Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Doc.
.. May 2011

Protection of privacy and personal data on the Internet and online media

Report[1]
Committee on Culture, Science and Education
Rapporteur: Mrs Andreja RIHTER, Slovenia, Socialist Group

Summary

The digitalisation of information has caused unprecedented possibilities for the identification of individuals through their data. Personal data are processed by an ever growing number of private and public instances globally. Personal information is put into cyberspace by users themselves as well as third parties. Individuals leave identity traces through their use of information and communication technologies (ICT). Profiling of Internet users has become a wide phenomenon.

The fundamental human right to respect for private and family life, home and correspondence as guaranteed by Article 8 of the European Convention on Human Rights includes the right to the protection of personal data as well as the obligation to establish appropriate safeguards under domestic law in this regard. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention No 108") requires that personal data be processed fairly and securely for specified purposes on a legitimate basis only, and establishes that everyone has the right to know, access and rectify their personal data processed by third parties or to erase personal data which have been processed without right.

The Committee on Culture, Science and Education calls for a plan of action for the promotion of common legal standards for the protection of privacy and personal data on ICT-based networks and services throughout Europe and beyond in the framework of the Convention No 108.

[1] Reference to committee: Doc. 12021, Reference 3608 of 2 October 2009. Report approved unanimously by the committee on 12 May 2011.

A. Draft resolution

1. While welcoming the epochal progress in information and communication technologies (hereafter "ICT") and the resulting positive effects on individuals, societies and human civilisation as whole, the Parliamentary Assembly notes with concern that the digitalisation of information has caused unprecedented possibilities for the identification of individuals through their data. Personal data are processed by an ever growing number of private and public instances globally. Personal information is put into cyberspace by users themselves as well as third parties. Individuals leave identity traces through their use of ICT. Profiling of Internet users has become a wide phenomenon. Companies sometimes control employees and business contacts through ICT.

2. In addition, ICT systems are often intruded in order to gain data of legal entities, in particular commercial companies, financial institutions, research institutions and public authorities. Such access might cause economic losses to the private sector and might negatively impact the economic well-being of states, their public safety or national security.

3. The Assembly is alarmed by such developments challenging the right to privacy and data protection. In a democratic state governed by the rule of law, cyberspace must not be regarded as outer space from a legal point of view.

4. The Assembly recalls the fundamental human right to respect for private and family life, home and correspondence as guaranteed by Article 8 of the European Convention on Human Rights (ETS No 5, hereafter "ECHR"). This right includes the right to the protection of personal data as well as the obligation to establish appropriate safeguards under domestic law in this regard.

5. The Assembly underlines the need to eradicate the use of ICT to possess or transmit pornographic material involving children under the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No 201).

6. Recalling its long-standing support of the right to protection of privacy since its Recommendation 509 (1968) on human rights and modern scientific and technological developments, the Assembly welcomes and supports Resolution No 3 on data protection and privacy in the third millennium, which was adopted by the 30th Council of Europe Conference of Ministers of Justice (Istanbul, 24-26 November 2010).

7. As the Assembly declared in its Resolution 428 (1970) on mass communication media and human rights, "where regional, national or international computer-data banks are instituted, the individual must not become completely exposed and transparent by the accumulation of information referring even to his (or her) private life. Data banks should be restricted to the necessary minimum of information required."

8. Referring to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108, hereafter "Convention No 108"), the Assembly emphasises that the right to the protection of personal data includes, in particular, the right that personal data be processed fairly and securely for specified purposes on a legitimate basis only, and that everyone has the right to know, access and rectify their personal data processed by third parties or to erase personal data which have been processed without right. Compliance with these obligations must be supervised by an independent authority in accordance with the Additional Protocol (ETS No 181) to Convention No 108.

9. The Assembly reaffirms that all member states should only agree to transfer personal data to another state or an organisation where such state or organisation is a Party to Convention No 108 and its Additional Protocol or otherwise ensures an equally adequate level of protection for the intended data transfer. Transfers of personal data, which violate the right to protection of private life under Article 8 ECHR, may be the subject of proceedings before the European Court of Human Rights.

10. The Assembly welcomes that Convention No 108 has been signed and ratified by nearly all Council of Europe member states – with the regrettable exception of Armenia, Russia, San Marino and Turkey – and notes that Articles 7 and 8 of the Charter of Fundamental Rights of the European Union contain largely the same principles. With the growing globalisation of ICT-based services, it is of utmost urgency for Europe as a whole to adhere to the same standards and seek to involve other countries around the world.

11. While Article 17 of the International Covenant on Civil and Political Rights (hereafter "ICCPR") recognises the right to privacy, the legal interpretation and practical implementation of this Article falls significantly short of European standards. The Assembly therefore believes that any global initiative should

be based on Convention No 108 and its Additional Protocol, both of which are in principle open to signature by non-member states of the Council of Europe.

12. Although precautionary technologies and software, voluntary self-regulation by ICT companies and private users as well as improving user awareness may reduce the risk of interference with privacy and the harmful processing of personal data through ICT, the Assembly believes that only specific legislation and effective enforcement can sufficiently protect the right to protection of privacy and personal data as required by Article 17 ICCPR and Article 8 ECHR.

13. The Assembly deplores that the absence of globally accepted international legal standards on data protection regarding ICT-based networks and services leads to legal insecurity and to the need for national courts to fill this void through the interpretation of respective domestic laws in the light of Article 17 ICCPR and Article 8 ECHR on a case-by-case basis. The latter not only exposes individuals to a unequal protection of their rights, but also entails different and changing requirements for ICT companies and users globally, causing virtually unpredictable liabilities.

14. The Assembly welcomes the international co-operation established among independent data protection authorities and supports their efforts in ensuring a common international protection of privacy and personal data in the wake of technological progress, as expressed in their resolutions adopted in Madrid in 2009 and Jerusalem in 2010. The Assembly shares their view that Convention No 108 should be promoted globally, as it is the most advanced set of standards in this sector under public international law.

15. Recalling the Convention on Cybercrime (ETS No 185), the Assembly welcomes that more than one hundred states worldwide have passed legislation which complies with the spirit of this convention. Under Articles 2, 3 and 4 of this Convention, its Parties are obliged to consider as an offence punishable under domestic criminal law any intentional access to, interception of, and interference with computer data without the right to do so. Such computer data may include personal data of natural persons and secret data of legal persons on computer networks.

16. Recalling Article 10 of the Convention on Human Rights and Biomedicine (ETS No 164) and Article 16 of the Additional Protocol to this Convention concerning Genetic Testing for Health Purposes (CETS No 203), the Assembly emphasises the right of everyone to the protection of personal health data including the right to be informed of, and to consent or not to, any collection and processing of such data through ICT. Medical and health data of persons require the highest level of data protection, as they constitute one of the core elements of a person's private life and human dignity.

17. The Assembly also recalls the obligation to respect the right to privacy and data protection under the Convention on Access to Official Documents (CETS No 205) as well as the limits to the protection of personal data under the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No 198) and the Convention on Mutual Administrative Assistance in Tax Matters (ETS No 127 and CETS No 208).

18. The Assembly endorses the following general principles concerning the protection of privacy and personal data in an ICT environment:

18.1. the protection of private life or privacy is a necessary element of human life and the humane functioning of a democratic society; where the privacy of a person is violated, his or her human dignity, liberty and security are at stake;

18.2. the right to protection of privacy and personal data is a fundamental human right, which imposes on states the obligation to provide an adequate legal framework for such protection against interference by public authorities as well as private individuals and entities;

18.3. individuals shall be able to control the use of their personal data by others, such use including any accessing, collection, storage, disclosure, manipulation, exploitation or other processing of personal data, with the exception of the technically necessary or lawful retention of ICT traffic data and localisation data; the control of the use of personal data shall include the right to know and rectify one's own personal data and to have erased from ICT systems and networks all data which were provided without legal obligation;

18.4. personal data of an individual shall not be used by others without right, unless this person has given his or her prior consent, which requires an expression of consent in full knowledge about such use, i.e. the manifestation of a free, specific and informed will, and excludes an automatic or

tacit usage; consent can be withdrawn subsequently at any time; where consent has been withdrawn, personal data may not be used further;

18.5. where personal data of an individual shall be used with the intention to exploit such data commercially, this person shall also be informed of the concrete commercial exploitation in advance; where personal data may be used by others, because of individual consent or the public availability of otherwise anonymous data, the intentional accumulation, interconnection, personalisation and use of such accumulated data shall nevertheless require the consent of the person concerned;

18.6. personal ICT systems as well as ICT-based communications shall not be accessed or manipulated, if such action violates privacy or the secrecy of correspondence; access and manipulation through "cookies" or other automated devices without right violate privacy, in particular where such automated access or manipulation serves other, especially commercial, interests;

18.7. higher protection shall be afforded to private pictures, personal data of minors or persons with mental or psychological disabilities, personal ethnic data, personal medical, health or sexual data, personal biometric and genetic data, personal political, philosophical or religious data, personal financial data and other information forming part of the core area of private life; higher protection should also be afforded to personal data related to court proceedings or the professional secrecy of lawyers, medical professionals and journalists; such higher protection may be effectuated through self-regulatory, technical as well as legal means ensuring due accountability in case of infringements of data protection or privacy; periods should be specified beyond which such data shall no longer be kept or used;

18.8. public and private entities which collect, store, process or otherwise use personal data should be obliged to reduce the amount of such data to the lowest minimum necessary; personal data should be deleted which have become outdated or unused or where the purpose for their collection has been met or disappeared; the random collection and storage of personal data should be avoided;

18.9. everyone shall have an effective remedy against an unlawful interference with his or her right to protection of privacy and personal data before domestic courts; voluntary arbitration and self-regulatory bodies as well as independent data protection authorities should complement the judicial system in ensuring the effective protection of this right; public authorities and commercial companies should be encouraged to establish mechanisms for receiving and processing complaints against them by individuals alleging infringements of their right to data protection or privacy, as well as mechanisms for ensuring internally compliance with the right to privacy and data protection; unlawful infringements of privacy and data protection should be penalised.

19. The Assembly welcomes that the Parties to Convention No 108 have started to prepare a possible revision of this convention in the wake of technological progress and a growingly fierce commercial competition in ICT-based services.

20. The Assembly calls on the parliaments of Armenia, Russia, San Marino and Turkey to initiate their ratification of Convention No 108 without delay, thus enabling their countries to play an active role in the further development of this convention.

21. The Assembly calls on its observer delegations from Canada, Israel and Mexico to initiate debate in their respective parliaments about signing and ratifying Convention No 108 and participating in its further development. The observer delegations are invited to report progress in this regard to the Assembly [Committee on Culture, Science and Education] in due course.

22. The Assembly invites the states co-operating otherwise with the Council of Europe, in particular the Council of Europe observer states Japan, the USA and the Holy See, to promote their authorities' accession to Convention No 108.

23. The Assembly calls on the European Union to continue to support broad accession to Convention No 108 and its Additional Protocol and to become itself Party once the necessary amendments allowing this accession will have entered into force.

24. The Assembly invites the Venice Commission to report to the Assembly [Committee on Culture, Science and Education] in how far its member and observer states have domestic legislation which would be in accordance with the universal human right to protection of privacy and personal data in the light of

Convention No 108 and its Additional Protocol, and whether those states which are not parties to this convention would consider signing and ratifying it.

25. The Assembly asks the Secretary General of the Council of Europe to seek high-level support from the United Nations in promoting accession to Convention No 108 by states worldwide, including in particular through the United Nations Internet Governance Forum, the International Telecommunication Union and UNESCO.

26. The Assembly asks the Secretary General of the Council of Europe to ensure through specific internal rules and regulations the protection of privacy and personal data of Council of Europe staff as well as members of Council of Europe bodies. The ubiquitous use of ICT within the Council of Europe and its exterritorial legal status must not compromise the protection of privacy and personal data. In this context, the position and work of the Council of Europe's Commissioner for Data Protection should be strengthened and the internal regulatory framework revised accordingly.

27. Welcoming international efforts by different stakeholders to ensure the right to protection of personal data in the ICT environment, such as the Madrid 2009 and Jerusalem 2010 resolutions by independent data protection authorities and the various data protection initiatives by the International Chamber of Commerce, the Assembly invites all stakeholders to join forces with the Council of Europe in order to ensure that individual initiatives do not contradict each other or risk being used in order to blur a common approach to the universal right to respect for privacy and personal data or lower existing legal standards.

B. Draft recommendation

1. Referring to its Resolution … (2011) on the protection of privacy and personal data on the Internet and online media, the Parliamentary Assembly welcomes and supports Resolution No 3 on data protection and privacy in the third millennium adopted by the 30th Council of Europe Conference of Ministers of Justice (Istanbul, 24-26 November 2010) and calls for a plan of action for the promotion of common legal standards for the protection of privacy and personal data on ICT-based networks and services throughout Europe and beyond in the framework of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108, hereafter "Convention No 108").

2. The Assembly recommends that the Committee of Ministers:

2.1. actively seek the signature and ratification of Convention No 108 and its Additional Protocol by the European Union and those member states which have not yet done so, and call on all parties to Convention No 108 which have not yet done so to accept the amendments allowing the European Union to accede to this convention;

2.2. encourage and support, through their member states' Permanent Representations to the United Nations, the signature and ratification of Convention No 108 by non-member states worldwide, in particular those states that are observers to the Council of Europe or are parties to enlarged partial agreements or signatories to other Council of Europe conventions;

2.3. provide adequate budget within the secretariat of the Council of Europe for the further legal development of Convention No 108 in line with Resolution No 3 of the 30th Council of Europe Conference of Ministers of Justice (Istanbul, 24-26 November 2010), and call on member and observer states as well as the European Union to provide voluntary additional funding for such work;

2.4 invite the Parties to Convention No 108:

i. to take account of Assembly Resolution …. (2011) when revising their convention,
ii. not to lower the established protection of privacy and personal data,
iii. to establish a mechanism for monitoring compliance of Parties with their obligations under this convention,
iv. to bear in mind Assembly Resolution 1744 (2010) on extra-institutional actors in the democratic system when consulting private stakeholders;

2.5. promote the signature and ratification of the Convention on Cybercrime (ETS No 185) by all member states as well as by non-member states;

2.6. promote the signature and ratification of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No 201) by all member states as well as by non-member states;

2.7. ask its Steering Committee on Bioethics to propose standards for the ICT-based processing of medical and health data under the Convention on Human Rights and Biomedicine (ETS No 164) and its additional protocols;

2.8. bring this Recommendation and Resolution …. (2011) to the attention of competent ministries and data protection authorities in member states.

C. Explanatory memorandum by Mrs Rihter, rapporteur

* * *

1. Introduction

1.1. Preparation of this report

1. Having tabled the Motion on privacy and the management of private information on the Internet and other online media (doc. 12021 of 17 September 2009), I was appointed rapporteur by the Committee on Culture, Science and Education on 8 December 2009. As Slovenian Minister for Culture from 2000 to 2004, media policy and new media have been subjects close to my heart.

2. The Sub-Committee on the Media organised the Council of Europe's Open Forum on Privacy and Internet Freedom at the United Nations Internet Governance Forum (IGF) in Vilnius (Lithuania) on 15 September 2010. This Open Forum allowed invited experts as well as all IGF stakeholders to express their views on this subject at the beginning of the preparation of my report. The transcript of the Open Forum is accessible at http://www.intgovforum.org/cms/2010-igf-vilnius/transcripts/646-1.

3. I am particularly grateful for the thematic contributions by Mrs Maud de Boer-Buquicchio, Deputy Secretary General of the Council of Europe, Mrs Catherine Pozzo di Borgo, Vice-Chair of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter "Convention No 108") and Deputy Government Commissioner to the National Commission on IT and Liberties (CNIL, Paris), Mr Richard Allan, Director of Policy EU with Facebook (London), Mrs Katitza Rodríguez, International Rights Director at Electronic Frontier Foundation and Member of the Advisory Board of Privacy International (San Francisco) and Professor Peng Hwa Ang from the Nanyang Technological University in Singapore.

4. Professor Cécile de Terwangne and Professor Jean-Noël Colin from the University of Namur (Belgium) were commissioned to prepare, along the thematic lines agreed with me, a background report on the legal and technical challenges to privacy and data protection in today's cyberspace. They presented their joint report to the Committee on Culture, Science and Education in Paris on 18 March 2011. This explanatory memorandum relies largely on the background report, and I am very grateful to Professor de Terwangne and Professor Colin.

5. On 18 March 2011, the Committee on Culture, Science and Education also organised a hearing on this subject with Professor de Terwangne and Professor Colin as well as Mrs Catherine Pozzo di Borgo speaking on behalf of the Consultative Committee of Convention No 108, Mr Michael Donohue, Senior Policy Analyst, Information Security and Privacy, OECD and Mr Olivier Matter, Lawyer, European and International Affairs, National Commission for Information Technologies and Liberties (CNIL), Paris. The presentations made during the hearing have enriched my report.

6. Representatives of the European Commission and the International Chamber of Commerce were excused at the hearing on 18 March 2011. Therefore, I contacted the European Commission and the International Chamber of Commerce, sending them the preliminary draft resolution for their comments.

7. The Data Protection Commissioner of the Council of Europe, Dr Karel Neuwirt, provided on 4 April 2011 an opinion on the draft report. I am grateful for this supportive opinion and took account of his suggestions in my final report.

8. In view of the strong international initiatives taken by independent data protection authorities, I also sent the preliminary draft resolution to the National Commission for Information Technologies and Liberties (CNIL), Paris and the Federal Institute of Access to Information and Data Protection of Mexico, which will host the 2011 Conference of Data Protection and Privacy Commissioners.

9. I thank everybody, who helped with this report, and hope it will be useful for achieving common standards on the protection of privacy and personal data in Europe and beyond in the age of cyberspace.

1.2. Basic concepts

10. The spectacular growth in information and communication technologies (ICT) has offered considerable opportunities and multiple benefits. Communication networks, especially the Internet, have enabled previously unimaginable services to be introduced while the efficiency and accessibility of existing services have been improved.

11. However, use of these technologies also presents new dangers for privacy and individual freedoms. There are many dark sides to the fate of personal data on the Internet: data gathered without an individual's knowledge, data reused for unacknowledged purposes, data kept for months or even years, data passed on to third parties, confidential data circulated. Individuals using the Internet and the whole range of online services that now exist have to a large extent lost control of their personal information. They do not know what happens to it and have no means of checking from afar who accesses it. A string of Internet and new media stakeholders, on the other hand, are familiar with their tastes, interests, movements, the places they frequent, the people they associate with, etc. These facts call into question the right to privacy and to data protection.

12. **Privacy**, in this context, should be understood not in the traditional sense of a private sphere to be protected and containing a set of private, or even confidential, information to be kept secret, but rather as the right to self-determination and autonomy and an individual's capacity to make existential choices.[2] Here we are talking, more specifically, about **informational self-determination**, that is, individuals' rights to 'know what is known about them', be aware of information stored about them, control how it is communicated and prevent its abuse. Privacy is thus not confined to a pursuit of confidentiality; it is an individual's **control** over his or her image in terms of information.

13. **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.

2. Protection of privacy and personal data in Europe

2.1. Legal standards

14. This section looks first at the binding legal provisions adopted by the Council of Europe. Next, reference is made to the International Covenant on Civil and Political Rights as the only binding universal

[2] For express recognition of the right to self-determination or personal autonomy contained in the right to respect for private life laid down in ECHR Article 8, see ECtHR: *Evans v. the United Kingdom*, judgment of 7 March 2006, no. 6339/05 (confirmed by the Grand Chamber judgment of 10 April 2007); *Tysiąc v. Poland*, judgment of 20 March 2007, no. 5410/03; and *Daroczy v. Hungary*, judgment of 1 July 2008, no. 44378/05.

instrument in the field of privacy. Lastly, European Union provisions are considered, as 27 out of 47 Council of Europe member states are also member states of the EU. The same approach is used for the list of policy standards below.

2.1.1. Article 8 of the European Convention on Human Rights

15. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms guarantees everyone the right to respect for his or her private and family life. Exceptions to this right are allowed if they are in accordance with the law and necessary in a democratic society (that is, they respect the principle of proportionality laid down in the case-law of the European Court of Human Rights – ECtHR) in order to protect the legitimate interests listed in Article 8, paragraph 2.

16. The ECtHR has expressly extended the scope of privacy to cover data protection, thus signalling that protection of personal data is fundamental to the right to respect for private life enshrined in Article 8. The Court holds that Article 8 requires domestic law to afford appropriate safeguards to prevent any misuse or abuse of personal data. Domestic law must also ensure that such data are relevant and not excessive in relation to the purposes for which they are stored and that they are preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[3]

2.1.2. Convention No 108

17. Born out of concern to strengthen the protection of privacy and other personal rights in the context of developments in the field of information technology, Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data was adopted on 28 January 1981.

18. This Convention contains the basic principles of data protection, principles which have been adopted by most national and international instruments in this field and are still relevant today, even if they probably need to be added to. They are as follows:

- Fair and lawful data collection
- Specified purpose (data stored for specified and legitimate purposes and not used in a way incompatible with those purposes)
- Data quality (relevant, appropriate, up-to-date, stored for a limited period)
- Special arrangements for sensitive data
- Data security
- Right of access, rectification and remedy
- Possible exceptions for the sake of paramount public or private interests

19. In 2001, Convention No. 108 was supplemented by an Additional Protocol regarding supervisory authorities and trans-border data flows.

20. The Consultative Committee established under Convention No 108 currently examines possible legal loopholes in the convention, caused by the rapid technological progress of ICT worldwide. The analytical report prepared for the Consultative Committee by Dr Jean-Marc Dinant, Professor Cécile de Terwangne and Mr Jean-Philippe Moiny of the University of Namur (Belgium) focuses on technological challenges such as geo-localisation, cookies and traceability and puts them in relation to the legal standards under Convention No 108.[4]

21. The Consultative Committee also pursued a public consultation on the possible modernisation of Convention No 108 until March 2011.

2.1.3. Convention on Cybercrime

22. The Convention on Cybercrime of 23 November 2001 was drawn up by the Council of Europe (CETS No. 185) but is open for signature by any state in the world.[5] It requires establishing as criminal

[3] ECtHR: *S. and Marper v. the United Kingdom*, judgment of 4 December 2008, nos 30562/04 and 30566/04, § 103; also *Rotaru v. Romania*, judgment of 4 May 2000, no. 28341/95, § 55; and *M.S. v. Sweden*, judgment of 27 August 1997.

[4] The report is available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/T-PD-BUR_2010_09%20FINAL.pdf

[5] It has thus been signed by the United States of America (which has also ratified it), Canada, Japan and the Republic of South Africa.

offences the breaching of data confidentiality by unauthorised access or illegal interception, interference with the integrity of data through their alteration or suppression, and interference with the integrity of the system. States Parties also have to establish the offences of computer-related forgery and computer-related fraud in order to prevent malicious tampering with data.

23. In addition, Parties must enable their authorities to obtain expedited preservation of data, including traffic data, in order to have them available for investigations. A signatory state can be required to preserve and disclose data under mutual assistance arrangements.

2.1.4. Convention on Human Rights and Biomedicine

24. Personal health data is one of the most sensitive personal data. The protection of privacy and personal data is, therefore, regulated in Article 10 of the Convention on Human Rights and Biomedicine (ETS No 164) and Article 16 of the Additional Protocol to this Convention concerning Genetic Testing for Health Purposes (CETS No 203).

25. The right of everyone to the protection of personal health data must include the right to be informed of, and to consent or not to, any collection and processing of such data.

2.1.5. Article 17 of the International Covenant on Civil and Political Rights

26. Article 17 of the International Covenant on Civil and Political Rights signed in New York on 16 December 1966 provides that: '(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.' This is the only binding provision protecting privacy at global level.

2.1.6. Articles 7 and 8 of the EU Charter of Fundamental Rights

27. The Charter of Fundamental Rights of the European Union[6] has been legally binding since the Lisbon Treaty came into force. While Article 7 of this Charter enshrines the right to privacy in the usual terms, Article 8 departs from tradition by securing a separate right to protection of personal data within the general catalogue of fundamental rights. Article 8 provides that everyone has the right to the protection of personal data concerning him or her; the data must be processed fairly for specified purposes and on a legitimate basis (consent or some other basis laid down by law); and everyone has the right of access to his or her data and the right to rectify them. Compliance with these rules must be subject to control by an independent authority.

2.1.7. EU Data Protection Directive 95/46

28. Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[7] took up, in greater detail, the principles contained in Convention No. 108. However, it offers improved protection rules on a variety of points. It has established criteria for making data processing legitimate. The catalogue of the data subject's rights has been extended. Right of access includes the right to know the source of the data and the logic used to process them. The directive establishes the right to object to processing of personal data and the right not to be subject to wholly automated decisions. In addition, the controller is required to give certain information to the data subject. Currently, the EU data protection law is undergoing a reform.

29. The rules governing trans-border data flows are very detailed and resulted in the Additional Protocol to Convention No. 108.

2.1.8. EU Privacy and Electronic Communications Directive 2002/58

30. Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector[8] is a specific directive complementing the general directive (95/46/EC) for regulating data protection in the electronic communications sector. It lays down an obligation to ensure confidentiality of electronic communications as well as traffic data and location data, with

---

6 See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF.

7 *O.J.E.C.* L 281 of 23 November 1995, pp. 31-50.

8 *O.J.E.C*, L 201 of 31 July 2002, pp. 37-47.

some exceptions. It introduces a duty to ensure data security, now coupled with a requirement to notify any serious risks to data. However, this requirement applies only to providers of publicly available electronic communications services. The directive also deals with use of cookies and sending of spam.

2.1.9. EU Data Retention Directive 2006/24

31. The EU Data Retention Directive (2006/24) of 15 March 2006 requires providers of communication services (Internet, fixed and mobile telephony, fax) systematically to retain everyone's traffic and location data for periods of between six months and two years.[9] This directive is currently being revised.

32. Data retention and access to such data by law enforcement authorities has become a politically important aspect in fighting crime and terrorism. In this respect, the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No 198) and the Convention on Cybercrime (CETS No 185) could serve as international legal references as well as the Convention on Mutual Administrative Assistance in Tax Matters (ETS No 127 and CETS No 208).

2.2. Policy standards

Resolution 428 (1970) of the Parliamentary Assembly of the Council of Europe containing a declaration on mass communication media and human rights

33. Through its Resolution 428 (1970) containing a declaration on mass communication media and human rights, the Council of Europe's Parliamentary Assembly established already more than 40 years ago that, "where regional, national or international computer-data banks are instituted, the individual must not become completely exposed and transparent by the accumulation of information referring even to his (or her) private life. Data banks should be restricted to the necessary minimum of information required."

34. This Resolution followed-up Assembly Recommendation 509 (1968) on human rights and modern scientific and technological developments, which had called on the Council of Europe Committee of Ministers "to study and report on the question whether, having regard to Article 8 of the (European) Convention on Human Rights, the national legislation in the member States adequately protects the right to privacy against violations which may be committed by the use of modern scientific and technical methods."

35. It was adopted together with Assembly Recommendation 582 (1970) on mass communication media and human rights, which reaffirmed the earlier appeal by recommending that the Committee of Ministers consider "the establishment of an agreed interpretation of the right to privacy provided for in Article 8 of the European Convention on Human Rights, by the conclusion of a protocol or otherwise, so as to make it clear that this right is effectively protected against interference not only by public authorities but also by private persons or the mass media."

Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy

36. In its 'declaration on mass communication media and human rights' in Resolution 428 (1970), the Parliamentary Assembly defined the right to privacy as "the right to live one's own life with a minimum of interference". Almost thirty years later, the Assembly specified in Resolution 1165 (1998) that, "in view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition".

37. The 1998 resolution contains guidelines intended to supplement national privacy provisions and covering various legal proceedings and penalties to be made available to individuals whose privacy has been infringed.

Resolution 1797 (2011) of the Parliamentary Assembly of the Council of Europe on the need for a global consideration of the human rights implications of biometrics

38. The Parliamentary Assembly recently adopted Resolution 1797 (2011) on the need for a global consideration of the human rights implications of biometrics,[10] which calls on member states to inter alia "promote proportionality in dealing with biometric data, in particular by limiting their evaluation, processing

---

9 *O.J.E.C.*, L 105 of 13 April 2006, pp. 54-63.

10 See http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta11/ERES1797.htm.

and storage to cases of clear necessity, namely when the gain in security or in the protection of public health or of the rights of others clearly outweighs a possible interference with human rights and if the use of other, less intrusive techniques does not suffice."

Resolution (73) 22 of the Committee of Ministers of the Council of Europe on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector

39. The Committee of Ministers developed the first set of political principles through its Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector.[11] Through the adoption of this Resolution on 26 September 1973, the Committee of Ministers considered that it was urgent, pending the possible elaboration of an international agreement, to take steps to prevent further divergences between the laws of member states in this field.

40. Resolution (73) 22 defined inter alia that: "information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated; rules should be laid down to specify the periods beyond which certain categories of information should no longer be kept or used; without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties; the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information; every care should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way; electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirection of information, whether intentional or not." Such standards seem still pertinent in the current ICT era.

Resolution (74) 29 of the Committee of Ministers of the Council of Europe on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector

41. Resolution (73) 22 was complemented a year later by Resolution (74) 29 on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector. Besides a comparable set of standards, Resolution (74) 29 stated that, "especially when electronic data banks process information relating to the intimate private life of individuals or when the processing of information might lead to unfair discrimination, (a) their existence must have been provided for by law, or by special regulation or have been made public in a statement or document, in accordance with the legal system of each member state; (b) such law, regulation, statement or document must clearly state the purpose of storage and use of such information, as well as the conditions under which it may be communicated either within the public administration or to private persons or bodies; (c) that data stored must not be used for purposes other than those which have been defined unless exception is explicitly permitted by law, is granted by a competent authority or the rules for the use of the electronic data bank are amended."

Recommendation (99) 5 of the Committee of Ministers of the Council of Europe for the protection of privacy on the Internet

42. Recommendation (99) 5 is aimed at Internet service users and providers. It contains 'guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways' to be incorporated in codes of conduct. These guidelines set out principles of fair practice for privacy and data protection in Internet communications and exchanges.

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

43. Adopted on 23 November 2010, Recommendation (2010) 13 proposes supervision of the widespread phenomenon of profiling (see 3.2 and 4.2 below). The appendix to the recommendation contains principles that should ensure fair and lawful profiling. A list of cases in which profiling is lawful is provided. The controller is required to limit the risk of error, take security measures and provide data subjects with information about his or her profiling activities. With certain exceptions, individuals are entitled to access their data, correct them, be informed of the purpose of the profiling and the logic used to attribute their profiles, and, last but not least, object to use of their data or to a decision taken solely on the basis of profiling.

---

[11] See https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2.

Resolution No. 3 of the European Ministers of Justice on data protection and privacy in the third millennium

44. In Resolution No 3, adopted on 26 November 2010 at their 30th ministerial conference in Istanbul, the Council of Europe Ministers of Justice show their support for bringing Convention No. 108 up to date in order to find ways of guaranteeing protection of personal rights in the face of the new challenges posed by technology and the globalisation of information. This updating should meet ministers' concerns with regard to issues such as transparency, effective exercise of rights, data security breaches, jurisdiction and applicable law in respect of virtual and transborder relationships (e.g. cloud computing and social networks) and liability.

45. The ministers note that Convention No. 108 is currently the only potentially universal binding legal instrument in the field of data protection. It could therefore become the universal instrument demanded by national data protection authorities. The ministers consequently invite parties outside the Council of Europe to take part in the updating process.

United Nations guidelines concerning computerised personal data files, adopted by the General Assembly of the UN on 14 December 1990

46. The United Nations General Assembly adopted on 14 December 1990 guidelines concerning computerised personal data files.[12]

47. These guidelines are the only political standard established by the United Nations since the entry into force of Article 17 ICCPR. They state that information about persons should not be used "for ends contrary to the purposes and principles of the Charter of the United Nations".

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980

48. The OECD Guidelines of 1980[13] contain what are known as 'fair information principles'. These basic principles of data protection are almost identical to those in Convention No. 108. Unlike the latter, they are not legally binding.

49. The OECD is currently reviewing its data protection guidelines with a view to modernising them. Most of the OECD member states are legally bound by EU law and/or Convention No 108.

Madrid Resolution of 2009 adopted by data protection and privacy commissioners

50. The 2009 Madrid Resolution[14] was the result of joint work by data protection authorities in fifty countries under the leadership of the Spanish Data Protection Agency. It is intended to provide a model incorporating universal standards of data protection, thus covering data protection values and principles that are safeguarded on five continents.

51. In addition to standard aspects of data protection, this resolution contains new elements such as proactive measures (procedures to detect and prevent security breaches, appointment of a data protection officer, privacy impact assessments, etc.) and the accountability principle, which calls for internal arrangements that can be used to demonstrate that the controller is complying with data protection rules.

Jerusalem Resolution of 2010 adopted by data protection and privacy commissioners

52. At their 32nd International Conference in Jerusalem (27-29 October 2010), data protection authorities adopted a resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data.[15]

---

12 See http://ec.europa.eu/justice/policies/privacy/instruments/un_en.htm.

13 See http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html.

14 Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data: http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf.

15 See http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26499/ResoutiononInternationalConference.pdf

Doc.

53. This initiative was responded to by the 30th conference of the Council of Europe Ministers of Justice in their Resolution No. 3 on data protection and privacy in the third millennium (see above), which invited non-European states to accede to Convention No 108 and supported its modernisation.

3. Technology-related challenges to privacy and data protection

54. Ever greater computing power and storage capacity and ever-increasing connectivity are making possible the development of new technologies and applications that constitute a genuine challenge to privacy and data protection. They often entail bulk collection of personal data on citizens, on-line buyers, social network users, etc, sometimes without their knowledge, and an increasingly common use of identifiers (such as IP addresses, RFID tag identifiers and session identifiers) enabling a user to be linked with his or her actions, geographical position or personal data. Moreover, these data can be analysed and correlated to infer further information, for profiling purposes for example. Lastly, the storage and passing on of collected or inferred data tend more and more often to be beyond the control of the data subject, who is powerless with regard to the use, and sometimes misuse, of these data.

55. The consequence is an increased risk of data leakage and tracing of individuals, thus damaging their privacy. It is therefore necessary to look at a number of emerging or changing technologies, their effects and operating as well as the potential dangers that they pose to privacy and data protection.

56. The European Commission had commissioned a comparative study on different approaches to new privacy challenges in the light of technological developments, which was presented by its authors LRDP Kantor Ltd. (Cambridge/London/Oxford) on 20 January 2010. This study proposed some modernisation of the EU Directive 95/46 on data protection.[16]

3.1. Convergence of communication systems

57. Changes in communication systems and information-sharing/information-delivery services are leading to ever greater convergence between these various systems, resulting in less and less transparency regarding the actual tools used and, above all, a loss of control over the dissemination of information, which circulates, is aggregated, reformatted or forwarded.

58. Thus the telephone, provided with computing power and storage capacity, has become 'smart' (smart phones); a computer can be used to telephone; videoconferencing is available on MP3 players; behind a fax number may lie an e-mail address; and calls to a mobile phone can be rerouted to a landline before arriving in the voice mailbox of a VoIP (Voice over Internet Protocol) service consulted on a PC. These examples show how very complicated it is for a user to determine the type of communication system being used and especially where the data sent or received are going to or coming from.

59. Mention may also be made here of developments such as Microsoft's Outlook Social Connector, which can show a person receiving an e-mail the sender's Facebook status. This illustrates the ever-increasing confusion between hitherto clearly separate spheres and the risk of unwanted disclosure of data that this allows.

3.2. Examples of new technologies

Geo-location

60. Increasingly sophisticated and accurate methods exist to establish a user's geographical position, whether directly through data from his or her terminal (using a GPS chip, increasingly common in mobile phones) or through the network to which the user is connected (by triangulating GSM stations or using databases containing the location of WiFi networks – consider the data collected by Google Street View cars in this connection[17]).

61. Electronic management of public transport also makes it possible to track users' movements, for example when they swipe their travel cards. A user's position is sometimes stored or notified to third parties

[16] See the report at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

[17] See http://pro.clubic.com/entreprises/google/actualite-343282-google-acces-wi-fi-repertories-grande-bretagne.html and http://www.infos-du-net.com/actualite/17071-google-wi-fi-reseaux.html (sources in French only).

without informing the user or obtaining his or her consent, opening the way to movement tracking, profiling of absences from home, etc. This calls into question the freedom to move around anonymously.

62. Even more perniciously, geo-location data from photographs (such as those taken with a mobile phone), combined with face recognition technologies as found in software such as Apple iPhoto® and Google Picasa®, enable the location of a person in a photo to be determined without his or her knowledge.

User traceability

63. Contrary to popular belief, browsing the Web leaves far more indications than where we go and what we do in real life. Surfing the Internet leaves various people with a record of what has been done (IP address, service provider, page from which user has come, browsing history, etc). Tools such as IPv6 addressing and cookies (see below) make it possible to identify individual computers and therefore their users. The situation is unlike that in real life, in that there is no question of strolling along the information highways, visiting virtual shops, reading a newspaper or showing an interest in an advertisement – without this being known. One has to wonder about such constant transparency, which would surely not be accepted in the real world.

Ipv6 addressing

64. Because of the proliferation of systems connected to the Internet, the address space defined by the IPv4 standard[18] has been exhausted, jeopardising the growth of the Web. The Ipv6 standard has been created in response, providing a much larger number of separate addresses.[19] By way of illustration, Ipv6 would allow every individual on earth to have several dozen billions of addresses for his or her own personal use.

65. An IPv6 address can be allocated to a device in a variety of ways, one of which uses the device's physical address (MAC address) to generate an Ipv6 address, thus linking traffic to the device and even directing it to an individual. Other methods avoid this situation by generating addresses semi-randomly or using an address server which assigns them automatically.[20]

66. Whether or not an IPv6 address can be used for identification will therefore depend on either the default settings of the system used or the expertise of the user.

Cookies

67. The arrangements concerning cookies are defined by the Web browsing protocol (HTTP) and enable a Web server to send to a user's browser a series of data which the browser will send back to it upon subsequent visits (only to that particular site). A cookie has a limited lifetime, determined either by closing of the browser or by an expiry date. Cookies are thus stored locally by the browser, usually on the user's hard disk.

68. Cookies are used by Web servers for session management and personalisation, but they can also be used for tracing. Moreover, it should be noted that, upon visiting a site, a browser may receive cookies from third-party sites, because the original site includes content from those third-party sites. This technology is often used for audience monitoring and profiling for advertising purposes.

69. Although the most common browsers allow users to manage and even block cookies, these functions are seldom used, either because of ignorance or simply because blocking cookies would make Internet browsing unfeasible.

Smart grids

70. Power distribution grids are now migrating towards a smart model (smart grids) that incorporates information technology in order to optimise generation and distribution, the aim being to match generation and consumption as closely as possible, thus leading to energy savings, avoidance of power cuts, etc. A

[18] IPv4 provides for an address format with 4 bytes, each with a value of between 0 and 255, giving $2^{32} \approx 4.10^9$ possible addresses.

[19] IPv6 uses an address format with 16 bytes, each with a value of between 0 and 255, giving $2^{128} \approx 256.10^{36}$ separate addresses.

[20] Using DHCP protocol

smart grid is based on smart meters fitted with sensors and linked through a network to a system that collects, collates and analyses consumption data.

71. Smart meters send the operator real-time consumption data, enabling consumers to be profiled: absence or presence in the building, use of appliances with an energy signature, etc.

72. Moreover, within the building itself, appliances can also be connected to the smart meter, not only reporting consumption instantaneously but also allowing the meter to influence this consumption, for example by automatically adjusting the temperature of a thermostat or turning off air-conditioning at times of peak consumption.

73. Here again we are witnessing bulk collection of data that can be linked to a person or group of people, enabling their attributes and behaviour to be pinpointed. The risk of uncontrolled disclosure is even greater, when this information is collected by third parties, as in the case of Google's PowerMeter system.[21]

RFID and the Internet of things

74. RFID (radio frequency identification) is an identification technology relying on three components:
- A tag, which is attached to or incorporated in the object to be identified;
- A reader, used to read the tag when it is within range;
- An information system, which receives data from the reader and processes it.

75. The tag consists of an antenna and an electronic chip containing, as a minimum, an identifier. When a tag is read by a reader (using electromagnetic waves), it sends the reader its identifier. The tag structure is very simple, allowing mass production at a cost permitting use on a massive scale, usually just a few pence.[22] Contact with the reader is not required to scan the tag; the scanning distance can vary between a few centimetres and a few dozen centimetres, or even further, depending on the type of tag.

76. RFID tags are used for stock and supply control, collecting road tolls, management of supermarket stocks, check-outs and after-sales service, luggage tracking at airports, and as a means of identifying animals. In some cases, tags may be implanted in human beings – for example, to ensure the safety of children or the elderly, or, on a lighter note, to monitor access to and manage drinks orders in discotheques. Since the identifier is specific to a particular tag, the latter's movements – and therefore the movements of the person or object to which it is attached – can thus be tracked in relation to readers. Since tags are read from a distance, users are not necessarily aware when they are being scanned, which may lead to data leakage or tracking without their knowledge. Simultaneous scanning of a large number of tags allows tagged objects or persons to be identified almost instantaneously in the immediate environment, thus again facilitating profiling of tagged individuals.

77. Various technical solutions are now in existence (and more continue to be developed) to limit the scope for misuse of RFID technology. But they often add significantly to the manufacturing cost, hindering large-scale deployment. Recently, the Article 29 Data Protection Working Party of the EU endorsed a Framework Privacy Impact Assessment for RFID applications.[23]

78. The Internet of things takes the idea of the Internet and identification a (big) step further with the vision of a world in which everything is interconnected: not just people but also things. The Internet thus emerges from the strictly virtual world to include objects from the real physical world using technologies such as RFID, near field communication (NFC), geolocation and sensor networks. Here, the connected objects function largely independently, being able to acquire and transmit information collected through sensors, process it and interact with users and their environment.

79. Although the Internet of things is a young field, where scientific and commercial applications are still in their infancy, it is clearly based on bulk collection and processing of information, most of which can be either directly or indirectly linked to individuals and, by this very fact, present a threat to their privacy.

---

[21] Google PowerMeter is a system enabling users to view their energy consumption on the Web, the data being provided by the smart meter installed in the user's home. Access to this information is usually restricted to the user in question.

[22] It should be noted that a tag can be more sophisticated: it may contain more information than just the identifier and have its own battery in order to be able to transmit over longer distances or act as a sensor, for example.

[23] See http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

Web crawlers

80. A Web crawler (also known as a Web spider) is software written to scan the Web automatically and index content visited, thus providing data for search engines in order to make searching more effective and facilitate access to information. It works by analysing the pages visited, following hyperlinks recursively.

81. Some malicious crawlers analyse pages to harvest e-mail addresses for spam. Others may also browse pages to aggregate and correlate data collected and infer further information.

Biometric data

82. Biometric methods, based on an individual's physiological attributes such as fingerprints, retina, voiceprint and DNA, are increasingly being used to authenticate individuals (verify their identity), whether for electronic payments, border control, access control, face recognition, etc.

83. Biometric data must first be collected before they can be compared with the template to confirm identity. This requires storage of a large amount of personal data, some of which, such as DNA, are an invasion of an individual's privacy, which includes his or her ancestry and descendants.

84. The Assembly adopted recently Resolution 1797 and Recommendation 1960 (2011) on the need for a global consideration of the human rights implications of biometrics, which specifically addressed the protection of personal data and privacy.[24]

Privacy by design

85. The term 'privacy by design' refers to a set of principles drawn up for the design, development and operation of information systems in order to ensure that privacy and data protection aspects are properly taken into account at the design stage and that these systems therefore comply with statutory and regulatory requirements in this field.

86. Mrs Ann Cavoukian, the Information and Privacy Commissioner of Ontario (Canada), is the person behind this initiative, which is based on respect for the user, user transparency regarding data collection and processing, and refusal to compromise by sacrificing privacy to other goals. The basic principles are security measures that are proactive, data protection by default (any exceptions having to be approved by the data subject), and data protection embedded in information systems, rather than being an add-on, and extending throughout the lifecycle of the data collected.

87. These principles are applicable not just to information technology, but also to business practices and physical infrastructure. There is a website on this topic,[25] which, besides providing a general introduction, illustrates the applicability of the approach through numerous case studies, thus demonstrating that it is possible to design efficient systems satisfying business requirements without necessarily sacrificing data protection.

Cloud computing

88. Cloud computing is a recent paradigm of IT. The term covers both the services accessed and delivered through the Internet and the information systems and hardware/software providing these services.

89. The 'cloud' allows considerable flexibility in managing and allocating resources, with the investment model based more on usage-related invoicing, as well as for integrating services between and within organisations, irrespective of geographical position.

90. Various tiers of cloud services are available, the following being the three main ones:

- Infrastructure as a Service (IaaS): The services provided are infrastructure services – principally system hardware and software – and connectivity; infrastructure management is left to the customer;
- Platform as a Service (PaaS): The services provided take the form of a platform, consisting of infrastructure but also a software environment enabling customers to develop or run their own

[24] See http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta11/ERES1797.htm and http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta11/EREC1960.htm.

[25] See http://www.privacybydesign.ca/.

applications; overall management is therefore shared between the service provider and the customer;

- Software as a Service (SaaS): The provider here supplies the customer with a complete applications solution, covering both infrastructure and application software. Such services are offered, for example, by salesforce.com for business management and by Google through Google Mail, Google Documents, Google Calendar, etc.

91. Cloud computing is thus an extension of the security perimeter towards the Internet, where it is extremely hard to exercise effective control. The user entrusts data storage to a third party, the service provider, who hosts the data and processes them in a manner often unknown to the user. This necessitates a genuine relationship of trust between user and service provider – trust that may be reinforced by contractual guarantees. The main challenges concern protecting cloud data, preserving their integrity and maintaining appropriate access control.

Deep packet inspection

92. Data circulating on a network are usually transmitted in the form of packets comprising header and content; the header contains the information needed to allow the network infrastructure to deliver the packet to its destination.

93. Filtering of network traffic to authorise transit – done mostly by firewalls – is based on routing data in the packet header, usually the message source and destination. Deep packet inspection is also based on content-related criteria, analysing not just the header but also the body of the message, that is, its content.

94. This method is obviously more costly in terms of time and resources. It allows information system security to be improved by detecting and filtering out malicious content. However, it can also be used for the purposes of surveillance or censorship.

4. Usage-related challenges

4.1 Data processing

By government authorities

95. Growth of ICT-based e-government is leading to networking of government authorities. This change rests mainly on data-sharing between authorities, the creation of look up files and huge data warehouses, and the interconnection of previously separate databases. This model raises serious questions concerning privacy. The previous 'silo' model of government, in which each body had its own separate data for its specific statutory mission, was presented as a safeguard against an omniscient state for which its citizens would be totally transparent. 'Practical obscurity' was the key to balance in relations between government and the public. This safeguard has disappeared in the name of efficiency. Questions now have to be asked about individuals' control of the data collected on them, the transparency of data interchange and the proportionality of processing.

96. Use of unique identifiers for the purposes of interconnection and transverse access to an individual's data has further increased the risks of loss of control and failure to respect proportionality. Concerns relating to processing of personal data by public authorities have been heightened by the fact that such processing is used as the basis for decisions such as granting of a pension, recognition of special status, assessment for tax purposes, opening of a criminal investigation, etc.

97. Martin Scheinin, the Special Rapporteur of the United Nations on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, condemns the erosion of privacy by state counter-terrorism measures in his report to the 13th session of the UN Human Rights Council.[26] Many states have dramatically expanded their powers in the name of national security and public safety, including overt and secret surveillance, the interception of communications and profiling of persons.

98. The Council of Europe Convention on Access to Official Documents (CETS No 205) tries to balance the right to information with the protection of privacy and personal data.

[26] See http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf.

By commercial bodies

99. Personal data have an economic value. This value is significant in three respects:

- For providers of Internet-based services: knowing the profile of Internet users interested in products or services and being able to break down this interest in detail (web pages visited, links clicked on, frequency of visits, etc) allows them to choose the best way of presenting what they offer;
- For commercial users of databases containing personal information: gathering data from every possible source allows them to build up extremely full databases that can be used and sold on for marketing and mailing;
- For actual operation of the Web: Most services offered on the Internet are free in appearance only. It is user exposure to advertising that finances them. The business model is based on marketing. The latter will be all the more profitable if recipients' profiles are accurate and allow advertisements to be targeted effectively.[27]

100. In each of these three examples, collection and collation of data to create user profiles have become vital operations. Yet in too many cases these operations occur without the knowledge of the people concerned. They often entail use of data for other than the original purpose. And the amount of data collected inevitably raises the question of proportionality. For example, is it necessary, or simply customary, for search engines (such as Google) to keep all the words entered by a particular individual (identified by a cookie) for months on end? Such a set of words is usually incredibly revealing of the user's interests, activities, plans, etc.

101. The National Commission for Information Technologies and Liberties (CNIL) in Paris monitors and punishes violations of privacy and data protection in France since 1974. While 90% of the cases pursued by the CNIL involved violations committed by the public sector in the past, 90% of all cases concern violations by the private sector today. The amount of cases tripled from 2005 to 2009. In its decision 2011-35 of 17 March 2011, the CNIL imposed a fine of 100,000 Euros against Google in France for having collected and processed secretly a large number of personal data derived from Wi-Fi networks and the Google Location Server while taking pictures through mobile cameras for Google Map and Google Street View.[28]

By employers

102. ICT has given employers surveillance tools that would have been unimaginable in the past. Magnetic access cards tell the network operator who is where at what time, whereas ordinary keys gave no such indications. CCTV allows both visitors and staff to be watched. Staff surveillance also occurs through monitoring of Internet browsing and e-mail use on company systems. For employees working off site, geographical location and tracking systems allow fleets of taxis fleets, broken down vehicles or driving vehicles to be managed remotely and their movements to be monitored in real time.

103. ICT also provides tools of insight. A good many employers use the Internet to find information about prospective employees. Google and Facebook, in particular, thus play the part of informers, revealing to a future employer many aspects of the applicant not included in his or her CV.

104. Among famous privacy violations by employers, the case of the Deutsche Telekom seems particularly severe. In 2005 and 2006, top managers of the Deutsche Telekom (Bonn, Germany) had hired a private detective to investigate alleged information leaks within the company. The Deutsche Telekom had used secretly its access to mobile phone data and computer data of staff members and journalists. Following the publication of this scandal through the media in 2008, the German Parliament and the public prosecutor in Bonn started investigations. The Deutsche Telekom subsequently established the post of a company data protection commissioner and sought damages from the meanwhile fired top managers.

105. The Consultative Committee on Convention No 108 currently analyses the need to revise Recommendation R (89) 2 by the Council of Europe Committee of Ministers to member states concerning the protection of personal data used for employment purposes. A report prepared for the Consultative Committee by Mr Giovanni Buttarelli, Assistant European Data Protection Supervisor of the EU, formulates proposals for the revision of this Council of Europe Recommendation. He suggests that "it would be necessary to prohibit more explicitly activities which consist, even occasionally, in the processing of personal

[27] The marketing profits from the Google and Facebook sites amount to several billion dollars annually.

[28] See http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/D2011-035.pdf.

data for the direct and primary purpose of remote monitoring (physical or logical) of work and other personal conduct. Employers should abstain from using the results of this unlawful processing, even when employees are aware of it." [29]

By individuals themselves

106. In many cases, individuals are not fully aware of the impact of their actions when on the Internet. Web 2.0 has given them an opportunity to interact, comment, publish content themselves, and continuously share knowledge, photos, videos, news, moods, etc. However, the spread of information on the Internet sometimes considerably exceeds what might be expected. The example of information drawn from public Facebook pages and automatically attached to e-mails by e-mail software without the senders' knowledge has already been mentioned above. The power behind the Web robots which provide data for the search engines allows information to be retrieved from scattered sites that was published for what was believed to be a limited audience. Something written for a specific circle (a comment on a forum, for example) is therefore likely to reappear removed from its context and juxtaposed with other information.

107. Once information (text, pictures or video) has been published, it is no longer possible to control what happens to it. Deleting it from the original site will not prevent it from continuing to exist wherever it was copied or downloaded prior to deletion. And there is really no chance of ensuring that the use made of the information (for example, on the other side of the world or by persons unknown) will respect the purpose for which it was originally published.

108. This loss of control is particularly disturbing because it is coupled with an 'eternity effect'. Unlike human memory, the electronic memory erases nothing involuntarily. Data can perpetually be retrieved from the past unless it has been decided to spend time and energy deleting them (when it is actually possible to delete them).

109. Individual acts of spite are also a cause for concern. Publishing defamatory or confidential information on Facebook, posting a private or humiliating video on YouTube, or placing a false article about somebody on Wikipedia can cause immeasurable damage in off-line life.

4.2. Profiling

110. The Committee of Ministers of the Council of Europe adopted last year Recommendation (2010) 13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling.[30] Profiling consists of applying algorithms to aggregated data to reveal correlations and develop profiles. The latter are used for individuals, in order to determine how they are to be treated (whether or not as tax evaders, marketing targets for a particular product, possible terrorists on the move, etc). Profiling for business purposes (see above), security reasons or other motives is easy to do, using widely available data (traces, search engine queries, etc) and cookies, for example.

111. Profiling meets legitimate social needs and interests: risk analysis, fraud identification, market segmentation, matching supply and demand, etc. However, it may unjustifiably deprive some individuals of access to certain services. The existence of profiles leads to information being filtered, sorted and selected according to the recipient. This is overwhelmingly true of marketing information today. Will it be the case for all information tomorrow? Profiling may also be a tool of discrimination. How is it possible to challenge a profile or its inappropriate use? Most of the time, the individuals concerned are unaware that these profiles exist, and the people using them have no understanding of the basis on which they have been developed. Lastly, profiling raises serious concerns as to proportionality. The amounts of data collected and the periods for which they are kept are in many cases out of all proportion.

4.3. Data retention

112. Data relating to Internet and new-media use constitute a goldmine of information for police investigations and crime prevention. Since the 11 September 2001 attacks, provisions have been adopted at European level to harmonise the circumstances in which content data, traffic data and location data can be

[29] See http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/T-PD%20BUR(2010)11%20EN%20FINAL.pdf.

[30] See https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864.

kept for the criminal authorities. These data cover the duration, date, recipients and location of all communications, the volume of text messages and e-mails, etc.

113. It is interesting to see the changes in these provisions. The November 2001 Convention on Cybercrime provides that states may, at an authority's request, require expedited preservation of specified data for a maximum period of ninety days, whereas the Data Retention Directive (2006/24) of 15 March 2006 requires providers of communication services (Internet, fixed and mobile telephony, fax) systematically to retain everyone's traffic and location data for periods of between six months and two years. The evaluation of this Directive is ongoing.

5. Conclusions

5.1. Self-regulation

114. While technology raises concerns, it also provides answers. The technical design of tools can ensure that data collection is minimised. The exercise of rights (of access, rectification and objection) can be facilitated through online procedures. The default settings for data disclosure options can be limited rather than set at full. Thus the private sector can meet the concerns raised in this report by applying the principle of 'privacy by design'. It can also adopt or encourage Internet users to use privacy-enhancing technologies (PETs). However, private sector regulation should not be limited to technology but also cover existing customs and practices in this sector, described above.

115. A study on the economic benefits of privacy-enhancing technologies, which was prepared by the private consultancy firm London Economics in July 2010 for the European Commission, analyses the opportunities of privacy-enhancing technologies applied by companies and individuals.[31]

116. One of the weaknesses of self-regulation is that it depends on the initiative and goodwill of the people concerned. It is clear that collective awareness-raising inevitably puts pressure on them and can increase their motivation for reasons relating to their image or that of an entire industry. Another weakness lies in the fact that, unlike legislation, self-regulation is not the result of bringing together different points of view in order to find a balance. Since the rules are mostly laid down by a single category of people, they reflect only the concerns taken into consideration by those people and their own view of a socially and economically acceptable balance.

117. Self-regulatory measures should support and supplement statutory rules. They would undoubtedly strengthen the latter's effectiveness. They ought to be widely encouraged, but, given their weaknesses, should not take the place of national and international legal standards. In order to be successful, a good self-regulation programme should: provide an added value and contribute to proper application in practice of the principles and rules enshrined in the legal framework, taking into account the specific features of the various sectors; involve all stakeholders concerned, including data protection authorities, in the preparation phase, in a transparent way; provide for robust monitoring and enforcement mechanisms, which would foster the trust of individuals; and create a mechanism for its regular review and improvement.

118. However, improved effectiveness will inevitably depend also on raising and extending users' own awareness.

5.2. International law

119. Existing legislation is too ineffectual and has too many shortcomings in its data protection rules. Convention No 108 and the general EU Data Protection Directive were drawn up before the advent of the Internet. It was impossible to take account of the global dimension of information services and any virtual and trans-border context when these data protection rules were drawn up. The frighteningly widespread lack of clarity in the system and the pernicious opportunities for surveillance could not have been anticipated.

120. The relevant provisions most certainly need to be updated, and this should entail the incorporation of new principles such as data minimisation, increased liability and better security (including requirements relating to breaches of data security). Individuals' rights should be strengthened (right to object – including objection to automated decisions, right to data deletion, etc.). Transparency requirements should be established or redesigned.

---

[31] See http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

Doc.

121. Compliance with legislation can be improved by, amongst other means, strengthening the powers of regulatory authorities and introducing the right to take legal class action. Machinery could also be set up to check national legislation before ratification of Convention No 108.

122. Convention No 108 is the only existing and advanced set of standards in this sector under public international law. Therefore, it is necessary to promote accession to Convention No 108 by as many states as possible globally, and to start the drafting of a new protocol to this convention in order to adapt the established standards to new challenges.