover that the social network owns all the content the user uploads, including pictures and videos. If the provider does not claim to own it, they do claim the right to share it. Smart phones and cameras are able to geo-tag when and where digital photos are taken by embedding latitude/longitude coordinates into the picture's metadata. Top social media sites have been criticised for violating their own policies in pursuance of profit.

Social networks mine this information to sell to marketing companies in order to more readily target your buying habits. This wealth of person information is a marketer's dream. Twelve thousand six hundred tweets per minute mention brand names. (Brandwatch 2013) Brandwatch's study of conversation and behaviour on Twitter found big sporting events attracted male dominated sport conversation. Brands can use this fodder as information to indicate where and when to run promotional campaigns, and capitalize on sporting events by taking part in the conversation with their target audience.

3.3 Data & Privacy in the Cloud

In *Privacy in Context*, Helen Nissenbaum (2010) defines privacy in terms of expected flows of personal information, modelled with the construct of context-relative information norms. When the flow of information adheres to entrenched norms, all is well. When these have been violated, protest and complaint result. Hence, the first challenge is to manage the persistence, replicability, scalability, and searchability of the self.

The loss of control by cloud-service consumers represents a serious threat to data integrity, confidentiality, and privacy principles. The Madrid Resolution (2009) sets out universal principles for the protection of personal data and privacy. It states that there is an urgent need to protect privacy in a world without borders and attain a joint proposal for the establishment of international standards on privacy and data protection. Its purpose is to define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data, and to facilitate the international flows of personal data inherent in a globalised world.

The basic principles governing the use of personal data include the following:

1. Lawfulness and fairness: personal data must be fairly processed, respecting the applicable national legislation as well as the rights and freedom of individuals and in conformity with the purposes and principles of the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights.
2. Proportionality: personal data should be limited to such processing as is adequate, relevant, and not excessive in relation to the purposes for which it was intended.
3. Purpose specification: processing of personal data should be limited to the fulfilment of the specific, explicit, and legitimate purposes for which it was collected.
4. Data quality: personal data should be kept accurate and up to date wand not be retained beyond the period for which it was intended.
5. Openness: the data controller shall have transparent policies with regard to processing of personal data.

6. Accountability: the data controller shall take all the necessary measures to observe the principles and obligations set out in the Madrid Resolution and in the applicable national legislation, and have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the regulatory authorities (Madrid Resolution, 2009).

These basic privacy principles are common to various countries' legislation and have found a consensus in terms of their corresponding geographic, economic, and legal application environments. Further, the Madrid Resolution (2009) encourages States to implement proactive measures to promote better compliance with applicable privacy protection laws relating to the processing of personal data, through instruments such as procedures to prevent and detect breaches in, or adaptations of, information systems and/or technologies for the processing of personal data, particularly when deciding on the technical specifications, development, and implementation of such systems and technologies.

4 Challenges

4.1 Challenges to the Cloud

Maintaining the levels of protection of data and privacy required by the Madrid Resolution and current local legislation in cloud computing infrastructure is a new challenge, as is meeting the restrictions on cross-border data transfer. This is not just a compliance issue. As cloud services process users' data on machines that the users do not own or operate, this introduces privacy issues and can lessen users' control. Hence, there is a key challenge for software engineers to design cloud services in such a way as to decrease privacy risk. As with security, it is necessary to design in privacy from the outset, and not just bolt on privacy mechanisms at a later stage (Pearson, 2009).

According to industry analysts, the ICT sector is poised for strong growth of cloud services (Gardner, n.d.). Users are creating an ever-growing quantity of personal data. IDC predicts that the 'digital universe' – the amount of information and content created and stored digitally – will grow from 1.8 zettabytes (ZB) in 2011 to over 7 ZB by 2015 (IDC, 2010). Key aspects of cloud computing are that there is an infrastructure shared between organisations that is off-premise. Therefore, there are threats associated with the fact that the data is stored and processed remotely, and because there is an increased usage of virtualisation and sharing of platforms between users. Protection of personal, confidential and sensitive data stored in the cloud is therefore extremely important.

Another feature of cloud computing is that it is a dynamic environment, in that for example service interactions can be created in a more dynamic way than traditional e-commerce scenarios. A report by the Federal Trade Commission (FTC, 2010) on *Protecting consumer privacy in an era of rapid change* analyses the implications for consumer privacy of technological advances in the IT sphere. According to FTC, users are able to collect, store, manipulate and share vast amounts of consumer data for very little cost. These technological advances have led to an explosion of new business models that depend on capturing consumer data at a specific and individual level and over time, including profiling, online behavioural advertising (OBA), social media services and location-based mobile services.

Services can potentially be aggregated and changed dynamically by customers, and service providers can change the provisioning of services. In such scenarios, personal and sensitive data may move around within an organisation and/or across organisational boundaries, so adequate protection of this information and legal compliance must be maintained despite the changes. There are concerns that the speed and flexibility of adjustment to vendor offerings that benefits business and provides a strong motivation for the use of cloud computing might come at the cost of compromise to the safety of data. This is a big issue: safety of data in the cloud is a key consumer concern, particularly for financial and health data. Rapid changes to cloud environments challenge enterprises' ability for maintaining consistent security standards, and providing appropriate business continuity and back-up.

In particular, cloud computing enables new services to be made available in the cloud (without a great deal of expertise needed to do this) by combining other services: for example, a 'print on demand' service could be provided by combining a printing service with a storage service. This procedure of service combination is typically under less control than previous service combinations carried out within traditional multi-party enterprise scenarios. There might well be differing degrees of security and privacy practices and controls in each of the component services. On the other hand, the service provision might necessarily involve collection, storage and/or disclosure of personal and sensitive information, and this information might need to flow across service providers' boundaries.

The FTC (2010) points out that many participants in public round tables set up to explore the privacy issues and challenges associated with twenty-first century technology and business practices have 'expressed concern that this growth in data collection and use [is] occurring without adequate concern for consumer privacy. They stated that these activities frequently are invisible to consumers and thus beyond their control.' Furthermore, companies have no control over their data, which, being entrusted to third-party application service providers in the cloud, could now reside anywhere in the world. Nor will a company know in which country its data resides at any given point in time. This is a central issue of cloud computing which conflicts with the European Union (EU) requirements whereby a company must at all times know to where the personal data in its possession is being transferred. Cloud computing thus poses special problems for multinationals with EU customers (ITU-T Technology Watch Report, 2009).

4.2 Challenges of Big Data

Complexity, scale, timeliness, heterogeneity, and privacy problems with Big Data impede progress at all phases of the pipeline that can create value from data. The problems start right away during data acquisition, when the data tsunami requires decisions, currently in an ad hoc manner, about what data to keep and what to discard, and how to store what is kept reliably with the right metadata. Much data today is not natively in structured format. For example, tweets and blogs are weakly structured pieces of text, while images and video are structured for storage and display, but not for semantic content and search. Transforming such content into a structured format for later analysis is a major challenge. The value of data explodes when it can be linked with other data, thus data integration is a major creator of value. Since most data is directly generated in digital format today, there are opportunities and challenges to influence the creation in order to facilitate later linkage and to automatically link previously created data. Data analysis, organization, retrieval, and modelling are other foundational challenges. Data analysis is a clear bottleneck in many applications, both due to lack of scalability of the underlying algorithms and due to the complexity of the data that needs to be analysed. Finally, presentation of the results and its interpretation by non-technical domain experts is crucial to extracting actionable knowledge (Agrawal, 2011).

During the last 35 years, data management principles such as physical and logical independence, declarative querying and cost-based optimization have led to a multi-billion dollar industry. More importantly, these technical advances have enabled the first round of business intelligence applications and laid the foundation for managing and analysing Big Data today. The many novel challenges and opportunities associated with Big Data necessitate rethinking many aspects of these data management platforms, while retaining other desirable aspects (Ibid).

5 Privacy by Design

Privacy is an essential human right, enshrined in the Universal Declaration of Human Rights and International Covenant of Political and Civil Rights. Article 12, the Universal Declaration of Human Rights, states that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation.' Everyone has the right to the protection of the law against such interference or attacks.' Article 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right.

In Europe, the Charter of Fundamental Rights of the European Union (2000) became legally binding in European Union law as part of the Lisbon Treaty (in force since December 2009). Article 16(1) of Treaty on the Functioning of the European Union (TFEU), as introduced by the Lisbon Treaty, establishes the principle that everyone has the right to the protection of personal data concerning him or her. Moreover, with Article 16(2) TFEU, the Lisbon Treaty introduced a specific legal basis for the adoption of rules on the protection of personal data. EU Directive 95/46/EC, and e-privacy and electronic communications Directive 2002/58/EC covering also data retention, are the main legal instruments in Europe covering privacy and the processing of personal data.

The Madrid Resolution provides international standards for the protection of privacy, but there is as yet no universally binding privacy legislation covering all the countries in the world. In a cloud computing service, privacy becomes more complex. Applying legal frameworks to the cloud is not easy when regimes are not harmonized, depend on the location of data and involve blurred division of responsibilities between stakeholders. In Europe, the 27 Member States have implemented the 1995 EU Directive differently, resulting in difficulties in enforcement. According to the European Commission, a single EU law can do away with the current fragmentation and costly administrative burdens, which could save businesses some €2.3 billion a year (EU Commission Press Release, 2012). An ENISA report (2011) summarizes a number of rules and challenges associated with Directive 95/46/EC in the context of 'the cloud computing environment, for which the roles of controller and processor still need to be determined on a case-by-case basis and in relation to the nature of the cloud services.'

5.1 Article 29 Data Protection Working Party

The European Commission has proposed one, single, technologically neutral and future-proof set of rules across the EU when it reviewed the Data Protection Directive in 2011 (EU Commission Press Release, 2012). In particular, more emphasis is being placed on strengthening the accountability of data controllers, including the obligation to notify data breaches, and by putting forward the principle of 'privacy by design.' To do this an Article 29 Data Protection Working Party (WP29) was set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data. (see, http://ec.europa.eu/dataprotectionofficer/introduction_en.htm)

In a joint reaction by WP29 to the consultation on the legal framework for the fundamental right to protection of personal data, the principle of 'privacy by design' was proposed to emphasize the need to implement Privacy Enhancing Technologies (PETs), 'privacy by default' settings and the necessary tools to enable users to better protect their personal data. The purpose of 'privacy by design' is to anticipate privacy risks to the development of the system and assess the impact of the system on individuals' privacy throughout the system's life cycle, thus ensuring that appropriate controls are implemented and maintained. It aims to prevent privacy intrusion events before they happen. This principle of 'privacy by design' should therefore be binding not only for data controllers, but also for technology designers, producers and business partners (Cavoukian & Abrams, 2010; WP29, 2009).
Some of the key changes that were announced the European Commission on the review of the EU Data Protection Directive are:

- A single set of rules on data protection, valid across the EU will simplify the administrative burden; unnecessary administrative requirements, such as notification requirements for companies, will be removed.
- Instead of the current obligation of all companies to notify all data protection activities to data protection supervisors, the Regulation provides for increased responsibility and accountability for those processing personal data. The principles of 'privacy by default' and 'privacy by design' are emphasized to ensure that individuals are informed in an easily understandable way about how their data will be processed.
- Organizations will only have to deal with a single national data protection authority in the EU country where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when their data is processed by a company based

outside the EU. Wherever consent is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed.
- People will have easier access to their own data and be able to transfer personal data from one service provider to another more easily (right to data portability).
- A 'right to be forgotten' will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it.
- EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.
- Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules. This can lead to penalties of up to €1 million or up to 2% of the global annual turnover of a company.
- A new Directive will apply general data protection principles and rules for police and judicial cooperation in criminal matters. The rules will apply to both domestic and cross-border transfers of data. (EU Commission Press Release, 2012)

The processing of personal data thus requires the emergence and development of standardized, technical privacy protection measures to implement 'privacy by design.' This concept - recommended in many reports - consists in the building in of privacy requirements from the very outset of a system's development and throughout its life cycle (Cavoukian & Abrams, 2010; FTC, 2010; WP29, 2009).

5.2 In practice

The joint reaction of the Article 29 Working Party (WP29) and the Working Party on Police and Justice (WPPJ) to the consultation on the legal framework for the fundamental right to protection of personal data introduced a definition of the 'privacy by design' principle. In practice, the implementation of the privacy by design principle will require the evaluation of several, concrete aspects or objectives. In particular, when making decisions about the design of a processing system, its acquisition and the running of such a system the following general aspects / objectives should be respected:

- Data minimization: data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible.
- Controllability: an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding consent and objection should be supported by technological means.
- Transparency: both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled.
- User-friendly systems: privacy-related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users.
- Data confidentiality: it is necessary to design and secure IT systems in a way that only authorized entities have access to personal data.
- Data quality: data controllers have to support data quality by technical means. Relevant data should be accessible if needed for lawful purposes.
- Use limitation: IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data warehouses, cloud computing, digital identifiers) have to guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way. (13th Annual Report, 2009)

Data integrity and availability are essential elements in the provision of cloud computing services. According to Directive 95/46/EC, Article 17, the controller and its processors must implement technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access; having regard to the state of the art and the cost of their implementation, such measures must ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The right to be forgotten is an essential element to personal control over their data. It is not about rewriting history. The Commission's proposal protects freedom of expression and the freedom of the media, as well as historical and scientific research. Equally, personal data may be kept for as long as they are needed to carry out a contract or to meet a legal obligation. In short, the right to be forgotten is not absolute (Justice Newsroom, 2012).

Individuals should be equally concerned with their privacy whether it be from Social Media or Government. Secondary use is the exploitation of data obtained for one purpose for an unrelated purpose without the subject's consent. How long will personal data be stored? How will the information be used? What could it be used for in the future? The potential uses of any piece of personal information are vast. Without limits on or accountability for how that information is used, it is hard for people to assess the dangers of the data's being in the government's control. (Solove, 2011)

The use of Privacy Impact Assessments to show how differing privacy requirements apply at different phases of design, and suggest some top tips for software engineers with specific technology to be used has been advocated by some industry partners (Pearson, 2009). In November 2007 the UK Information Commissioners Office (ICO) launched a Privacy Impact Assessment (PIA) process to help organizations assess the impact of their operations on personal privacy. This process assesses the privacy requirements of new and existing systems. Primarily intended for use in public sector risk management, it is increasingly seen to be of value to private sector businesses that process personal data.[2]

Further, Pearson (2009) recommends for there to be a role for PIAs within the cloud computing environment to determine the level of privacy risk, and the privacy measures which should be used to address this in the particular context. A Privacy Impact Assessment should be initiated early in the design phase, and its output fed into the design process in an iterative manner (Ibid). As cloud computing develops, it is likely that a range of different services will be offered, and that there will be a corresponding differing requirement in the level of privacy and security required. A PIA would help determine the appropriate level for the given context. As such, differing privacy requirements need to be considered according to the product lifecycle stage, namely:

1. Initiation: setting high level recommendations
2. Planning: describing privacy requirements in detail
3. Execution: identifying problems relating to the privacy solutions which have been proposed, considering alternative solutions if necessary, and documenting issues and any privacy exposures
4. Closure: using audit and change control procedures in the production environment; considering privacy protection during backup, fault repair, business continuity and disaster recovery
5. Decommission: ensuring secure deletion and disposal of personal and sensitive information (ibid).

Cannon (2004) describes processes and methodologies about how to integrate privacy considerations and engineering into the development process. This is managed via the creation of several documents during various phases of the development process, such as privacy sections in feature specification documents, a privacy statement for the developed application which should be readable by end users, policy file expressing the privacy statement, privacy specification (which documents the privacy aspects of the application and how they are dealt with), deployment guide (which describes privacy

[2] Similar methodologies exist and can have legal status in Australia, Canada and the USA.

properties settings of the system to inform end users) and review document (which summarizes privacy issues and how they are dealt with for a formal review by privacy experts).

5.3. The use of Privacy Enhancing Technologies (PETs) where appropriate

There is no commonly accepted definition of Privacy Enhancing Technologies (PETs), although broadly speaking they can be thought of as '… any technology that exists to protect or enhance an individual's privacy, including facilitating individuals' access to their rights under the Data Protection Act 1998' (UK Information Commissioner's Office, 2008). Examples include:

- Privacy management tools that enable inspection of service-side polices about the handling of personal data (for example, software that allows browsers to automatically detect the privacy policy of websites and compare it to the preferences expressed by the user, highlighting any clashes (Prime, 2008)
- Secure online access mechanisms to enable individuals to check and update the accuracy of their personal data
- Pseudonymisation tools that allow individuals to withhold their true identity from those operating electronic systems or providing services through them, and only reveal it when absolutely necessary; these technologies include anonymous web browsers, pseudonymous email and pseudonymous payment. The mechanisms may be designed for complete anonymity, or else pseudonymity (i.e. anonymity that is reversible if needed, for example in case of fraud).

Among the protection modes, PETs refer to a broad range of individual technologies at different levels of maturity. One challenge for the standardization of PETs in cloud computing is to mitigate cloud-specific concerns on a case-by-case basis and in relation to the nature of the cloud services. By definition, cloud computing should be easy for the customer to use. For the cloud provider and cloud developer, the situation is more complex. Standards should facilitate interoperability of privacy solutions in distributed architectures. In line with the corresponding legal frameworks, a basic principle of privacy requires life cycle security measures, for example data access control, and confidentiality/integrity of data against data breaches or leaks in transit and in data centres (ITU-T Technology Watch Report, 2012).

5.4 Comprehensive Reform of Data Protection Rules

The European Commission has advised that a comprehensive reform of the EU's 1995 data protection rules is needed to strengthen online privacy rights and boost Europe's digital economy. Due to the profound changes in technological progress and globalization, data is collected, accessed and used in ways never before imagined. Moreover, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement (Stockholm Program, 2010). A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year (Reding, 2012). The initiative will reinforce consumer confidence in online services and provide a boost to growth, jobs and innovation in Europe.

The main innovations of the proposed General Data Protection Regulation (COM (2012) 9 final) relate to the institutional system it creates rather than to the substance of data protection law. The consistency mechanism is at the core. The explanatory memorandum presented the proposed new legal framework for the protection of personal data in the EU which consisted of two legislative proposals:

- a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and
- a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012) 10 final).

Under the current Data Protection Directive 95/46/EC, a company operating in more than one EU country will have to deal with several Data Protection Authorities ('DPAs') with very different powers (up to one per Member State). This leads to uncertainty for business and situations where different rules can apply in each Member State for the same operation. There is no system to reconcile different DPA decisions apart from a non-binding discussion in the so-called Article 29 Committee, which brings together EU DPAs. The flaws of the present system were illustrated in the Google Street View case. The actions of a single company affected individuals in several Member States in the same way. Yet they prompted uncoordinated and divergent responses from DPAs (Business Week, 2010).

A Regulation is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation in accordance with Article 288 TFEU will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market (COM(2012) 10 final s 3.1).

The proposed Regulation establishes a new system of supervision for businesses or organizations processing personal data in more than one EU Member State or with a pan-EU impact, based on two elements. First, only one DPA is responsible for taking legally binding decisions against a company ('one stop shop'). That DPA is determined by the company's "main establishment" in the Union. Second, the proposed Regulation provides for mandatory cooperation between DPAs, and sets up a consistency mechanism at EU level to ensure coherent application of the rules which combines an advisory role for the European Data Protection Board (the 'Board') and a role for the Commission (COM(2012) 10 final s 3.2).

The three basic principles of the consistency mechanism: (1) DPAs take decisions on individual cases without an EU-wide impact; (2) Where there is an EU-wide impact, the Board is engaged and issues an opinion; and (3) The Commission acts as a backstop to ensure the consistency mechanism is effective (COM(2012) 10 final s 3.4.7.2). This is good for citizens and for business. In cases where there is no EU-wide impact, individual decisions are taken by national DPAs. This is the core of DPA independence. However, where there is an EU-wide impact, the matter is referred to the Board. The Board issues an opinion (non-binding) which must be taken into account by the national DPA. The onus is for DPAs to agree a position together. After the Board has issued its opinion, and where this is necessary in order to ensure the consistent application of the Regulation, the Commission may adopt a (non-binding) opinion. The DPA has to take the Commission's opinion into account before adopting its measure. The Commission's initial intervention is non-binding. Only if the Commission or the Board has "serious doubts as to whether the measure would ensure the correct application of the Regulation" the Commission may require the DPA to suspend the draft measure by a maximum of 12 months. This can only be done in two specific circumstances: (1) In order to reconcile diverging positions between a DPA and the Board; and (2) To adopt an implementing measure in particular where the proper functioning of the internal market is at issue (proposed Articles 57 – 63).

The consistency mechanism establishes a modified procedure that retains the role of national DPAs, guarantees cooperation between DPAs within the Board, and gives the Commission a role as a bulkhead. The role provided for by the Commission is the key supranational element of the proposal. Without a role for the Commission, the Board will be an intergovernmental club. This would be bad for citizens. The Commission acts as a necessary bulkhead to the Board ensuring that the Board acts decisively and protects the right to data protection enshrined in the Charter of Fundamental Rights. The threat of action by the Commission ensures that DPAs do not shy away from difficult cases. A consistency mechanism without the Commission would be bad for business. The Commission is the guardian of the internal market and is responsible for the proper implementation of EU law. The Regulation will not be properly applied based on knowledge of data protection laws alone. The internal market must be attained. The consistency mechanism is the way to do this. The role of the Commission does not interfere with the independence of DPAs who remain competent to tackle individual cases. The proposed Regulation strengthens DPAs by making sure they act in concert. The Commission's role is to ensure coherence and build the single market. (Justice Newsroom, 2013)

6 Conclusion

The global dimension of cloud computing requires standardized methodologies and technical solutions to enable participants to assess privacy risks and establish adequate protection levels. From a business point of view, privacy should represent an opportunity for cloud providers to promote brand image and differentiate services. However, privacy challenges require the involvement of a wide range of participants to cover multidisciplinary approaches benefiting all areas of society. Robust privacy protection needs interoperable built-in privacy components capable of ensuring compliance with principles such as data minimization in complex architectures. Privacy standards will play an important role in fostering the adoption of cloud services by promoting social responsibility and addressing privacy challenges. The implementation of PETs is seen as a good mechanism by data protection authorities to protect the data subject's rights and meet privacy principle objectives. Security is a process, not a product (Smedinghoff, 2008).

Effective data protection means putting individuals in control of their personal information by strengthening existing rights and by increasing access to those rights. The idea is simple. It is your data. You should have a say in how it is used.

References:

1. Agrawal, D. et al (2011) *Challenges and Opportunities with Big Data,* Cyber Center Technical Reports. Paper 1 at http://docs.lib.purdue.edu/cctech/1
2. Altman, I. (1977) *Privacy Regulation: Culturally Universal or Culturally Specific?* 33 Journal of Social Issues 3
3. Anderson, C. (2012) *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, Wired Magazine 16.07
4. Article 29 Data Protection Working Party (2009) *The Future of Privacy* at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf
5. Beckett, L. (2012) *Yes, Companies Are Harvesting – and Selling – Your Facebook Profile,* ProPublica, http://www.propublica.org/article/yes-companies-are-harvesting-and-selling-your-social-media-profiles
6. Boyd, D. (2010) *Privacy and Publicity in the Context of Big Data*. WWW Conference, Raleigh, North Carolina
7. Brandwatch (2013) *Brandwatch Report: Discover how the world's leading brands are using Twitter, from the type of activity they are engaged in to the platform that they perform it on. Analysis of global brands' Twitter activity* at www.brandwatch.com/wp-content/uploads/.../Brands-on-Twitter.pdf
8. *BusinessWeek*. (2010) *Google May Drop Street View in EU if Photo Storage Time Is Cut* at http://www.businessweek.com/#
9. Cannon, J.C. (2004) *Privacy: What Developers and IT Professionals Should Know*, London: Addison Wesley
10. Cavoukian, A., & Abrams, S. T. (2010) *Privacy by Design: essential for organizational accountability and strong business practices* at www.globalprivacy.it/Allegati_Web/57C2B8AA758546A0B76D5668F5CF5E16.pdf
11. Cisco (2012) *The Zettabyte Era* – White Paper at http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/VNI_Hyperconnectivity_WP.pdf
12. Clarke, R. (1999) *Internet Privacy Concerns Confirm the Case for Intervention*, 42 Communications of the ACM 2, Special Issue on Internet Privacy
13. Deloitte (2012) *Cloud Computing, Forecasting Change* at http://www.deloitte.com/view/en_GX/global/industries/technology-media-telecommunications/310b4debb2d5e210VgnVCM2000001b56f00aRCRD.htm

14. De Boni, M. & Prigmore, M. (2001) “A Hegelian basis for information privacy as an economic right”, in M. Roberts, M. Moulton, S. Hand, & C. Adams (eds) *Information systems in the digital world* - Proceedings of the 6th UKAIS Conference
15. ENISA (2009) *Cloud Computing Information Assurance Framework* at www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework
16. ENISA (2011) *Security & Resilience in Governmental Clouds* at www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-ingovernmental-clouds
17. EU Commission (25 January 2012) Press Release at http://europa.eu/rapid/pressReleaseAction.do?reference=IP/12/46&format=HTML
18. EU Commission (7 December 2012), *Myth-busting: what Commission proposals on data protection do and don't mean*, Justice News Room at http://ec.europa.eu/justice/newsroom/data-protection/news/121207_en.htm
19. EU Commission (6 February 2013) *The Proposed General Data Protection Regulation: The Consistency Mechanism Explained,* Justice News Room at http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm
20. EU Commission (2012) *Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*, COM (2012) 9 final.
21. EU Commission (2010) *The Stockholm Programme — An open and secure Europe serving and protecting citizens*, OJ C 115, 4.5.2010, p.1.
22. Federal Trade Commission (2010) *Protecting Consumer Privacy in an Era of Rapid Change: A proposed framework for businesses and policymakers* at www.ftc.gov/os/2010/12/101201privacyreport.pdf
23. Gartner. (n.d.) *Worldwide Cloud Services Market to Surpass $68 Billion in 2010* at www.gartner.com/it/page.jsp?id=1389313
24. Gates, Bill (1999) *Business @ the Speed of Thought: Using a Digital Nervous System*, London: Penguin Books
25. Graham M. (2012) *Big data and the end of theory?* The Guardian at http://www.guardian.co.uk/news/datablog/2012/mar/09/big-data-theory
26. IBM (2012) *What is Big Data?* at http://www-01.ibm.com/software/au/data/bigdata/
27. IDC (2010) *IDC Predictions 2011: Welcome to the New Mainstream* at www.idc.com/research/predictions11/downloads/IDCPredictions2011_WelcometotheNewMainstream.pdf
28. Information Commissioner’s Office, UK (2007) *PIA handbook* at http://www.ico.gov.uk/
29. Information Commissioner’s Office, UK (2008) *Data protection guidance note: privacy enhancing technologies* at http://tinyurl.com/56th6c
30. International Covenant on Civil and Political Rights (1976) Article 17
31. ITU-T Technology Watch Report (2009) *Distributed Commuting: Utilities, Grids & Clouds* at www.itu.int/dms_pub/itu-t/oth/23/01/T23010000090001PDFE.pdf
32. ITU-T Technology Watch Report (2012) *Privacy in Cloud Computing,* at http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx
33. Kirkpatrick, D. (2011) *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*, New York: Simon & Schuster
34. Littleson, R. (2011) *Anyone for 1 quadrillion intelligent, connected devices on the Internet?* Entitlement and Compliance Management at http://blogs.flexerasoftware.com/ecm/2011/07/anyone-for-1-quadrillion-intelligent-connect-devices-on-the-internet.html
35. Madden, M. (2012) *Privacy Management* at http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx
36. Madrid Resolution (2009) International Standards on the Protection of Personal Data and Privacy, International Conference of Data Protection and Privacy Commissioners at www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptos/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

37. Meeker, M. (2011) *Internet Trends* at http://www.kpcb.com/insights/2012-internet-trends
38. McKinsey Global Institute (2011) *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, at http://www.mckinsey.com/mgi
39. Miniwatts Marketing Group (2011) *Internet Usage Statistics* at http://www.internetworldstats.com/stats.htm
40. National Institute of Standards and Technology (2012) at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
41. Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Berkley, CA: Stanford University Press
42. Ohm, P. (2012) *Don't Build a Database of Ruin*, Harvard Business Review
43. Pearson, S. (2009) *Taking Account of Privacy when Designing Cloud Computing Services*, HP Laboratories, HPL-2009-54
44. PRIME (2008) *Privacy and Identity Management for Europe* at http://www.prime-project.org.eu
45. Reding, V. (2012) Commission proposes a comprehensive reform of EU data protection rules, Brussels, press conference at http://ec.europa.eu/avservices/video/player.cfm?ref=82655&sitelang=en
46. Shah, S., Horne, A. and Capellá, J. (2012) *Good Data Won't Guarantee Good Decisions*, Harvard Business Review
47. Smedinghoff, T. (2008) "Defining the Legal Standard for Information Security" in ed. Chander, A., et al *Securing Privacy in the Internet Age*, Berkeley, CA: Stanford University Press
48. Smith, B. (2012) *Putting People First: Moving Technology and Privacy Forward*, Transcript of Keynote Address at the 34th International Conference of Data Protection and Privacy Commissioners, Punta Del Este, Uruguay
49. Solove, D. (15 May 2011) *Why Privacy Matters Even if You Have 'Nothing to Hide'* at http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/
50. 13th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2009 at http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm
51. Twitter (2013) *Celebrating Twitter* at http://blog.twitter.com/2013/03/celebrating-twitter7.html
52. Universal Declaration of Human Rights (1948) Article 12
53. Weber, R. H. & Weber, R. (2009) *Social Contract for the Internet Community?: Historical and Philosophical Theories as Basis for the Inclusion of Civil Society in Internet Governance?* Scripted 6(1).