Privacy in Cloud Computing

ITU-T Technology Watch Report
March 2012

Privacy concerns are increasingly important in the online world. It is widely accepted that cloud computing has the potential to be privacy disabling. The secure processing of personal data in the cloud represents a huge challenge. Adoption of privacy-enhancing technologies to support such activities in the cloud will depend upon the existence of uniform ways of handling personal data at the international level and on technical standards which can help to demonstrate compliance with legal and regulatory frameworks.

The rapid evolution of the telecommunication/information and communication technology (ICT) environment requires related technology foresight and immediate action in order to propose ITU-T standardization activities as early as possible.

ITU-T Technology Watch surveys the ICT landscape to capture new topics for standardization activities. Technology Watch Reports assess new technologies with regard to existing standards inside and outside ITU-T and their likely impact on future standardization.

Acknowledgements

This report was written by Stéphane Guilloteau, France Télécom Orange, France, and Venkatesen Mauree of the ITU Telecommunication Standardization Bureau.

The authors are thankful to the support given by colleagues at the ITU Secretariat. The authors would like to thank Dr Stefan Köpsell, Dresden University, Germany and Mr Gwendal Le Grand, Commission Nationale de l'Informatique et des Libertés (CNIL), France.

Please send your feedback and comments to tsbtechwatch@itu.int.

The opinions expressed in this report are those of the authors and do not necessarily reflect the views of the International Telecommunication Union or its membership.

This report, along with other Technology Watch Reports can be found at www.itu.int/techwatch.

Cover picture by Winui, Shutterstock.

Technology Watch is managed by the Policy & Technology Watch Division, ITU Telecommunication Standardization Bureau.

Call for proposals

Experts from industry, research and academia are invited to submit topic proposals and abstracts for future reports in the Technology Watch series. Please contact us at tsbtechwatch@itu.int for details and guidelines.

Table of contents

Page

I. Introduction 1

2. Cloud computing paradigm and privacy 2

3. Challenges to privacy in cloud computing 5

3.1 Complexity of risk assessment 5

3.2 Emergence of new business models and implications for consumer privacy 5

3.3 Regulatory compliance 6

4. Privacy by design 7

5. Using PETs to implement privacy by design 11

5.1 Description of data processing flows 11

5.2 Using PETs 12

6. Standardization activities 14

6.1 International Telecommunication Union (ITU) 14

6.2 International Organization for Standardization (ISO) 15

6.3 Organization for the Advancement of Structured Information Standards (OASIS) 15

6.4 Cloud Security Alliance (CSA) 16

7. Conclusion 17

Bibliography 18

Privacy in Cloud Computing

I. Introduction

Just a few years ago, people used to carry their documents around on disks. Then, more recently, many people switched to memory sticks. Cloud computing refers to the ability to access and manipulate information stored on remote servers, using any Internet-enabled platform, including smartphones. Computing facilities and applications will increasingly be delivered as a service, over the Internet. We are already making use of cloud computing when, for example, we use applications such as Google Mail, Microsoft Office365[1] or Google Docs. In the future, governments, companies and individuals will increasingly turn to the cloud.

The cloud computing paradigm changes the way in which information is managed, especially where personal data processing is concerned. End-users can access cloud services without the need for any expert knowledge of the underlying technology. This is a key characteristic of cloud computing, which offers the advantage of reducing cost through the sharing of computing and storage resources, combined with an on-demand provisioning mechanism based on a pay-per-use business model. These new features have a direct impact on the IT budget and cost of ownership, but also bring up issues of traditional security, trust and privacy mechanisms.

Privacy, in this report, refers to the right to self-determination, that 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. In other words, it refers to more than just confidentiality of information. Protection of personal information (or data protection) derives from the right to privacy via the associated right to self-determination. Every individual has the right to control his or her own data, whether private, public or professional.

Without knowledge of the physical location of the server or of how the processing of personal data is configured, end-users consume cloud services without any information about the processes involved. Data in the cloud are easier to manipulate, but also easier to lose control of. For instance, storing personal data on a server somewhere in cyberspace could pose a major threat to individual privacy. Cloud computing thus raises a number of privacy and security questions. Can cloud providers be trusted? Are cloud servers reliable enough? What happens if data get lost? What about privacy and lock-in? Will switching to another cloud be difficult?

Privacy issues are increasingly important in the online world. It is generally accepted that due consideration of privacy issues promotes user confidence and economic development. However, the secure release, management and control of personal information into the cloud represents a huge challenge for all stakeholders, involving pressures both legal and commercial.

This report analyses the challenges posed by cloud computing and the standardization work being done by various standards development organizations (SDOs) to mitigate privacy risks in the cloud, including the role of privacy-enhancing technologies (PETs).

[1] Microsoft Office 365 is the Software as a Service (SaaS) commercial offering of Microsoft Office.

2. Cloud computing paradigm and privacy

There is as yet no single, commonly-agreed definition of "cloud computing". The United States National Institute of Standards and Technology (NIST, http://csrc.nist.gov) has defined it as follows [16]:

"Cloud computing is a model for enabling 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."

Under this definition, the cloud model promotes availability and is composed of five essential characteristics, three delivery models and four deployment models.

The five key characteristics of cloud computing are on-demand self service, ubiquitous network access, location-independent resource pooling, rapid elasticity and measured service, all of which are geared towards seamless and transparent cloud use. Rapid elasticity enables the scaling up (or down) of resources. Measured services are primarily derived from business model properties whereby cloud service providers control and optimize the use of computing resources through automated resource allocation, load balancing and metering tools.

The three cloud service delivery models (see figure 1) are: Application/Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). ITU Technology Watch published a separate report on the cloud computing phenomenon in March 2009 [15]. 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.

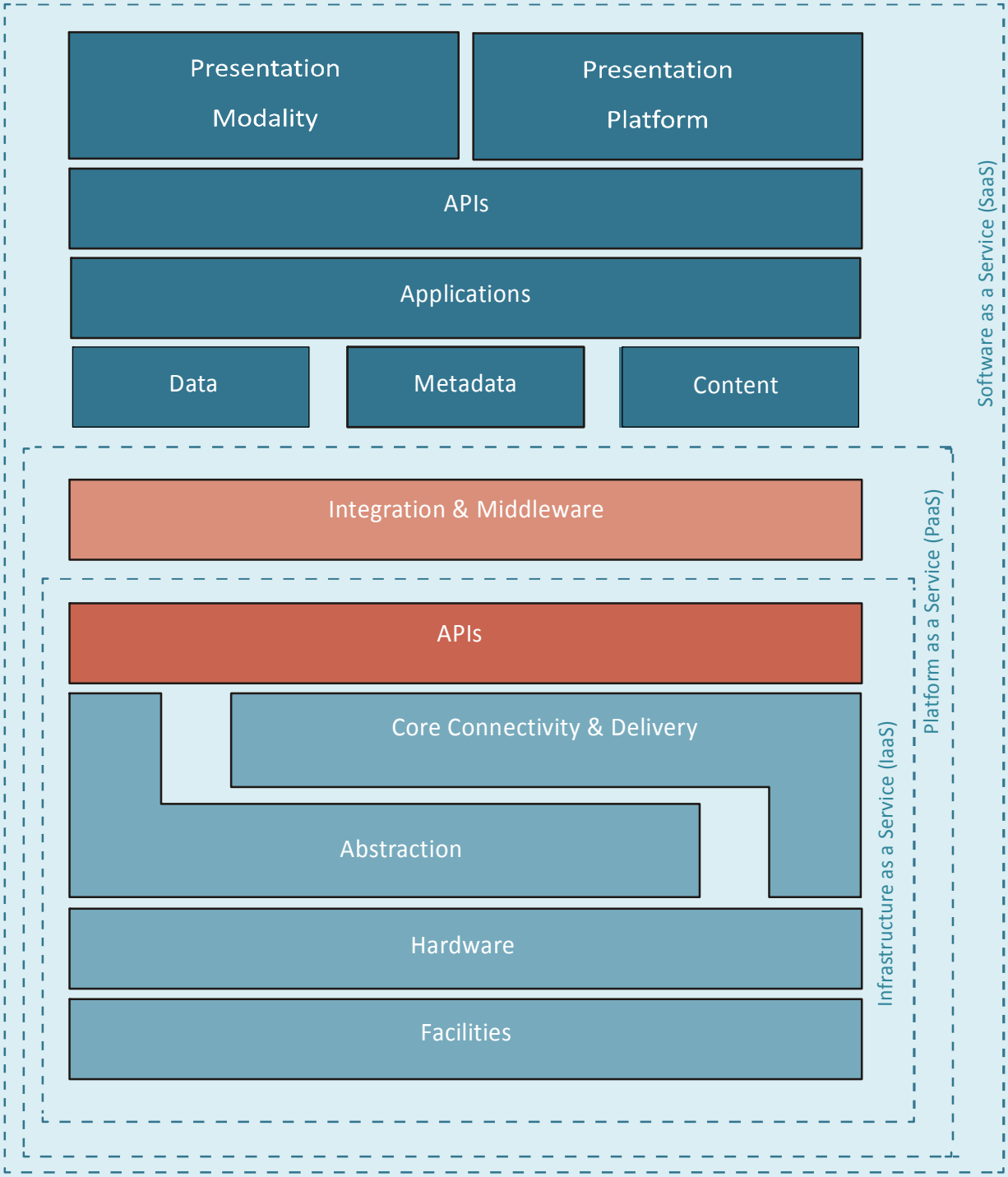
SaaS enables the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a client interface such as a web browser (e.g. web-based email such as Gmail or CRM from Salesforce). With the SaaS model, the consumer has 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 to give sensible data to a SaaS. Secondly he might be able to "secure" the sensible data before he inputs them into the SaaS (e.g. their exists plugins for browsers supporting encryption of input form fields. This could be used to send only encrypted mails using Gmail).

PaaS provides tools, supported by a cloud provider, that enable developers to deploy applications (e.g. Salesforce's Force.com, Google App Engine, Mozilla Bespin, Zoho Creator). 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 (and related infrastructure). Assume for instance that some developer has developed a cloud application which encrypts all data before it is stored within the cloud storage provided by the PaaS. In this case the developer has to trust that the platform/infrastructure is not compromised. Otherwise the attacker might get access to the clear text (i.e. before encryption happens) – because he can control the execution environment (e.g. virtual machine monitor, hardware etc.).

IaaS provides the consumer with computing resources to run software. One example of IaaS is Amazon EC2 Web Services. 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. IaaS is the model that guarantees more direct control but also leaves the customer responsible for the implementation of technical and procedural security and resilience measures [6]. With respect to standardization there

should be some way for the consumer in an IaaS cloud environment to express his privacy/security related requirements. For example, if the IaaS is based on virtualization, the consumer might want to express that the IaaS provider is not allowed to migrate the virtual machines from EU based data centers to US based ones due to data protection laws and regulations.

Figure 1. Cloud reference model



Source: Cloud Security Alliance

The loss of control by cloud-service consumers represents a serious threat to data integrity, confidentiality and privacy principles. A good reference for use in defining universal principles for the protection of personal data and privacy is the Madrid Resolution. This resolution was approved by data protection authorities from fifty countries, gathered in Madrid in 2009 within the framework of the 31st International Conference of Data Protection and Privacy. It states the 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 globalized world.

The basic principles that must govern the use of personal data include those of lawfulness and fairness[2], proportionality[3], purpose specification[4], data quality[5], openness[6] and accountability[7] [20].

These basic privacy principles are common to various countries' legislation on the matter and enjoy wide consensus in terms of their corresponding geographic, economic or legal application environments.

Moreover, the Madrid Resolution 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 adaptation of, information systems and/or technologies for the processing of personal data, particularly when deciding on the technical specifications and development and implementation of such systems and technologies [20].

There is no commonly accepted definition for the term Privacy Enhancing Technologies (PETs). In general PETs are viewed as technologies that:

a) Reduce the risk of contravening privacy principles and legislation.
b) Minimize the amount of data held about individuals.
c) Allow individuals to retain control of information about themselves at all times.

Proactive-measure requirements can be met through the implementation of PETs, designed to safeguard the data subject's privacy and rights by protecting personal data and preventing its unnecessary and/or undesired processing. PETs include "opacity tools/technologies", i.e. tools and technologies which strive for data minimization like encryption, pseudonymisation, anonymisation etc., as well as transparency enhancing tools (TETs), providing users with information about privacy policies or granting them online access to their personal data.

---

2 Lawfulness and fairness principle: 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.

3 Proportionality principle: 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.

4 Purpose specification principle: processing of personal data should be limited to the fulfilment of the specific, explicit and legitimate purposes for which it was collected.

5 Data quality principle: personal data shall be kept accurate and up to date and not be retained beyond the period for which it was intended.

6 Openness principle: The data controller shall have transparent policies with regard to processing of personal data.

7 Accountability principle: 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.

3. Challenges to privacy in cloud computing

The promise to deliver IT as a service is addressed a large range of consumers, from small and medium-sized enterprises (SMEs) and public administrations to end-users. According to industry analysts, the ICT sector is poised for strong growth of cloud services [11]. 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[8] (ZB) in 2011 to over 7 ZB by 2015 [13].

This expanding quantity of personal data will drive demand for cloud services, particularly if cloud computing delivers on the promises of lower costs for customers and the emergence of new business models for providers. Among the main privacy challenges for cloud computing are:

a) Complexity of risk assessment in a cloud environment
b) Emergence of new business models and their implications for consumer privacy
c) Achieving regulatory compliance.

3.1 Complexity of risk assessment

The complexity of cloud services introduces a number of unknown parameters. Service providers and consumers are cautious, respectively, about offering guarantees for compliance-ready services and adopting the services. With service providers promoting a simple way to flow personal data irrespective of national boundaries, a real challenge arises in terms of checking the data processing life cycle and its compliance with legal frameworks.

In a cloud service, there are many questions needing to be addressed in order to determine the risks to information privacy and security:

- Who are the stakeholders involved in the operation?
- What are their roles and responsibilities?
- Where is the data kept?
- How is the data replicated?
- What are the relevant legal rules for data processing?
- How will the service provider meet the expected level of security and privacy?

To address these issues, the Madrid Resolution states that every responsible person shall have transparent policies with regard to the processing of personal data. Stakeholders need to specify requirements for cloud computing that meet the expected level of security and privacy. In Europe, the European Network and Information Security Agency (ENISA) provides recommendations to facilitate understanding of the shift in the balance of responsibility and accountability for key functions such as governance and control over data and IT operations and compliance with laws and regulations. [8]

3.2 Emergence of new business models and implications for consumer privacy

A report by the Federal Trade Commission (FTC) 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. [10]

FTC 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

[8] 1 zettabyte = 10^{21} bytes or 1 billion terabyte.

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".

According to FTC, the increasing low-cost data storage capability will lead companies to retain the data they collect indefinitely, thereby creating the incentives and opportunity to find new uses for it. As a result, consumers' data may be subject to future uses that were not disclosed – and may not even have been contemplated – at the time of collection. However, in Europe there are legal instruments specifying the data retention period for personal data.

A September 2008 Pew Internet Data Memo reported that 69 per cent of Americans had either stored data online or used web-based software applications at least once. Using a Hotmail or Gmail account for e-mail, storing Firefox or Google browser bookmarks online, sharing friendships in cyberspace on social networks such as Facebook, maintaining a blog on WordPress and storing personal videos and photos on YouTube and Flickr are just some of the ways in which many people are already "working in the cloud" every day. [18]

A number of challenges are also posed by cloud service aggregators, which integrate multiple SaaS services into a "single" service. An example of a cloud service aggregator would be a multiple cloud SaaS travel booking platform for use by travel agents, which may include a customer relationship management application, a travel and accommodation booking and reservations application, a credit card processing application, a financial and accounting application and an e-commerce application – all of which would be handled by the user as a single application. The fact that the applications may not all be operated by the same SaaS provider could result in differences in terms of reliability and security. Such models could become more widespread in the future, and their legal and security/privacy implications need to be clearly understood.

3.3 Regulatory compliance

It is widely accepted that data protection and regulatory compliance are among the top security concerns for chief information officers (CIOs).

According to the Pew Internet and American Life Project, an overwhelming majority of users of cloud computing services expressed serious concern about the possibility of a service provider disclosing their data to others. Ninety per cent of cloud application users said they would be very concerned if the company at which their data were stored sold them to another party. Eighty per cent indicated that they would be very concerned if companies used their photos or other data in marketing campaigns. Sixty-eight per cent of users of at least one of the six cloud applications said they would be very concerned if companies providing such services analysed their information and then displayed adverts to them based on their actions [18].

An October 2008 study by IDC reported that 74.6 per cent of surveyed IT executives and CIOs expressed the view that security is the biggest challenge for the cloud computing model [12]. Stakeholders therefore increasingly feel the need to prevent data breaches. The reasons for this are obvious, given the potentially disastrous consequences of a personal data breach. In recent months, many newspaper articles have revealed data leaks in sensitive areas such as the financial and governmental domains and web community. Incidents in the digital universe such as the data breach experienced by Sony or the release by WikiLeaks of US diplomatic cables do little to reassure stakeholders about data security. Such breaches are not cloud specific but can nevertheless have a negative impact on confidence in the security of data processing. Such breaches can, moreover, result in penalties, legal action, business loss and social harm.

One of the missions of the data protection authorities is to prevent the so-called "Big Brother" phenomenon which refers to a scenario whereby a public authority processes personal data without adequate privacy protection. In such a situation, end-users may view the cloud as a vehicle for drifting into a totalitarian surveillance society.

The ever-growing amount of data processed in a cloud service can represent an increasingly attractive target for both external and internal attackers harbouring fraudulent, political or commercial motivations. The specificities of cloud computing therefore make the data protection incentive even greater. For example, the cloud provider should provide encryption to protect the stored personal data against unauthorized access, copy, leakage or processing.

Moreover, in a cloud environment, 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 where the personal data in its possession is being transferred to. Cloud computing thus poses special problems for multinationals with EU customers.

4. 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[9]. Article 12 of the Universal Declaration of Human Rights states that "*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*." 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). 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 recent 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[10].

A recent ENISA report 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". [8]

The United States does not have an overarching governmental regulation as is the case in Europe, but follows a sectoral approach with privacy and data protection needs being addressed through a plethora of regulations and laws, including self-regulation. A number of privacy principles are also to be found in other organizations and countries[11]. The privacy legislations in other countries are also important. Countries in the developing world (e.g on the African continent, India and China) are currently planning the introduction of

9 See www.un.org/documents/instruments/docs_en.asp?type=conven

10 See http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML

11 Some examples of other privacy principles: OECD (Privacy Principles 1980), Generally Accepted Privacy Principles (GAPP) from AICPA, FTC Fair Information Practice Principles (FIPPs) (ref: United States Privacy Act of 1974), Consumer Privacy Protection Principles (CPPPS), Asia-Pacific Economic Cooperation (APEC) Privacy Framework - Information Privacy Principles (2005) and International Security, Trust & Privacy Alliance (ISTPA) Privacy Principles.

privacy and data protection laws. The differences in privacy legislation globally can become a trade barrier and prevent innovation[12].

According to a report of the Business Sotware Alliance in February 2012[13], it was observed that there is a huge divide between developed and developing countries in terms of adequate legislation for protection of personal data. The report also highlighted that even among developed countries there are conflicting data protection regulations which could hamper transfer of personal data across borders. For example, some developed countries are considering restricting provision of cloud services only to local companies within the country. An international approach is necessary to bring together the multiple data protection regimes and harmonize the business rules for providers and protection rules for the citizen. Without greater coordination at international level on government policies the main advantage and efficiency of cloud computing which is to be able to move data and software services freely across borders will not be achieved.

Box 1: Odense Municipality Case [5]

A recent ruling by the Danish Data Protection Agency (DDPA) provides a relevant example of the regulatory problems that can arise in practice. In February 2011, DDPA published an opinion concerning cloud computing. The opinion was among the first of its kind to be issued by a European data protection authority, and is therefore of interest to stakeholders.

The case in question concerns a Danish municipality's plans to use Google Apps within the school system for processing sensitive personal data when registering information about lesson planning and assessments of lesson plans and individual students' educational development.

According to the aforementioned ruling, when initiating the processing of personal data, the controller authority or company is responsible for structuring that processing such as to ensure compliance and ensure that processed data relating to citizens are at all times protected by the requisite security measures. DDPA rejects Odense Municipality's use of cloud computing to store certain sensitive information, primarily on the grounds of security concerns. It does not concur with Odense Municipality's view that confidential and sensitive data about students and parents can be processed in Google Apps.

The question is whether the municipality can meet the Danish Data Protection Act's requirements in terms of ensuring that the security measures are upheld by the data processor, given that the municipality does not know where the data are physically located. It is unclear how the following requirements of the Danish Data Protection Act will be met:

- Deletion of data so that it cannot be recreated.
- Transmission and login: the municipality has not made clear whether encryption will be used when transferring data between the various data centres.
- No information has been provided about what data are logged or how long the log is stored.

DDPA is willing to reconsider the case for a revised statement if Odense Municipality continues to work on it and seeks solutions to the identified issues.

The Odense Municipality case confirms that a serious risk assessment must be made before switching to cloud services and standards should play an essential role in bringing about better compliance and fostering the adoption of cloud services. This being the case, stakeholders have to prepare for future regulatory changes.

The European Commission has proposed one, single, technologically neutral and future-proof set of rules across the EU when it reviewed[14] the Data Protection Directive (See Box 2) in 2011. In particular, more

12 See www.economist.com/node/21543489

13 See http://portal.bsa.org/cloudscorecard2012/

14 See European Commission Press Release of 25 January 2012: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=EN&guiLanguage=en

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*"[15]. In a joint reaction by the Article 29 Data Protection Working Party[16] (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 PETs, "privacy by default" settings and the necessary tools to enable users to better protect their personal data. This principle of "*privacy by design*" should therefore be binding not only for data controllers, but also for technology designers, producers and business partners [4][19].

Box 2: Review of the EU Data Protection Directive

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.

Source: European Commission Press Release, 25 January 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[17] – consists in the building in of privacy requirements from the very outset of a system's development and throughout its life cycle.

15 The purpose of privacy by design is to anticipate privacy risks prior 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.

16 The Article 29 Data Protection Working Party 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/justice/data-protection/article-29/index_en.htm).

17 See [4], [10] and [19]

To be effective, "*privacy by design*" needs to be based on a modern global approach to developing operational solutions that simultaneously address both legal and technological challenges. Sound privacy protection calls for interoperable, built-in privacy components capable of ensuring compliance with privacy principles.

In Resolution 130 (Rev. Guadalajara, 2010) of the ITU Plenipotentiary Conference, on strengthening the role of ITU in building confidence and security in the use of information and communication technologies, the conference expressed its awareness that ITU and other international organizations, through a variety of activities, are examining issues related to building confidence and security in the use of ICTs, including stability and measures to combat spam, malware, etc., and protect personal data and privacy. To improve the interoperability of cloud solutions, standards are essential. In 2011, the Global Standards Collaboration (GSC) reaffirmed its Resolution GSC-15/25, on personally identifiable information (PII) protection, which recognizes that there is a large body of work and expertise scattered throughout the global community, including the standardization community, which addresses these issues at least in part.

GSC concluded that standardization of terms, definitions, frameworks and procedures is needed to ensure meaningful dialogue and consistency in addressing such concerns on a national, regional and global basis, and that such standardization needs to be consolidated into a distinct area of study for consistency and effectiveness, and resolved to support standardization activities in the sphere of PII protection.

Box 3: Privacy by design

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 introduces a definition of the "privacy by design" principle [21]:

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.

In February 2012, the GSM Association (GSMA) announced a set of Privacy Design Guidelines for Mobile Application Development[18] following feedback from industry stakeholders, regulators and civil society. Some of the big mobile phone companies in Europe, (i.e Orange, Vodafone and Deutsche Telekom) have agreed to adopt the guidelines[19]. According to the GSMA the guidelines would help to develop mobile apps that adhere to "privacy by design". The guidelines provide for the possibility for the user to be informed about what personal information the application will access, collect and use and with whom it will be shared and for what purpose. It also addresses how social networking apps should handle personal information including when a user wishes to leave a service. In particular it states that users "*must be able to delete their accounts, resulting in complete removal of all personal information and any content posted*".

As the lead study group on "Telecommunication security", which includes developing and maintaining security outreach material, coordination of security-related work and identification of needs and assignment and prioritization of work to encourage timely development of telecommunication security recommendations, ITU-T SG 17 covers the topic of cloud-computing security issues in its Question 8/17, while other SG 17 Questions address topics such as information security management and identity management. Where privacy issues are concerned, SG 17 is specifically tasked to study PII protection and develop mechanisms to ensure that access to PII is authorized only where appropriate.

5. Using PETs to implement privacy by design

The proactive measures defined in the Madrid Resolution include the adaptation of technologies to guarantee effective privacy protection where the processing of personal data is concerned. The main goal is to encourage self-regulation by companies and better implementation of privacy principles. The use of appropriate technical measures is an essential complement to legal means. PETs are technologies that protect privacy by protecting personal data and preventing its unnecessary and/or undesired processing but also by making a user aware of the stored data, its processing and the related data flows. Standardized privacy solutions could be very helpful in achieving this goal.

5.1 Description of data processing flows

According to the openness principle defined in the Madrid Resolution, every responsible person shall have transparent policies with regard to the processing of personal data. A description of data processing flows should be one of the first steps. This is essential to risk assessment and to ensuring the appropriate level of protection. A data flow table is a very useful tool for the data controller responsible for implementing privacy controls based on audit, risk assessment and certification. This table should follow the data life cycle steps: collection, transfer, use, storage, sharing and disposal of PII. It should include information such as type of personal data, who processed it, operating platform, processing application, purpose of processing, protection mode, storage lifetime, to whom the personal data will be transferred and at which location it will be stored.

Table 1: Example of data flow table

Type of data	Persons entitled to process the personal data	Operating platform	Processing application	Purpose of data processing	Protection mode	Storage lifetime and disposal measure	Data recipients	If Data is transferred outside the country, indicate the destination country

[18] See www.gsma.com/Mobile-Privacy-Design-Guidelines

[19] See www.bbc.co.uk/news/technology-17178954

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.

Box 4: Life cycle security measures

Data integrity and availability are essential elements in the provision of cloud computing services. According to Directive 95/46/EC, 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 (Article 17).

The problem is that the concept of appropriate has been interpreted in different ways throughout EU Member States. Thus, although cloud service providers (CSPs) quite often implement widely recognized technical standards (e.g. ISO 27001) to secure customer data, these may not match perfectly to national requirements for appropriate measures. Further consistency and harmonization across the EU is required.

5.2 Using PETs

One objective of ICT standards is to define appropriate and effective technical measures for implementing privacy principles in cloud computing. Existing ICT standards are represented in Table 2 and defined below to illustrate some examples of PETs at different stages of the data life cycle.

The first example of PET in Table 2 is an implementation which would meet the data proportionality principle. According to this principle, the data controller must make reasonable efforts to limit the processed personal data to the minimum necessary. A system should be designed to collect only the minimal amount of data for a given purpose [20]. One relevant PET for this principle is the anonymous credential. Such a system allows a user to obtain a credential from one organization and then later prove possession of this credential to another organization without revealing anything more. Anonymous credential systems also allow selective disclosure by permitting the user to reveal some credential attributes or prove that they satisfy some properties (e.g. age < 25) while hiding all the other credential attribute information (this is in contrast to classic credentials which allow only the release of all the contained attributes). Two implementations of anonymous credentials currently exist. The first, Idemix [14], developed by IBM, is based on group signatures. The second, U-Prove, recently proposed by Microsoft, is based on blind signatures and the work of Stefan Brands [3].

The customer can anonymously access various cloud services without revealing to the service provider more about himself/herself than what is strictly needed to check his/her rights. In order to reduce the traceability of the user's transactions and respect his/her privacy, the data disclosed by the application are minimized. This PET should enable users to register with and obtain a service from a cloud provider. The credential includes the proofs of validity (e.g. rights to access) needed to consume cloud services, storage space or digital contents such as cloud-based video on demand.

Table 2: Technologies for privacy protection measures in the data life cycle

Data life cycle	Privacy principles	Privacy protection measures	Examples of PETs and ICT standards
Collection	Proportionality and purpose specification	Data minimization	Anonymous communication Anonymous credential Group and blind signatures ISO/IEC JTC1/SC27 WG2 and WG5
Storage	Accountability, Security measures Sensitive data	Confidentiality	Encryption AES NIST (FIPS 197)
Sharing and processing	Lawfulness and fairness, consent, right of access	Data access control	Privacy dashboard OASIS XACML, ITU-T X.1142
Deletion	Openness, right to delete	Confidentiality	Deletion Anonymization protocol Hash functions ISO/IEC JTC1/SC27 WG2

A second example involves the duty of confidentiality. The data controller and those involved at any stage of the processing have a duty to maintain the confidentiality of personal data. This obligation remains in force even after the cessation of the relationship with the data subject or, where appropriate, the responsible person. Cloud-stored data needs to be highly secured, for example by encrypting data processing in the cloud. Encryption is a fundamental tool that is recognized by security experts as guaranteeing the confidentiality of data. When implemented correctly, along with associated security keys and data management policies, encryption enables the user and the enterprise to isolate data and associated policies, particularly in shared, multi-tenant environments like cloud storage. Nevertheless, these methods could be very expensive in terms of computing power. The benefits gained with cloud computing are cancelled out by the overhead introduced when handling encryption of data making the processing of encrypted data unpractical for most use cases [7]. It is one of the big questions, if and how encryption and cloud computing can come together in a meaningful way.

Confidentiality is a key issue where personal data are of a sensitive nature. This applies in particular to personal data relating, for example, to racial or ethnic origin, political opinions, religious or philosophical beliefs, as well as to health or sexuality-related matters.

For the future of ICT standards, it could be interesting to take into account recent advances for processing of encrypted data such as the "*searchable encryption scheme*". Researchers can provide mechanisms capable of encrypting data in such a way that a token can be generated to allow a third party to search over the encrypted data. Using a searchable encryption scheme, a client can safely store its data with an untrusted cloud provider without losing the ability to search over it. One example given by Microsoft to illustrate the possibility for using this technology is electronic health. Given the importance and sensitivity of health-related data, it is clear that any storage platform for health records will need to provide robust confidentiality and integrity guarantees to both patients and healthcare service providers [17].

A third example involves the rights of the data subject. The possibility for a user to control his/her personal data as it is processed by applications is a fundamental right. To provide users with greater transparency and control over their own data, a dashboard can be used to summarize data used by applications and provide links to personal setting controls. There is a proposal by Google to offer a view into the data associated with the Google account. The Google dashboard is designed to give data subjects control over their data. It summarizes the data associated with each Google product (including Gmail, Calendar, Docs…) and provides links to personal setting controls. Nevertheless, European data protection authorities have

expressed concern over Google's measures. The French data protection authority, Commission Nationale de l'Informatique et des Libertés (CNIL), has been designated European data protection authorities to verify that the new privacy policy proposed by Google does not breach European data protection laws[20].

One important standard in the field of policy language for expressing information system security policy is the OASIS eXtensible Access Control Markup Language (XACML) standard – also available as Recommendation ITU-T X.1142 – which provides a standardized solution for implementing access control policy. Thanks to a dashboard solution based on XACML, a user can define preferences to control which entity (service provider for example) can access which data according to policies.

At the end of the contractual relationship between a data subject and his/her cloud provider, the data subject has the right to request from the responsible person the deletion of personal data that might be unnecessary. Technical measures and methodologies can offer solutions for securely deleting or anonymizing personal data. Standards should be very useful for defining requirements and avoiding the disclosure of personal data, as happened in 2006 with the privacy breach experienced by AOL owing to incorrect anonymization of the data of hundreds of thousands of users that had been posted online for processing by researchers.

6. Standardization activities

Despite growing concern about privacy in cloud computing, there is still a lack of standards. To foster adoption of cloud services, standards will set requirements for the assessment and selection of solutions that meet the expected level of security and privacy.

Work on standards is now in progress. Over the last few years, several bodies have been involved in efforts to develop an information privacy protection standard, and the main SDOs have now begun to study cloud computing. This section of the report summarizes the standard and best practice development activities now being pursued in the interests of protecting privacy in the cloud.

6.1 International Telecommunication Union (ITU)

ITU-T SG 17 has been working on cloud computing security since April 2010. The following five work items were recognized and are currently in progress:

- Security guideline for cloud computing in telecommunication area (draft Rec. ITU-T X.ccsec)
- Security requirements and framework of cloud based telecommunication service environment (draft Rec. ITU-T X.srfctse)
- Requirement of IdM in cloud computing (draft Rec. ITU-T X.idmcc)
- Framework of the secure service platform for virtual network (draft Rec. ITU-T X.fsspvn)
- Security functional requirements for Software as a Service (SaaS) application environment (draft Rec. ITU-T X.sfcse).

In addition, several work items addressing technical measures for PII protection are likewise assumed to be of interest in the context of cloud computing:

- Guideline for management of personally identifiable information for telecommunication organizations (draft Rec. ITU-T X.gpim)
- Guideline on anonymous authentication for e-commerce service (draft Rec. ITU-T X.sap-5)
- eXtensible Access Control Markup Language (XACML) 3.0 (draft Rec. ITU-T X.xacml3)
- Telebiometrics related to physics/chemistry/biology/culturology/psychology (draft Recs. ITU-T X.th2, X.th3, X.th4, X.th5, X.th6)

[20] See www.cnil.fr/la-cnil/actualite/article/article/les-nouvelles-regles-de-confidentialite-de-google-soulevent-des-inquietudes/?tx_ttnews%5BbackPid%5D=2&cHash=040aec30fbe8a27b0688e33bd0984536

- Integrated framework for telebiometric data protection in e-health and worldwide telemedicine (draft Rec. ITU-T X.tif)
- Criteria for assessing the level of protection for personally identifiable information in identity management (draft Rec. ITU-T X.priva)
- Open identity trust framework (draft Rec. ITU-T X.oitf).

The Focus Group on Cloud Computing (FG Cloud), set up in June 2010, has identified cloud data security as an important study item for ITU-T. The group considers that telecom providers have an important role to play in this domain since they are seen as a trusted partner by consumers such as enterprises and end-users. FG Cloud has concluded its work on cloud security threats and requirements from both a user and a service provider perspective in December 2011 and has made proposal for a study item on cloud security in ITU-T SG 17.

6.2 International Organization for Standardization (ISO)

The main ISO/IEC technical committee for the discussion of privacy and IT security standards is JTC 1/SC 27. This includes standards for privacy-enhancing technologies and especially credential-based solutions. The subject of anonymous authentication mechanisms intersects with the standardization work being done in two SC 27 working groups (WGs), namely WG2, which develops standards based on algorithms such as blind and group signatures, and WG5, which works on requirements and guidelines.

WG5 is responsible for other privacy standards, the most advanced of which are ISO/IEC 29100 Privacy Framework and ISO/IEC 29101 Privacy Architecture Framework:

- The Privacy Framework serves as a basis for the technical reference architecture, implementation and use of specific privacy technologies and overall privacy management, privacy controls for outsourced data processes, privacy risk assessment and specific engineering specifications.
- The Privacy Architecture Framework guides the implementation of controls associated with a privacy framework to ensure the proper handling of PII within an information and communication technology environment.

ISO/IEC JTC 1/SC 27 has decided to establish a study period (Cloud Computing Security and Privacy) to investigate the security requirements for cloud computing and what would be a feasible program of standards work to meet these requirements. The respective SC 27 working groups are dealing with topics such as information security management, risk management, application and network security, cybersecurity, business continuity, privacy and identity management. The study period will also consider contributions from ITU-T, SC 38 and other groups involved in cloud computing security.

ISO/IEC JTC 1/SC 38 (Distributed Application Platforms and Services) has established a Study Group on Cloud Computing (SGCC) in order to provide JTC 1 with cloud computing standardization issues and develop new proposals for cloud computing work items to be studied in JTC 1. The security issues in JTC 1/SC 38/SGCC are currently under consideration.

6.3 Organization for the Advancement of Structured Information Standards (OASIS)

OASIS is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. The OASIS IDCloud (Identity in the Cloud) Technical Committee (TC) works to address the serious security challenges posed by identity management in cloud computing. The IDCloud TC identifies gaps in existing identity management standards and investigates the need for profiles to achieve interoperability within current standards. It performs risk and threat analyses on collected use cases and produces guidelines for mitigating vulnerabilities. The purpose of the TC is to harmonize definitions/terminologies/vocabulary of identity in the context of cloud computing, identify and define use cases and profiles, and identify gaps in existing identity management standards as they apply in the cloud.

6.4 Cloud Security Alliance (CSA)

CSA's mission is to promote the use of best practices for providing security assurance within cloud computing and to provide education on the uses of cloud computing to help secure all other forms of computing[21]. Nine CSA working groups are looking into the development of best practices to secure the cloud:

- Group 1: Architecture and Framework
  Responsible for technical architecture and related framework definitions.
- Group 2: Governance, Risk, Compliance (GRC), Audit, Physical, Business Continuity Management (BCM), Disaster Recovery (DR)
  Responsible for governance, risk management, compliance, auditing, traditional/physical security, business continuity management and disaster recovery.
- Group 3: Legal Issues: Contracts and E-Discovery
  Responsible for legal guidance, contractual issues, global law, eDiscovery and related issues.
- Group 4: Portability, Interoperability and Application Security
  Responsible for application layer security issues and developing guidance to facilitate portability and interoperability between cloud providers.
- Group 5: Information Management and Data Security
  Responsible for identity and access management, encryption and key management, identifying enterprise integration issues and solutions.
- Group 6: Data Center Operations and Incident Response
  Responsible for incident response and forensics, as well as identifying new issues related to cloud-based data centre operations.
- Group 7: Information Lifecycle Management and Storage
  Responsible for data-related issues in the cloud.
- Group 8: Virtualization and Technology Compartmentalization
  Responsible for understanding how to compartmentalize technologies used for multi-tenancy, including, but not limited to, virtualization.
- Group 9: Security as a Service
  Responsible for understanding how to deliver security solutions via cloud models.

Some of the work of CSA includes best practice documents (referred to as security guidance) on how to secure the cloud. Cloud Controls Matrix is a security control framework for cloud providers and cloud consumers, and the Cloud Trust Protocol will serve as a mechanism for cloud service consumers to request and receive information from cloud service providers in order to meet security, privacy and compliance requirements.

[21] See https://cloudsecurityalliance.org/about/

7. Conclusion

Cloud computing is still in its infancy. This is an emerging technology which will bring about innovations in terms of business models and applications. The widespread penetration of smartphones will be a major factor in driving the adoption of cloud computing. However, cloud computing faces challenges related to privacy and security.

The global dimension of cloud computing requires standardized methodologies and technical solutions to enable stakeholders 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 stakeholders 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.

In cloud services, the implementation of PETs will depend on the availability of standards to assess privacy risks and describe means of ensuring data protection compliance. PETs can ensure that breaches of the data protection rules and violations of individuals' rights are not only forbidden and subject to sanctions, but are also a technically daunting undertaking. The embedding of privacy by design features when designing technologies is increasingly supported by regulators and is also being included in the reform of the EU Data Protection Directive.

Cybercriminal activities impacting cloud computing environments – for example, fraud and malicious hacking – are threats that can undermine user confidence in the cloud. Cloud computing providers face multiple, and potentially conflicting, laws concerning disclosure of information. Achieving a better understanding of jurisdictional issues is critical and should be tackled through enhanced dialogue.

ITU could have an enabling role to play in developing technical standards, guidelines and methodologies for implementing privacy by design principles, including assessment of risks to personal information in the cloud. These can be used as best practices by service providers in order to ensure compliance with legal frameworks for personal information protection. ITU could consider organizing an event on this topic to promote the standards work being done in this area. ITU-T SG 17 has taken the initiative, through a number of study Questions, to work on specific topics related to cloud security. However, a good deal of work remains to be done in the area of cloud privacy. Cloud security is set to form a major part of SG 17's future work, while extensive collaboration with other standardization bodies and industry groups would help to expedite progress and avoid duplication of effort.

Bibliography

[1] G.W. Van Blarkom, J. B. (2003). *Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents.* Retrieved from e-Europe: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15263-00-2005-Apr.pdf

[2] Prof. Ian Goldberg, D. W. (n.d.). *Privacy Enhancing Technologies for the Internet.* Retrieved from University of California, Berkeley: www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html

[3] Brands, S. (2000). *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. The MIT Press; ISBN 0-262-02491-8.

[4] Cavoukian, A., & Abrams, S. T. (2010). *Privacy by Design: essential for organizational accountability and strong business practices.* Retrieved from www.globalprivacy.it/Allegati_Web/57C2B8AA758546A0B76D5668F5CF5E16.pdf

[5] The Danish Data Protection Agency. (2010). *Processing of sensitive personal data in a cloud solution.* Retrieved from www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/

[6] ENISA. (2009, Nov.). *Cloud computing information assurance framework.* Retrieved from ENISA: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework

[7] ENISA. (2009). *Cloud Computing Security Risk Assessment.* Retrieved from www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[8] ENISA. (2011). *Security & Resilience in Governmental Clouds.* Retrieved from www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

[9] Enterprise Privacy Group. (2008). *Privacy by Design: An Overview of Privacy Enhancing Technologies.* Retrieved from www.ico.gov.uk/upload/documents/pdb_report_html/pbd_pets_paper.pdf

[10] Federal Trade Commission. (2010). *Protecting Consumer Privacy in an Era of Rapid Change: A proposed framework for businesses and policymakers.* Retrieved from www.ftc.gov/os/2010/12/101201privacyreport.pdf

[11] Gartner. (n.d.). *Worldwide Cloud Services Market to Surpass $68 Billion in 2010.* Retrieved from www.gartner.com/it/page.jsp?id=1389313

[12] IDC. (2008). *IT Cloud Services Forecast.* Retrieved from http://blogs.idc.com/ie/?p=224

[13] IDC. (2010). *IDC Predictions 2011: Welcome to the New Mainstream.* Retrieved from www.idc.com/research/predictions11/downloads/IDCPredictions2011_WelcometotheNewMainstream.pdf

[14] IBM. (n.d.). *Identity Mixer.* Retrieved from www.zurich.ibm.com/security/idemix/

[15] ITU-T Technology Watch Report. (2009). *Distributed Commuting: Utilities, Grid & Clouds.* Retrieved from www.itu.int/dms_pub/itu-t/oth/23/01/T23010000090001PDFE.pdf

[16] Mell, P., & Grance, T. (2009). *NIST Definition of Cloud Computing.* Retrieved from NIST www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

[17] Kamara, S., & Lauter, K. (2010). Cryptographic Cloud Storage. *Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization.*

[18] Horrigan, J. (2008). *Use of Cloud Computing Applications and Services.* Retrieved from Pew Research Center: www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx

[19] Article 29 Data Protection Working Party. (2009). *The Future of Privacy.* Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

[20] Madrid Resolution, International Standards on the Protection of Personal Data and Privacy, International Conference of Data Protection and Privacy Commissioners. 5 November 2009. Retrieved from www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

ITU-T Technology Watch surveys the ICT landscape to capture new topics for standardization activities. Technology Watch Reports assess new technologies with regard to existing standards inside and outside ITU-T and their likely impact on future standardization.

Previous reports in the series include:

Intelligent Transport Systems and CALM
ICTs and Climate Change
Ubiquitous Sensor Networks
Remote Collaboration Tools
NGNs and Energy Efficiency
Distributed Computing: Utilities, Grids & Clouds
The Future Internet
Biometrics and Standards
Decreasing Driver Distraction
Standards and eHealth
The Optical World
Trends in Video Games and Gaming
Digital Signage

http://www.itu.int/ITU-T/techwatch

Printed in Switzerland
Geneva, 2012