

*An authoritative contribution to the
European Commission's Public Consultation*

*New Challenges for Privacy:
advanced technologies, effective legal frameworks
and active responsibility*



European Privacy Association (ABSL)
Square de Meeus, 37 - 4th Floor
1000 Brussels, Belgium

Telephone: +32 2 791 75 18
Fax: +32 2 791 79 00

info@europeanprivacy.eu
www.europeanprivacy.eu

December 2009

About the European Privacy Association

The European Privacy Association is a non-party-political pan-European network of privacy, data protection and security experts based in Brussels, Belgium. Its aim is to provide a 'space' for bringing together experts from across Europe, to engage with them as we seek out new policies to enhance privacy, e-security and data protection. EPA will work closely with European institutions, particularly the European Parliament, academia, civil society, and industry. EPA will engage with policy makers, industry, advocates, and the media, to bring forward new ideas and to propose policy frameworks to deal with pressing privacy issues as they arise. EPA will therefore be a clearinghouse for new ideas on preserving and enhancing privacy protection across Europe.

Members, the Policy & Scientific Advisory Committee and the Executive Board of EPA are delighted to have been given the opportunity to contribute to the Commission's consultation. The ever increasing, global, challenges relating to Privacy, whether in the legal, technical, political or academic sphere, and how this affects both private and public sector makes our contribution and the Commission's response all the more important. We look forward to continuing to work with the European Commission.

Background and purpose

The EU Commission, DG Freedom, Security and Justice has invited citizen, organisations and public authorities to submit their contributions to a public consultation on the legal framework for the fundamental right to protection of personal data within the period 9 July to 31 December 2009.

The European Privacy Association, EPA, hereby submits a contribution to the consultation, which is based on analyses, comments and examples collected among the members of the EPA Policy and Scientific Committee, the EPA Executive Board as well as members of the EPA Industry Forum.

The purpose of this note is, thus, to provide the EU Commission with information and knowledge stemming from highly respected European researchers within the field of privacy and from leading and innovative industrial actors within IT and communication.

This brief focuses on advanced technologies and challenges derived from the application of such technologies to handle and analyse personal data as part of public or private administration, communication or other activity.

In the first part, we describe a number of advanced technologies and identify positive and negative impact on the fundamental right to protection of privacy and personal data is highlighted. Where possible, we assess whether the existing legal framework provides effective protection and identify viable and sustainable solutions. The point of departure is taken in the responsibility of public authorities, private corporations and organisations to actively ensure that they respect and support privacy protection and are not complicit in privacy abuses. To this, we add requirements for viability and sustainability; hence, solutions must be robust and realistic in a short run perspective, and contain the potential for positive impact on data protection now and in the future.

In the second part, we discuss a number of challenges that are derived from the existing definitions and requirements under the EU Data Protection Directives and other relevant directives, and poses significant challenges for industry as well as for other stakeholders.

The last part of the brief contains the concluding observations of the European Privacy Association, which focuses on the need for further harmonisation of EU regulation within the field of data protection, suggestions for future supplementary regulation and self-regulation as well as for effective enforcement.

ADVANCED TECHNOLOGIES

1. Biometrics

1.1. Challenges

Over the last years, we have seen an increasing tendency to use biometrics for authentication purposes – in passports, ID-cards, at border controls etc. One challenge is that while other authentication techniques may offer degrees of pseudonymity or anonymity (for instance by attribute authentication), this is not possible with biometric authentication.¹

There are two sources of error when it comes to biometric matching: The system may identify an individual incorrectly against the claimed identity. This is referred to as false acceptance. If a biometric system fails to identify an individual that is registered in the system, it is referred to as false rejection. The probability that a system will incorrectly identify an individual is thus referred to as the False Acceptance Rate (FAR) whereas the probability that the system will fail to identify an enrollee is called False Rejection Rate (FRR).²

One of the challenges with tuning a biometric system is that if we set the threshold at a level where no one is falsely identified, the rejection rate will increase, and vice versa.

Biometric technologies can be based on many different physical characteristics. There are different challenges associated with the different characteristics:

Fingerprint recognition

Most of the fingerprint recognition systems that exist are based on proprietary algorithms associated with the manufacturer of the sensor. This means that in order for the system to work, the sensor and algorithm used for capturing and storing the biometric template must be the same as the one used for identification or verification at a later stage. In systems that use biometric templates, the idea is that even if you can breach the security of the storage medium, you should not be able to reconstruct the original fingerprint. Due to the lack of interoperability and standardisation in the field, using the same system for both capturing and verification is not always possible, in particular with law enforcement systems and border control systems where different countries and organisations are involved. As a result, the original image has to be stored in the database for these kinds of systems, leading to an increased risk of the fingerprint being compromised in case of security breaches.

Automated Facial Recognition

Automatic face recognition systems are systems where a person's image is captured automatically and compared to a database for identification or verification. As identification of a random person based on this technique would require an extremely large database, so such systems are normally used to verify that a person captured by the camera is not on a list of for instance known criminals or terrorists. The increase in CCTV over the last 10 years has led to more interest in the application of automatic face recognition.

Tests done by the German magazine c't show that systems may be fooled by still images or video loops.³

Another security limitation is the high incidence of twins. In addition to the spoofing potential, several other arguments have been launched against Automatic face recognition systems.⁴

1 From Extract from ESSTR Deliverable D1-6 "Responses to Terrorist Threats"

2 ICAO TAGMRTD/NTWG (2004) Biometrics Deployment of Machine Readable Travel Documents

3 Thalheim et.al (2002) *Body Check*

High potential for abuse

Pervasive automatic face recognition could be used to track individuals. If systems operated by different organizations can be matched to each other, it will be possible to track an individual from place to place.

Information may be combined with information from other technologies

Face recognition is the biometric technology that requires the least cooperation from the individual. This means that there is a bigger chance of having your biometric features captured without your knowledge with this technology. Information from face recognition systems is also easily combined with so-called location technologies.

Low accuracy rate

The technology has a low accuracy rate. Among the potential downsides are false positives, where a person might mistakenly be confused with a criminal or a terrorist. Conditions for image capture and recognition in most public places are not ideal, and this makes it more likely that errors will occur. As the database of facial images grows bigger, the chances of a false match to one of those images grows proportionally larger.

Citizens are unaware of the capabilities of surveillance systems

The public is poorly informed about the capabilities of surveillance cameras. They usually do not realize that through infrared images, or by extracting facial expressions, also elements relating to health or mood can be analysed.

DNA Identification

DNA or deoxyribonucleic acid is perhaps thought of as the ultimate identifier. Each person carries a unique genetic code (except for identical twins). Unlike fingerprints, there is no way to change a person's DNA by surgery or by rubbing away the prints.⁵

The analysis and processing of a DNA sample may reveal intimate information about a person, like hereditary factors and medical disorders. If a DNA sample is stored for an indefinite period of time, future technology may make it possible to extract even more information than today.⁶

DNA tests are difficult to circumvent under certain conditions (supervised sample collection with no possibility of data contamination). If sample collection is not supervised however, an impostor could submit anybody's DNA. We all leave DNA traces wherever we go (a single hair can provide a sample) and so it is impossible to keep DNA samples private.⁷

Spoofing

Spoofing is a general problem with biometrics. One way to try and avoid spoofing is by implementing so called liveness detection. By monitoring live characteristics like pulse or papillary response, the biometric devices become a source of sensitive biometric data:⁷

- Pupillary response depends on whether one has been drinking or taking drugs, pregnancy and age
- Changes in blood flow are associated with several medical conditions, as well as with emotional response
- Nervousness can be recognised in a voice-pattern

Social exclusion

4 Agre, P. E. (2003) *Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places*

5 OECD Working Party on Information Security and Privacy (2004): *Biometric-based technologies*

6 Van der Ploeg, I. (2005): *Biometric Identification Technologies: Ethical Implications of the Informization of the Body*

7From www.biteproject.org

The use of biometrics could lead to people being socially excluded without a reason. For most biometrics there is a small percentage that cannot enrol to a system that uses the biometric that they have a problem with.⁸

Security

One of the major advantages with biometrics is that they are so strongly linked to a person. They cannot be lost or revealed by accident, like a password or a PIN code. This means that other types of personal data can better be protected by using biometrics, than by traditional methods. Biometric authentication provides better access control, and identity theft becomes a lot more challenging when personal data are linked exclusively to the right person.⁹

This is, however, also the greatest liability of biometric systems. Once a set of biometric data has been compromised, it is compromised forever. For authentication systems based on physical tokens such as keys and badges, a compromised token can be easily cancelled and the user can be assigned a new token. Similarly, user IDs and passwords can be changed as often as required. But the user only has a limited number of biometric features (in most cases one face, ten fingers, two eyes). If the biometric data are compromised, the user may quickly run out of biometric features to be used for authentication.¹⁰ In cases of identity theft, it would be very difficult for the victim to prove misuse by an impostor.

1.2. Assessment of legal framework

Today, it is not fully clear how biometric data should be assessed within the EU Data Protection Directive. One question is whether biometric data should be categorized as sensitive data, and in the affirmative, whether this should cover all biometric data or just data revealing e.g. health sensitive data.

Other questions are linked to usage and linkage of biometric data with other data sets; if a company uses biometric data, e.g. fingerprints as part of an access control scheme, and link such data to other personal data on the staff as well as e.g. biometric data such as retinal patterns of the eye (for specific authentication purposes), two questions arise:

- a) if the compilation of non-sensitive data reveals a detailed profile of a person, should such data compilation in itself be seen as protected under the Directive provisions on sensitive data,
- b) how should we handle the compilation of biometric data, sensitive as well as non-sensitive, that are linked to other data sets; are the requirements in the directive sufficient to provide the citizen with adequate data protection.

The answers to such questions presuppose clarification of whether the so-called hash value of biometric data can be transformed into data revealing biological or genetic information about a specific person. Such regeneration is challenged by scientists, but consensus does not seem to have emerged. This is especially important in relation to the use of DNA, retinal patterns of the eye, thermogrammes and other biometric data building on physical or genetic data and as such may contain information regarding a person's permanent or temporary health issues.

⁸From Extract from ESSTRT *Deliverable D1-6 "Responses to Terrorist Threats"*

⁹Albrecht, A. (2003) *BIOVISION: Privacy Best Practices in Deployment of Biometric Systems*

¹⁰Ratha, Connell and Bolle (2001) *Enhancing security and privacy in biometrics-based authentication systems*

2. Cloud computing

2.1. Challenges

This is one of the most promising and novel Internet-related technologies. It is based on the “Cloud Computing Services¹¹” idea, i.e. that computing will be increasingly be delivered as a service from vast warehouses of shared machines. Documents, e-mails and other data will be stored on-line, “in the cloud”, making them accessible from any PC or mobile device. This emerging network architecture pits applications residing on third-party servers, managed by private firms that provide remote access through web-based devices. This is supposed to make life easier and cheaper for consumers: no need to install new software and, generally, availability of free service (supported by advertising or subsidised by the few users who pay for premium service).

The three main risks about which awareness should be promoted, and solutions offered and advanced, are: (i) Profiling-related consumers’ privacy; who is unwilling to pay for cloud-based services, will have to come to terms with some advertising based on her on-line activity¹²; while most users will be happy to trade some privacy for free services, it is increasingly clear that such a “voluntary” release of personal data and information is not often very informed; (ii) Data stored in the cloud may not be safe; data security breaches and data loss/destruction are ever more becoming consumers’ main concern –and, in the US, the focus of practically all legislative and regulatory effort, at both federal and state levels; (iii) Consumers, once released their data “in the cloud”, as opposed to the current practice to store them in the comfort of their personal PCs, or their servers¹³, may not technically “own” them any longer (unless otherwise unambiguously stated in service contracts), possibly being left at the whim of cloud computing services providers¹⁴, and/or to lock-in arrangements, and/or possible failures by the telecommunication systems, needed to retrieve their personal data.

Other important issues arise from the concern that a single giant provider may establish a dominant position, acting as the ultimate controller of billions of personal/sensitive data, or from the indefinite retention of search histories by search engines¹⁵.

2.2. Assessment of Legal Framework

According to one of the most authoritative analyses so far offered by the IT industry, “...As more and more consumer and enterprise data moves into the cloud, increasing uncertainty about the legal and regulatory obligations related to that data could jeopardize the benefits of cloud computing.”¹⁶

Such perceived, and definitely not baseless, uncertainty does not seem to be at odds with the concerns voiced by the EU Commission, which did not dismiss the option of “further legislative or not legislative initiatives”, as

11 The technology may come in three forms: a) “Software as a Service”, or SaaS; b) Capacity Cloud Computing; c) Software Cloud Computing

12 Such is what the US Federal Trade Commission (FTC) defines “Online Behavioral Advertising”, or the “Tracking of a consumer’s online activity”. In February, 2009, the agency released a Staff Report setting forth self-regulatory principles which should govern companies engaged in such commercial practice.

13 However, many information society common services, like e-mail, are already web-based.

14 That would allow possible scenarios of “data hostages”, where consumers would be denied access to their data, for instance in the event of non-payment of fees; currently, several cloud computing services providers already state in their Terms and Conditions of Use that information provided become their property, that they will not accept liability for damages, that they reserve right to discontinue or disconnect service for whatever reason, with or without notice, etc. See the Cloud Computing page on the EPIC’s website; the EPIC (Electronic Privacy Information Center) is a US powerful privacy advocacy group, strongly engaged in the public discourse over these issues.

15 See “Battle of the Clouds”, *The Economist*, Oct. 17-23, 2009, at 13.

16 Microsoft Trustworthy Computing, “Privacy in the Cloud Computing Era. A Microsoft Perspective”, Nov. 2009.

necessary to “maintain”, “...in the light of the speed of technological change”¹⁷ the high level of protection so long afforded by the current legal framework.

Specifically, it is apparent that, in this context, jurisdiction, data security and transfer of data, together with the above-mentioned consumer-related concerns, are becoming issues of top relevance, for purposes of thoroughly assessing the adequacy of such current legal framework.

On jurisdiction, the EU regulators’ well-settled stance reflects the adoption of a very expansive interpretation of the Art. 4 of 46/95/EC Directive¹⁸. In a far-reaching 2002 opinion, the Article 29 Data Protection Working Party adopted a resolution addressing the application of EU data protection law to non-EU websites¹⁹, focusing on the “making use of equipment” language in Art. 4 (1)(c) of the Directive. The 2008 Working Party’s opinion on search engines²⁰ reaffirmed the stance, citing its 2002 Document, again stating that performing “activities” (at stake, in the 2002 Document, was the cookies setting) involving a local user’s PC is enough to found application of EU data protection law. Further, if the processing of personal data²¹ takes place in the context of “establishment” – expansively, again, defined as to include a local office, a subsidiary, or a third-party agent – in the territory of a Member State under Art. 4 (1)(a), then EU protection law applies.

Since, as per the search engines²², even local customer support, or ad sales, would constitute processing of personal data in the context of an establishment, thus virtually every web site collects and processes personal data; and if the site is accessed by an EU server, it is potentially subject to EU data protection law²³.

With regards to the impact of such regulatory interpretations, this contribution’s tentative stance is that an over-restrictive regime, in terms of jurisdiction-based regulatory enforcement, would only be prone to promote, in the age of the cloud computing, a technological forum-shopping of some sort²⁴.

As per developments in the area of trans-border data flows, while all data transferring under Art. 25 of the 1995 Directive is still subject to the familiar restrictions, it is well worth noting that the Art. 29 Working Party has continued its efforts to provide guidance: in reference with the Binding Corporate Rules, it has published a list of the items that should not be overlooked by companies, when drafting the BCRs²⁵; as recently as March, 2009, it issued an opinion to update the standard controller-to-processor contract clauses²⁶. For its part, the Data Protection Unit of the Directorate-General for Justice, Freedom and Security published a very useful and detailed FAQ paper addressing the various options for dealing with cross-border data transfers²⁷.

17 All quotations in italics from: *Communication from the Commission to the European Parliament and Council*, COM (2009) 262, final, Brussels, June 10, 2009.

18 See, for a useful overview, Arien Siegel *et al.*, “Survey of Privacy Law Developments in 2009: United States, Canada and the European Union”, American Bar Association Section of Business Law, *The Business Lawyer*, Vol. 065 – No. 01, Nov. 2009, pp. 300-301.

19 “Art. 29 Data Prot. Working Party, Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites” (May 30, 2002) (WP 56), cited in A. Siegel, *supra*.

20 “Art. 29 Data Prot. Working Party, Opinion 1/2008 on Data Protection Issues Related to Search Engines” (Apr. 4, 2008) (WP 148), cited in A. Siegel, *cit. supra*.

21 Note that the Art. 29 WP’s view is that an IP address, by itself, can constitute personal data. See WP 148, *supra*, at 9.

22 However, Google has challenged the applicability of EU data protection law. See A. Siegel, *cit., supra*.

23 *Id.*

24 The new technological architecture, in fact, makes all but possible such an outcome: think of the Roy Bates’ “Principality of Sealand” saga, where the server is located at bay, in international waters, or the likeness that private operators will soon be able to launch satellites—for example, Mr. Branson of *Virgin Atlantics* anticipated that his company envisions a program of tourist shuttles in orbit over the next years.

25 “Art. 29 Data Prot. Working Party, Working Document Setting Up a Table with the Elements and Principles to Be Found in Binding Corporate Rules” (2008) (WP 153), cited, in the context of this discussion, by A. Siegel, *cit. supra*.

26 “Art. 29 Data Prot. Working Party, Opinion 3/2009 on the Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, Under Directive 95/46/EC” March 5, 2009 (WP 161).

27 See discussion in A. Siegel, *cit. supra*, at 303, in reference with the Directorate’s document: “Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries”.

The impact of the overall restrictions on the free flow of data to third countries may represent a burden for the EU business community, that to a certain degree outweighs the presumed benefits in terms of users' privacy, and add a confusing element of the sometimes-inconsistent implementation in the Member States' national legislations²⁸.

As such, the multinational companies' obligations to comply, in the event of litigation, from one side, with the US discovery and E-discovery civil proceedings rules²⁹, and, from the other side, with the EU data protection laws, has currently the chilling effect of leaving businesses in a thoroughly awkward exposure to sanctions or possibly adverse outcomes in both jurisdictions³⁰, especially whereas, in the context of cloud computing technology, companies would choose to take advantage of the hugely enhanced cloud data storages and overall cost-saving services, available with the new technology.

In reference with the issues related to data retention and users' search histories over the Internet, the above cited Working Party 2008 Opinion on search engines is, of course, the *locus* where to seek for some guidance about the European positions. Under such Opinion, the applicability of the Data Protection Directive include also search engines operating outside the EU³¹, even – due to the breadth, as above reminded, of WP's interpretation of "making use of the equipment" – when they do not have a place of business or a data centre in the EU³². Consequently, the WP adopts the view that search engines are the controller of the personal data contained in their search indexes³³, and, as such, fully responsible for compliance with EU data protection law, including the right of individuals to request updates or deletions of their personal data³⁴, and including the data security requirements, statutory in some Member States³⁵.

The same WP Opinion reiterates that general principles of limitation of data retention time limits, pursuant to 2006/24 Directive, not extending, however, the latter's overall applicability from ISPs and TC companies as to include search engines. Therefore, while allowing search engines to retain personal data for a time necessary for the specific purpose of the processing³⁶, but not for longer than the Data Retention Directive threshold of six months, both notice and following-session-deletion requirements under the Data Protection Directive are in full force.

In the related and crucial area, all the more in the cloud context, of the breach notification, in May 2008, WP 29 and the European Data Protection Supervisor (EDPS) published opinions supporting mandatory notification to users by ISPs and TC companies for breaches of personal data³⁷. The new rules, proposed by both opinions, would enhance the currently-rarely-applied data breach requirements, effectively covering any on-line service providers, including health care, banking and insurance institutions, thereby much better addressing what is all but sure to become the real single major concern of consumers/users in the cloud era.

28 See the comprehensive review, contained in the American Chamber of Commerce to the European Union *Position Paper on International Transfer of Personal Data*, Brussels, Dec. 3, 2008, calling for a "flexible mechanism for international data transfer" as "key for companies operating on both sides of the Atlantic", and welcoming "any effort to build upon the already existing exceptions under the Directive to further improve the management of personal data in an international context."

29 Leaving alone other stringent compliance rules, like those imposed by the Serbanes-Oaxley Act, when it comes to corporate internal investigations, or, worse, public prosecutors' investigations in instances of suspected criminal malfeasance.

30 While Member States' national data authorities, in some cases, like e.g. Italy, do not hold an official position on this issue, developments like the French CNIL recent rigid *Deliberation*, which followed suit the Art. 29 WP Recommendation of February 2009 (WP 158), do not help easing matters for cross-border legal and corporate compliance.

31 See WP 148, cit. *supra*, at 8.

32 See A. Siegel, cit. *supra*, at 303.

33 See WP 148, cit. *supra*, at 14.

34 *Id.* at 15; A. Siegel, at 304.

35 See, for example, Italy *Legislative Decree 196/2003*.

36 Under the three grounds outlined in the Opinion for legitimate processing – a) user's consent; b) performance of a contract with the user; c) search engine's legitimate interest – it is arguable that ground three is a catch-all tool for purposes of fraud preventing, system security; law enforcement and such. See A. Siegel, at 304.

37 "Art. 29 Data Prot. Working Party, Opinion on the Review of the Directive 2002/58/EC on Privacy and Electronic Communications (May 15, 2008) (WP 150); Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council Amending, Among Others, Directive 2002/58, 2008 O.J. (C 181).

2.3. Viable and Sustainable Solutions

Cloud computing technology is a great opportunity. Together with the above-reminded benefits for the consumers, companies, by switching to cloud-based e-mail, accounting and customer-tracking systems can reduce complexity and maintenance costs, because everything runs inside a web browser³⁸. The Internet scalability feature will allow substantial incremental improvements and major scale economies.

Furthermore, this technology can only be developed through high-capital-intensity and high-innovation investments. A regulation-biased weighing of the benefit/risk balance for the users' privacy would only have a chilling effect on entrepreneurial initiative.

The complexity of the legal aspects related to this truly globalized scenario, which is briefly summarized above, seem to suggest a flexible, consensus-building model, based on agreements among "Big Areas"³⁹, a contract-based approach, supported by strong tools of international private law.

While there is no doubt that end-consumers and/or data subjects, specially whereas they are in a weak bargaining position, must be afforded protection within the jurisdiction where the services are actually provided⁴⁰, it is most likely that this aim will be more effectively pursued through strong contractual frames/clauses - covering both choice of law and choice of forum - to be inserted in the SLAs ("Service Level Agreements"), and to be framed as being readily and effectively actionable, under generally accepted and agreed-upon principles of consumer protection, instead of relying on some sort of administrative-like "international data authority".

A more rigid approach, however, should instead be sought in reference with data security and breach notification requirements.

Loss, destruction of data, identity theft, retaliation on consumers, grounded on unfairly strong bargaining positions of the cloud computing service providers should not only constitute very serious administrative and/or criminal violations, directly prosecutable in the consumers' jurisdiction - for instance, through a mandatory-legal-representative mechanism, for purposes of ensuring enforcement⁴¹ - but also actionable at law and in equity (injunctions and "cease-and-desist" orders) through class-action-like procedural devices and expansive cross-border recognition/enforcement tools. International organizations recognized certifications, like ISO security standards, should be all but mandatory, together with stringent and demonstrable implementation of compliance programs and policies⁴².

Finally, while the reasonableness-based trends towards mitigating the burdensome limitations, under the machinery of the EU-originated transfers of data, should be encouraged⁴³, and diplomatic-minded positions on "building upon already existing exceptions"⁴⁴ should be supported, a review of the whole 95/46/EC Art. 25 mechanism, at least in terms of easing cross-border legal proceedings and corporate compliance major and burdensome concerns for multinational businesses on both sides of the Atlantic⁴⁵, is needed.

³⁸ *The Economist*, cit. *supra*, at 13.

³⁹ An acceptable conceptual approach may be found in the 2004 APEC "Privacy Framework", or in the 2007 OCSE "Recommendations".

⁴⁰ The accepted principles of private international law governing E-commerce and, in general contract and tort cross-border jurisdiction (Brussels Convention, Rome I and II, and the on-going efforts to amend them) may provide some solutions.

⁴¹ Perhaps modelled on the state "doing business" statutes in the US.

⁴² The EU Commission's suggestion to "propose sector specific legislation at EU level in order to apply those principles to the technology in question" may be of some guidance. See "Communication from the Commission to the European Parliament and Council", Brussels, COM (2007) 87 final, at 10. But cfr. also the call for the "development and promotion of international standards for personal data protection and in the conclusion of bilateral or multilateral instruments.". COM (2009) 262 final, cit. *supra*, at 9.

⁴³ See the recent, seemingly promising openings from the 29WP and the Directorate Data Protection Unit, cited and discussed *supra* in the text, at 4, and footnotes n. 16, 17, 18.

⁴⁴ See the AMCHAM EU Position Paper, cit. *supra*, footnote n. 20.

⁴⁵ In even more straightforward terms, the Commission's classification of the United States as a jurisdiction which does not guarantee "an adequate level" of data protection, should be altogether overruled.

3. Intellectual property

3.1. Challenges

With the ubiquity of digital formats, the opportunities for copying intellectual property have changed. So far, this has mostly been an issue for music and film, but it is increasingly becoming a problem with e-books and digital-TV.

DRM is a form of technical protection system to prevent illegal use of digital intellectual property. DRM normally consists of two elements:

- *Identification of the work*, so called digital rights information. This is information about the work and what rights the user has to the use (the right to store, copy, print etc.)
- *Technical functionality* to enforce the attributes described in the digital rights information.

The DRM-system normally works as a combination of information that comes with the content and functionality built into the software or hardware that will make the content available to the consumer. All forms of digital content can be protected with DRM – whether they are made available in the form of downloadable files, CDs or DVDs or digital TV-signals.

The digital rights information will then contain information about what use has been agreed for the file(s) and the player will relate to this information by for example only allowing the content to be played once, by not allowing a TV-program to be recorded or a film to be seen beyond a certain time frame.

Technically, there are many ways to implement DRM, but the most common is to encrypt the content. The consumer then has to prove that he or she has legitimate access to the content, for instance by authentication.

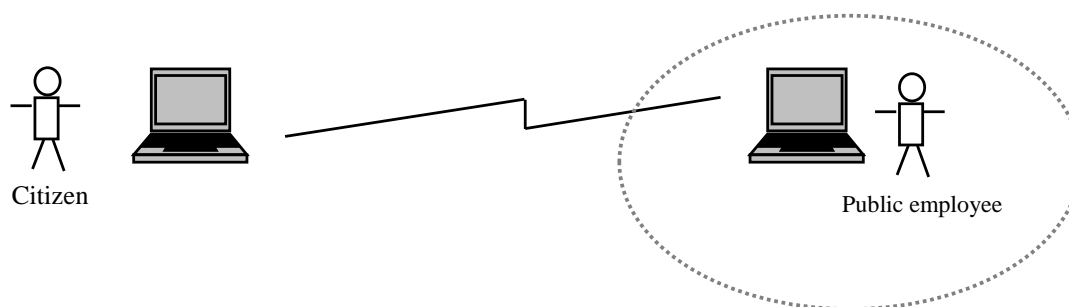
The use of DRM has led to privacy-concerns. Many of the DRM-systems demand that the user is authenticated to play for instance a media file. That way the distributor can get an overview of customers' media habits, and in theory use this for marketing purposes and in their pricing policy.

After a lot of pressure from consumers, most record labels abolished DRM, but it is still used for e-books, film and console and computer games. But because the illegal copying of music is seen as such a big problem to the music industry, they have started searching for other solutions.

4. Public administration and E-Government

4.1. Challenges

Traditionally contact between citizen and public services has been person to person, either in direct conversation, with telephone or letter. Even though computers have been used to perform public services since the eighties, the user interface was always a civil servant or another person employed by the public. With e-Gov, this communication will increasingly be through a machine interface – a computer.



Because of this, we will have to revisit some questions regarding risk and responsibility:

- Where does the responsibility of the public sector end, and where does the citizen's responsibility begin?
- What is "good enough" security?
- Is it enough to focus on the security of the public system, or do we also have to consider the security of the citizens' PCs, terminals or other equipment?

Because many public systems contain large amounts of sensitive data about the citizens, breaches in security can seriously affect the privacy of the data subjects. The most important security issues that also affect privacy are:

Large systems risk bigger weaknesses

eGov is often part of a bigger reform, involving the integration of systems or "silos" and increased exchange of data between systems. This type of consolidation leads to larger systems, more connected systems, and systems that are connected to the Internet. This removal of borders between different systems may result in public sector employees getting access to more personal information than they need in order to perform their tasks.

A large data system is more vulnerable than a small system, partly because it becomes more difficult to maintain full overview of the system. In addition, there are more components that can fail, and the consequences of errors affect more users.

A study by PhD students at the University in Bergen found that one or more public portals in 173 out of 212 countries had serious vulnerabilities.⁴⁶ One of the conclusions from the study is that a high level of complexity leads to loss of oversight, and that this increases the risk of weaknesses in the system.

Human error

Through the media, one can easily be led to believe that the biggest threat to computer systems comes from hackers and attempts at gaining system access from the outside. However, most breaches in security stem from errors and mistakes – human error – within the organisation.⁴⁷ Lack of training, poor routine description or lack of ability or interest in following the established procedures are often the cause.

PC security

Most competent system administrators have a series of checks that are run regularly on the organisation's network and computers, like virus checks, firewalls etc. Most people could also use a system administrator at home: Many personal computers lack these checks, and many of them run on unsecured wireless networks.

When citizens start using their personal computer for submitting sensitive information to the public sector, chances of this information falling into the wrong hands increase. How far should the public responsibility for users' security go? Who is responsible if something goes wrong on the user's end of the system – for instance if certificates or passwords are stolen? Identity theft is a growing problem and causes massive problems for those who are victims of it.

Challenges with e-mail and instant messaging (IM)

Instant messaging is becoming increasingly popular as a form of communication between citizen and for instance a public service centre. This form of communication has the advantage that you can service many "customers" at a time, and this is what makes it so popular with call-centres. Because IM is less established as a public sector technology than for instance e-mail, the security round this channel tends to be lower. Both e-mail and IM is often sent through servers that are beyond both the sender's and receiver's control, for instance in "the cloud". For public offices, it is important to be conscious of what kind of communication can be allowed through these channels, if the communication isn't encrypted.

4.2. Viable and sustainable solutions

Privacy Impact Assessment

A privacy impact assessment is a process to help organisations determine the privacy consequences of new projects and systems. The assessment should be carried out during the planning stage of the project. That way, privacy principles can be integrated during the project design, or the project can be shut down before it has become too expensive. For projects that are carried out, the results from the assessment can be an integrated part of the internal control system and the information security.⁴⁸

Privacy impact assessments should be carried out for all acquisitions or development of IT systems that collect, maintain or display personal information. In addition an assessment should be carried out if such a system is to undergo significant changes – including changes in use, conversion from paper-based systems to electronic and consolidation or centralisation of databases.

46 Moen, Klingsheim, Simonsen, Hole: *Vulnerabilities in eGovernments*, (UiB 2006. http://www.nowires.org/Papers-PDF/ICGeS_egov.pdf)

47 Senter for informasjonssikring: *IKT trusselbilde for Norge*, 2005

48 *Lov om behandling av personopplysninger* §13 og §14.

More transparency

IT can be difficult for a citizen to get an overview of the information registered in various public databases, as the data is stored in many different systems that the user will need to know about in order to submit a "freedom of information" request. Getting insight into what information is registered about you is an important privacy principle, and everybody has a right to request it. In practice, the right is not exercised actively, because it is seen as unnecessary and cumbersome.

But we also know that public systems contain both out-dated and wrong information. By giving the citizens access to their own information, each individual can control that the registered information – which may form the basis for important decisions – is correct and up to date. It is in the interest of both parties that the information is updated and correct.

When more information is exchanged and can be viewed by more people and in new contexts, it becomes more important to maintain a balance between the authorities and the regular citizen. If the public employees get access to more information, so should the citizens: In addition to reviewing their own data, they should also get information about who has requested what information about them, the full process of their case and access to logs that show who stored, changed or viewed their data.⁴⁹

This kind of user control has to come in addition to good internal control systems, such as reports that show data requests beyond what is considered normal (for example if a case worker has checked unusually many cases, cases that belong to other case workers etc.).

Differentiated access control

It is also important to make use of the opportunities offered by technology for giving differentiated access to the system, and through this ensure that the public employees don't get access to data they don't need. When data needs to be sent between public offices, it should be after the citizen has given his or her consent.

Avoid unnecessary authentication

In society today anonymity is virtually impossible. With eGov comes the need for authentication, to make sure that only the data subject can get access to his or her personal data. With more sensitive data, such as health data or data related to social security, the authentication mechanism needs to be strong, for instance a digital signature/PKI solution with sufficient security. However, when such solutions are in place, it is difficult to resist the urge to ask citizens for authentication every time they visit an eGov service.

eGov systems should not require authentication on a higher level than is necessary:

pseudonymous solutions – solutions where you can use a virtual identity such as a nickname - should be considered where possible.

Anonymous services should still be offered when it is not necessary to keep the user personally accountable. Attribute authentication (age, sex etc.) should be available where possible. Example: A public movie library

⁴⁹ Også en rapport fra det danske Teknologirådet, *Rettsikkerhed og aktivt medborgerskab i digital forvaltning*, peger på viktigheten av balanse mellom borger og myndigheter.

may enforce age limits for some movies. In this case, the service doesn't need to know who the user is, only that he or she is the right age.

5. Search Engines and Social Network Services

5.1. Challenges

It is widely recognised that when different pieces of data about a person can be put together, it reveals more about that person than the information items viewed separately. An important privacy principle related to databases containing information about persons, is therefore that only the data necessary to fulfil the purpose of the system should be collected, and that it should be deleted when it is no longer needed (the principle of purpose). This principle is somewhat difficult to enforce when dealing with social media, where the purpose of the use is to provide personal information for the world to see.

Data mining is a label for technologies which find useful patterns and rules within large amounts of data. As an indirect consequence these technologies foster the creation of large data pools (data warehouses) which could not have been analysed effectively with traditional methods.⁵⁰ With the use of mathematical, or rather statistical techniques, it becomes possible to search massive quantities of data for patterns of correlations that produce a new type of knowledge.⁵¹ Aggregation of data lead to more information about individuals, and in most cases of data mining, the data subject does not know that data is being aggregated about him or her – far less which databases or information resources are connected.

Search

Search technology has developed enormously over the last years, and some now claim that searching unstructured text soon will replace database technology as the best technology for retrieving connections and patterns of information.

More and more information, both on individuals and businesses are now available on the Internet and in different public and private database systems connected to the Internet. A search engine will systematically go through (crawl) the Internet and index (either make a copy of or register the most important keywords) the pages it finds.⁵²

Combining information from a range of sources can be used to create profiles- of consumers for marketing or to help identify suspicious profiles by law enforcement. Using search technologies, it is possible to set up automatic searches that go through different databases and publicly available sources continuously, searching for patterns.

One technology that is predicted to improve search on the Internet is the semantic web. The semantic web is about data rather than documents. Much of the motivation is about being able to access information that is today locked away in different proprietary databases. In order to make this work, information items need to be “tagged” the same way by everybody. The idea is to provide a common framework that allows data to be shared and reused across applications, enterprises, and community boundaries. The work on this a collaborative effort led by W3C with participation from a large number of researchers and industrial partners.⁵³

50 EPTA (2006) *ICT and Privacy in Europe – A report on different aspects of privacy based on studies made by EPTA members in 7 European countries*

51 Hildebrandt and Backhouse (2005) *D 7.2 Descriptive analysis and inventory of profiling practices*

52 Battelle, J. (2005) *The Search – How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*

53 World Wide Web Consortium (W3C): *Sematic web*, <http://www.w3.org/2001/sw/>

Rich media search is another aspect of search that is predicted to become more important in the future. Rich media search can be improved by integrating speech recognition to transcribe spoken words (from videos and recorded speech) into text which is subsequently indexed by the search engine.⁵⁴ We already see attempts at using image recognition in search, and with the improvement of this technology, it will be possible to identify and profile people without having previous information, such as a name.

Social networks

The US National Security Agency (NSA) has been known to use phone logs to build a basic picture of someone's contact network. Clusters of people in highly connected groups become apparent, as do people with few connections who appear to be the intermediaries between such groups. The idea is to see by how many links or "degrees" separate people from, say, a member of a blacklisted organisation.

By adding online social networking data to its phone analyses, the NSA could connect people at deeper levels, through shared activities, such as taking flying lessons.⁵⁵ In many cases there exists implicit and/or explicit information in the form of social networks, such as those on the Web. For example, the LinkedIn.com social network comprises a large number of people from information technology areas, and MySpace and Facebook contain large amounts of social network data. The semantic web is a way of enabling the connection of information from all such sites to look for networks. Research into this area is funded by the NSA.⁵⁶

54 FAST Search Best Practices TM (2006) *Searching Rich Media*

55 Marks, P. (2006) *Pentagon sets its sights on social networking websites*

56 Marks, P. (2006) *Pentagon sets its sights on social networking websites*

6. RFID

6.1. Challenges

RFID (Radio Frequency Identification) is a concept for automatic identification using radio waves. Tiny integrated circuits (tags) containing information are attached to documents or integrated in products or wrapping. A reader can be used to read the information on the RFID tags within range. A complete RFID application will normally involve tags, readers, a database system, and sometimes a form of decision support system.

RFID tags that contain personal information can be found in Travel documents (such as visas and passports). RFID also play an integral part in "the internet of things", where all types of items have a tag with a unique identifier, allowing localisation of and communication between objects.

The tag

The *tag* as the basic building block of RFID consists of an antenna and a small silicon chip containing a radio receiver, a radio modulator for sending a response back to the reader, control logic, some amount of memory and it may contain a power system. The tag is located on the object or person to be identified.

RFID tags come as both *active* and *passive* chips. Active tags contain a battery and will therefore be bigger than passive tags, but they can contain more information and work over longer distances. A typical example of active tags is tokens to allow toll-booths to recognise and bill passing cars.

Passive tags do not contain a battery, but get the needed energy from the radio signal from the reader. Typical security applications that utilise passive tags are Machine readable travel documents (biometric passports) and ID cards, but the most common use for this technology is in the retail industry, where RFID is used in the supply chain. In the latter case, the tags normally only contain an identifier, and the actual information is retrieved from a database. Passive tags can be very small, and a major concern is that users may not know that they are carrying a tag or know when it is being read.⁵⁷

Tags exist in many different shapes and sizes. The Hitachi mu-chip⁵⁸ is less than 0.44mm on a side and was designed for tracking documents printed in an office environment. Hitachi has also presented an even smaller chip – which is only 0,05mm on each side and looks like spots of powder to the naked eye.⁵⁹ Also the VeriChip,⁶⁰ an implantable tag, has the size of a grain of rice and – being a passive tag – a very limited reading range.

As for transmission, we can distinguish between *promiscuous* and *secure* tags. While most tags are promiscuous and will communicate with any reader, secure tags require the reader to provide a password or a different kind of authentication credential before the tag transmits to the reader. Most tags, both active and passive, communicate only when they are interrogated by a reader.

The reader

The RFID *reader* (transceiver/transmitter/receiver) consists of a radio frequency module, a control unit, and a coupling element for interrogating electronic tags using radio frequency communication.⁶¹ The reader sends a pulse of radio energy and then listens for the chip's response. Just like the tags, readers' sizes vary. The size

⁵⁷ Article 29 Data Protection Working Party (2005) *Working document on data protection issues related to RFID technology*

⁵⁸ RFID Journal (2003) *Hitachi Unveils Smallest RFID Chip*

⁵⁹ BBC News (2007) *World's tiniest RFID tag unveiled*

⁶⁰ See the VeriMed Patient Identification website: http://verimedinfo.com/patient_demo/

⁶¹ Sarma, Weis and Engels (2003) *RFID Systems and Security and Privacy Implications*

may vary from the size of a desktop personal computer with multiple antennas to readers of the size of a postage stamp, embedded in mobile phones.

The Backend system

In many RFID systems, the data received by the reader is communicated via an interface on the reader to a data processing subsystem, (or backend system). Depending on the RFID System, this might simply be a computer that match the transmitted serial number to a reference database, or it could be more complex and consist of several computers and servers.

The RFID chip will often contain only a unique serial number to allow unambiguous identification of the chip and thus the labelled object. From the identification of an object, a person carrying the object may be identifiable.⁶² Furthermore, RFID tags can also be placed directly on or in the data subject, for example by implantation, and thereby allow direct identification of individuals.

Depending on the RFID technology in question, information may be stored on the tags. In passports, for instance, the passport information, as well as an image of the face and fingerprint of the holder is stored on the tag. If the information is not encrypted or secured in other ways, it can be read by anyone equipped with an RFID scanner/reader.⁶³ In Norway, it was uncovered that on the tags used for tollbooth passing, the last 100 passings are stored on the tag. This information, revealing the movement pattern of the car, can be read by using a standard reader.⁶⁴

A number of possible attacks on RFID Systems exist with relevance for the integrity of the data transmitted or stored, and thus the quality of the data. The security of an RFID system can be broken for example by malicious code (malware) planted in the back end system and thereby gaining unauthorized access to the stored data, or by cloning of the data contained on the tag and simulating the original identity of the tag. In experiments, researchers have also successfully infected back end RFID middle ware systems through the RFID tag.⁶⁵

Attacks to RFID systems usually follow one of the four aims:⁶⁶

Spying: The attacker gains unauthorized access to information for example by eavesdropping or unauthorized access to back end systems.

Deception: The attacker deceives the operator or user of an RFID system by feeding in wrong information into the system.

Blocking, for example by applying Denial of Service (DoS): The availability of functions of the RFID system is compromised either on the level of a reader or the back end system.

Shielding or killing of tags for example by applying a Faraday-cage or destroying RFID tags: A single tag is not readable through application of for example physical measures.

62 See Directive 95/46/EC, recital 26 on the term "identifiable": "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."

63 From Extract from ESSTRT Deliverable D1-6 "Responses to Terrorist Threats"

64 The Norwegian Data Inspectorate (2007) *Statens Vegvesen holdt tilbake viktig AutoPASS-informasjon*

65 Rieback et al *Is Your Cat Infected with a Computer Virus?*

66 See German Federal Office for Information Security (2005) *Security Aspects and Prospective Applications of RFID Systems*

GENERAL ISSUES

7. Definitions, notification, data transfers, and data security

Although the Commission's consultation is in particular requesting input from stakeholders on "new" challenges for data protection and privacy, there are a number of existing areas under the EU Data Protection Directive (95/46/EC) ("the Directive") that pose significant challenges for industry and other stakeholders when applying them in practice. Some of those areas are: (1) the definitions under the Directive; (2) the notification and/or registration requirements with national data protection authorities; and (3) international data transfers.

7.1. Definitions under the Directive

Member States have the discretion in terms of the means to implement a European Directive (whilst the final goal or output should be the same). However, too often, the variances in the implementation of the Directive among the Member States are significant. This poses real challenges for companies operating on a multi-Member State basis when having to comply with a myriad of different approaches and laws while at the same time trying to run a global business as effectively as possible. Below are two examples of such challenges.

Controller and Processor

The increased debate over what really constitutes a controller vs. a processor is one area where the Directive needs to become more flexible and where also more harmonization between the Member States is sought. Some Member States allow for a certain degree of controller ship or discretion for a processor, whereas others do not offer this possibility, but would label the person a controller as soon as there is some power as to the determination of the purpose and means of the processing. Increasingly, during one and the same data processing exercise (including e.g., data transfers and outsourcing of services) a person can in one instance be considered a controller and, in the next, a processor, and then a controller again. The issue of who is really "in control" is not well defined and a more flexible approach of the definitions would be welcomed, taking into account the realities of the modern networked society in which we live where more than two distinct players are involved.

A closely linked concept is that of a co-controller or joint controller. It is not well recognized by the existing Directive or by the data protection authorities. However, a more harmonized interpretation of the concept would be welcomed as it is currently unclear when two persons are co-controllers.

Definition of Personal Data

Art. 2 of The Directive defines personal data as "any information relating to an identified or identifiable natural person." During the past couple of years, the debate around the definition of personal data has increased and one of the main points is whether and when one can consider a person to be "identifiable" and thereby be subject to the Directive's rules. Member States have differing approaches in this respect. A pragmatic approach to this concept should be favoured, i.e., what is the likelihood that the natural person may become

identifiable. By contrast, a more strict and non-pragmatic approach, favoured by some Member States, that no matter the reasonable likelihood, the mere fact that there may be a remote possibility, however slight, that the natural person becomes identifiable, even if the data controller is not able to decipher the identity of the person, and should thus fall under the definition of personal data.

The Art. 29 WP opinion on personal data (June 2007), clarifies to some extent these concepts and discusses in particular the border line between personal data and anonymous data. However, again, Member States may treat these concepts slightly differently, which could mean that the Directive would apply in one Member State but not in another, even with exactly the same facts and scenarios at hand. A more harmonized approach among the Member States needs to be taken.

7.2. Notification and Registration Requirements with National Data Protection Authorities

The notification and/or registration requirements vary greatly from one Member State to another. The exemptions from notification (e.g., in relation to employee data) vary widely, too.

Differing registration and/or notification requirements throughout the Member States

While some Member States have a very minimalist approach to the notification process (a simple ticking of a box or a yes/no answer may suffice), others require sometimes extreme detail in terms of the data processing and the description of the data flows. This makes the notification process very burdensome and bureaucratic for companies operating in several Member States and in a dynamic and fast-moving environment.

An added challenge is that some Member States require the notification of and the prior approval for data transfers and especially for the use of the Standard Contractual Clauses (“model clauses”). A more streamlined and shortened period of clearance and approval is welcomed. There should be no requirement for prior approval when using Binding Corporate Rules or Standard Contractual Clauses as a basis for transferring data.

Data Protection Officer

Some Member States advocate and/or require the use of a data protection officer (registered with the national data protection authority) as a substitute to the notification process. The specific company processing the information available to the DPA remains the same, but there is a lessened burden on part of companies who do not have to go through different notification processes. However, the majority of Member States does not offer this possibility. An increased use of data protection officers (“DPO”) and a more active encouragement on part of the Commission to make use of such a DPO would be much welcomed to the business community.

7.3. International Data Transfers

The Directive imposes significant barriers to international data flows by generally prohibiting the transfer of personal data located outside the EU/EEA. A handful of countries are to date considered by the EU as providing adequate data protection. The remaining alternatives (which are considered “exceptions”), are

either limited in scope (e.g., the EU-US Safe Harbour Agreement which only applies to transfers from the EU/EEA to the United States and which currently excludes transfers of data by companies with financial services or telecommunication service operations) and/or not recognized under the existing Directive. Therefore, the EPA believes that the points raised below should be considered when reviewing the existing Directive in order to improve and enhance the remit within which personal data can be transferred across borders.

Extension of list of “adequate” countries

There is a need to review the Commission criteria for approving non-EEA countries and acknowledging them as being adequate, thereby allowing personal data to be transferred to more countries without the need for any additional protection and assurances. Instead of measuring how a specific country’s data protection laws compare to the Directive, more emphasis should be put on actually examining the real protection afforded by the third country’s laws, even if the approach may be different.

Binding Corporate Rules

The concept and use of binding corporate rules (“BCR”) has evolved enormously over the past five years. BCRs are today one of the most workable alternatives available for companies that operate on a global scale. However, several obstacles remain and should be addressed in a review of the Directive. For instance, BCRs should be expressly recognized in the Directive as one of the available exceptions for transferring data outside the EU/EEA. Still today, some Member State are unable to recognize the very concept of BCRs as there is no legal basis for it either in the Directive, as implemented, or in other relevant national legislation. Moreover, even if there has been improvements in terms of the development of the concept of “mutual recognition” whereby those Member States who have signed up to this idea in theory mutually recognize the lead authority’s approval of a company’s BCRs. In practice, however, several Member States still require additional reassurances and some are very hesitant at all to relinquish such a core power to a lead authority. Finally, and as a follow up to the point above, BCRs should not be subject to overly onerous and burdensome national procedural requirements. We call upon the Commission, together with the Art. 29 WP, to compile a list of the specific national requirements and publish it in a transparent and public manner with the ultimate aim to streamline them.

Standard Contractual Clauses

Those companies that have not yet bought into the idea of BCRs invariably use Standard Contractual Clauses as it is the only other true legal basis available for operations on a global scale (i.e., not just EU-US data flows). However, some major challenges exist in this area as well. First of all, there are no uniform procedural requirements among the Member States with respect to the level of detail in the schedules required and the notification and/or approval of the Clauses (sometimes prior approval is needed). Second, the Commission clauses allow for one processor and one controller. However, increasingly, transfers involve multiple parties and therefore the multi-party context should be recognized in the Clauses. Third, onward transfers and sub-processing of data are increasingly commonplace and the Clauses should be amended to allow for this possibility.

8. Data security

8.1. The existing legal basis

In order to implant the Data Protection Law in the European Union, there are (3) aspects to cover regarding data protection set out by the Directives: (i) the legal (ii) the organizational and (iii) the technical.

The main Directives in Data Protection set out these aspects:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Regarding the security aspects the Directives set out:

- Directive 95/46/EC:

“Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.”

This measure includes the “processor” of the data, which shall act only on instructions from the controller when processing the data.”

- In the same way, the Directive 2002/58/EC, sets out

“Article 4

Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.”

And the Directive 2006/24/EC, sets out:

“Article 7. Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention”

Also, In the Madrid Resolution, which constitutes a proposal for a Draft of International Standard on the Protection of Privacy regarding of the processing of Personal Data, accorded with Most Authorities In Data Protection in the International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5 November 2009, we cannot appreciate a compromise or a goal to set out a document with the security/technical measures, the European countries must adopt internally.

This Resolution proposes:

“20. Measures

1. Both the responsible person and any processing service provider must protect the personal data subject to processing with the appropriate technical and organizational measures to

ensure, at each time, their integrity, confidentiality and availability. These measures depend on the existing risk, the possible consequences to data subjects, the sensitive nature of the personal data, the state of the art, the context in which the processing is carried out, and where appropriate the obligations contained in the applicable national legislation. 2. Data subjects should be informed by those involved in any stage of the processing of any security breach that could significantly affect their pecuniary or non-pecuniary rights, as well as the measures taken for its resolution. This information should be provided in good time, in order to enable data subjects to seek the protection of their rights.”

Under the premise the Directives and the recently Compromise do not propose the creation of a Document with the technical and security measures the countries must adopt and incorporate in its legislation about data protection and the fact that the appliances in information technology, it means software, hardware, telecommunication networks, are used and shared all over the world, we consider there must be an intent by the European Union to propose a technical measures that must be taken by the controllers and all the parties involved in the processing of personal data.

Examples of regulation from member states:

Spain

Spanish Legislation in security measures and the way the Spanish Data Protection Agency has provided a Guide for Security measures.

First of all, every entity which process personal data must adopt security measures, there is always a minimum must be accomplish and depending on the kind of data and its sensitive the technical and organizational measures must be increased.

These measures are imposed by automated and non-automated data and it's an obligation to have them in writing.

UK

In United Kingdom, ⁶⁷ there is not a specific security measures that companies need to implement when processing personal data, apart from the requirement to have a written data processing agreement. However, recent enforcement action by the ICO in cases of security breaches indicates that encryption of company laptops by data controllers is coming to be expected by the ICO.

There are not compulsory and well-defined rules to be applicable by all the actors who process personal data although there is information on the guidelines on the web site:

http://www.ico.gov.uk/for_organisations/data_protection_guide/principle_7_information_security.aspx.

⁶⁷ Information dated March 31, 2008

Belgium

In the case of Belgium, the obligations relating to security of data processing are quite complicated. Firstly, there is a *general* obligation to guarantee the security of the data⁶⁸, secondly there are *specific* technical and organizational measures described in the PPL and thirdly there are separate rules relating to the relationship controller-processor.

The controller or, if such is the case, his representative in Belgium, shall:

- 1) Watch carefully that the data are updated, that inaccurate, incomplete and irrelevant data, as well as data that have been obtained or further processed in violation of certain articles of the PPL are corrected or erased;
- 2) Take care that the access to the data and possibilities or processing for the persons who are acting under his authority, are limited to what is necessary for the fulfilment of their duties or for the requirements of the service;
- 3) Notify all persons acting under his authority about the provisions of this law and its implementing decrees, as well as about all relevant provisions in respect of the protection of the privacy with regard to the processing of personal data;
- 4) Ascertain that the programs for the automatic processing of personal data are in accordance with the information that has been notified to the Data Protection Agency and that no unlawful use is made thereof.

The security measures to be taken depend amongst others on the nature of the data, e.g. health related data deserve a more rigid protection than address data.

The PPL does not oblige to describe the measures in writing. However, it's recommended to store any written information relating to the technical⁶⁹ measures and to keep written documents relating to the organizational⁷⁰ measures.

France

In the case of France, all kinds of process must be protected by the security measures. Nowadays ⁷¹ there is not more precision than this because there have not been adopted the statutory Laws to detail which ones are the security measures related to each kind of processing. However, the declarations and request of

68 In order to guarantee the security of personal data, the controller or, if such is the case, his representative in Belgium, as well as the processor shall take the appropriate technical and organisational measures that are necessary for the protection of personal data against accidental or unauthorised destruction, accidental loss, as well as alteration of, access to and any other unauthorised processing of personal data. These measures shall ensure an appropriate level of security taking into account the state of the art in this field and the cost of implementing the measures on the one hand, and the nature of the data to be protected and the potential risks on the other hand.

69 These are the *physical* measures (such as restricting access to computers containing certain data, store any data carriers in locked and secured areas) and the *logical* measures (such as protection against hackers, viruses, the use of passwords, etc.)

70 E.g. the creation of i) a written inventory of the most important aspects of each '*processing*' of personal data (containing amongst others the nature of the data, the purposes of the processing, the connections between eventual other databases and the categories of persons to whom the data are disclosed) and ii) a written privacy policy (explaining amongst others the importance of compliance with the law and giving specific instructions/guidelines on how to guarantee the security).

71 April 2008

authorization for the processing before the Commission Nationale de l'Informatique et des libertés (CNIL) must set out the security measures adopted

Italy

In the case of Italy, the Italian Legislative Decree 196 of 30 June 2003, The Code, provides some specific security measures to be implemented by companies. In particular, it distinguishes between: **(i)** so called "minimum security measures", which are set forth in the Code in a very precise manner and, in case of non-enforcement, are punished by criminal sanctions- and **(ii)** "appropriate measures" -which are generally defined as all suitable measures, in consideration of technological innovation, to minimize the risks of damage taking into account the nature of the data and the features of the processing. In case of non-enforcement of the appropriate measures, data controllers shall only incur in civil liability and therefore, if any damage occurs, they shall be responsible.

The security measures to be adopted are different depending on **(i)** the type of means used for the processing (electronic means) and **(ii)** the type of data concerned (sensitive or not sensitive).

Processing personal data without electronic means shall only be allowed if the following minimum-security measures are adopted

Furthermore, please note that in case of processing of sensitive data, the Code provides the adoption of more restrictive security measures

In case of processing of sensitive and/or judicial⁷² data by electronic means the data controller shall draw up a so-called Security Policy Document ("**DPS**") in which it shall describe the security measures adopted.

Portugal

In the case of Portugal, Article 15 of the Data Protection Act further describes the special security measures to be implemented in order to protect sensitive data (i.e., data related to health and sexuality, religious, political and philosophical views, union and political affiliation, private life, and racial or ethnic origin) and data related to illicit activities, as well as criminal offences and administrative infringements.

Those measures shall permit the data controller to: control the entry to the premises where the data are located; control the media where the data is contained; control the input/alteration of personal data and when and by whom it is made; control the use of and access to the data; control the transmission of the data; and control the transportation of the respective media where the data is located.

It is further indicated that the Data Protection Agency may waive the obligation to implement certain security measures, provided the respect of fundamental rights, freedom and guarantees of the data subjects.

Article 15 further indicates that the data controllers' systems must guarantee logical separation between data relating to health and sex life, including genetic data, and other personal data. It also provides that in cases of circulation over a network of data referred to in articles 7 and 8, when such circulation may jeopardize the fundamental rights, freedoms and guarantees of data subjects, the Data Protection Authority may determine that transmission must be encoded.

⁷² Pursuant to Article 4 of the Code, "judicial data" shall mean personal data disclosing the measures referred to in Section 3(1), letters a) to o) and r) to u), of Presidential Decree no. 313 of 14 November 2002 concerning the criminal record office, the register of offence-related administrative sanctions and the relevant current charges, or the status of being either defendant or the subject of investigations pursuant to Sections 60 and 61 of the Criminal Procedure Code".

It is not expressly established by the Data Protection Act that the security measures need to be described in writing and there is no need to register any such document at the Agency. However, it is advisable to have a description of those measures in writing as evidence, in case the Data Protection Agency decides to confirm that the necessary security measures have been implemented.⁷³

8.2. Assessment of legal regulation

On the basis of the descriptions above of security measures adopted as a compulsory law by the countries mentioned, the picture is that:

1. There is not a harmonized system of security measures in place in member states. In some cases, they are more rigid than in others.
2. There is not an obligation to put in writing the security measures in all member states.
3. The levels of security are not the same in the member states mentioned.

8.3. Viable and sustainable solutions

The following issues should be taken into consideration when adapting the EU directive to new IT development and challenges related to data security:

1. To propose a document with the security measures the European Union must adopt and incorporate to data protection legislation, according to the kind of data, its sensitive and importance of protection, taking in consideration the information society and telecommunications devices used all over the world. Also, relevant stakeholders should be taken into consideration.
As a second step, to propose jointly with the participation of the experts in technologies, governments, mainly a document with the security measures that referred to a specific technology, for example PETS, social networks, cloud computing.
2. To get the compromise of the different authorities to accord the same level of enforcement in the accomplishment of the data protection law. For example in Spain, the Spanish Data Protection Authority gives recommendations, guidelines and also impose sanctions and administrative fines but in the case of UK, Generally, the ICO prefers to encourage compliance through education and awareness-raising, deploying its enforcement powers only as a last resort. The ICO is active in negotiating with companies it believes to be in breach of the UK legal requirements; it has limited resources and powers. Usually only when a breach of the law is continuing despite the ICO's efforts at persuading an organization to comply, will enforcement action be taken.
3. To set out a coherent model of sanctions and administrative fines. There is not equity in the European Countries so the enforcement of the law is different in each country.

9. Concluding observations

Based on the analyses above, the European Privacy Association would like to point at the following areas where there exists a need for further harmonisation among the member states:

- A more harmonized approach among the Member States needs to be taken concerning the definition of personal data, including biometric data;
- A harmonised approach should be taken to the usage of RFID tags, including the possibility to opt out, and for automatic deactivation;
- A harmonised yet flexible approach to the definitions of controller and processor is needed that takes into consideration the current technological level and practices;
- The notification and/or registration requirements vary greatly from one Member State to another. There is a need for a more simple and harmonised notification scheme.
- A harmonised approach to security measures that takes into consideration specific technologies such as privacy enhancing technologies, social networks, and cloud computing.

According to the European Privacy Association, the following new concepts and tools should be considered when revising the personal data protection regulation and structure:

- Integration of personal data protection in IT architecture and products via promotion of standardized Privacy Impact Assessment tools.
- Renewal of the criteria for approving non-EEA countries as “adequate” countries. An examination should take its point of departure in real protection afforded by the third country’s laws, even if the approach may be different from that of the EU directive;
- The concept and use of *Binding corporate rules* (“BCR”) should be expressly recognized in the Directive as one of the available exceptions for transferring data outside the EU/EEA.
- Uniform procedural requirements among the Member States with respect to the use and content of *Standard Contractual Clauses*;
- A new approach to cloud computing based on a flexible, consensus-building model, and a contract-based approach, supported by strong tools of international private law.

In order to ensure transparency and effective enforcement, the European Privacy Association points at the need for:

- A coherent model of sanctions and administrative fines applicable in all member states;
- Strengthening of the mandate and functioning of Data Protection Officers and Authorities in all member states, including allocation of adequate resources to both basic functions and new functions stemming from e.g. BCR approval processes.