THE RIGHT TO DIGITAL PRIVACY: A EUROPEAN SURVEY

Eric Caprioli,[1] Ygal Saadoun[2] & Isabelle Cantero[3]

Translated by Mirella Andee

The right to Privacy has drastically evolved since its emergence and has become an entrenched right across most modern democracies. The first recognition of this right was made centuries ago in Europe, but proper legal enforcement tools were slow to develop. The nature of this right implied such a delay. Indeed, throughout the Enlightenment, which reached its peak during the 18th and 19th centuries, liberty-seekers across the western world primarily fought to restore those fundamental rights that were needed to freely and equally participate in governance. First set out by the Athenian democracy, those rights had been mostly abandoned and excluded from the political and philosophical landscape which had become dominated by monarchies and autocracies.

At the time, privacy was mainly assimilated with freedom from government coercion and the right to respect the secrecy of personal documents. The King was the main threat to people's privacy, as William Pitt, an 18th century British Parliament Member, decried: "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter, the rain may enter, - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement!"[4] In 1765, Lord Camden, wrote, "We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have."[5] In 1766, the Swedish Parliament enacted the

[1] Ph. D, Peace and Development Law, University of Nice Sophia-Antipolis. Mr. Caprioli is head of the Caprioli and associates Law firm and is a lecturer at the Paris II – Sorbonne University. He is a Member of the French delegation at the United Nations Commission on International Trade Law ("UNCITRAL").

[2] Graduating student at the Pantheon-Sorbonne University in Paris (2006). Mr. Saadoun works as a legal journalist at the French Senate and is a professional translator for various multi-national companies. He has also worked for various political and media think-tanks in both the United States and Europe.

[3] D.E.S.S., Business Administration, Institute of Business Administration - University of Nice Sophia Antipolis. Ms. Cantero is head of the Privacy and Personal Data Protection Department at the Caprioli and Associates Law firm.

[4] *See* Brief of Amici Curiae Civil Liberties and Consumer Groups in Support of Defendants' Objections to Magistrate Judge's Discovery Order, at 6, Paramount Pictures Corp., et. al. v. Replay TV, Inc., et. al., 2002 WL 32151632, (C.D.Cal. 2002), *available at* http://www.epic.org/privacy/replaytv/amici_brief_eick_order.pdf (Last visited May 25, 2006) (*quoting* Charles J. Sykes, The End of Privacy, 83 (1999)).

[5] *See* Privacy and Human Rights 2003, An International Survey of Privacy Laws & Developments: Overview, *available at* http://www.privacyinternational.org/survey/phr2003/overview.htm. (*quoting* Entick v. Carrington, 1558-1774 All E.R. Rep.45.).

Access to Public Records Act that required that all information held by public authorities be used for legitimate purposes. Napoleon enacted several provisions in the newly-drafted Code Pénal protecting the secrecy of letters.[6] In 1858, France prohibited the publication of facts related to private life and set strict rules for violators.[7] Legislation relating to privacy across Europe was unsatisfactory, particularly at a time when the State's role increased significantly. The quantity of information and personal data collected by administrative apparatuses subsequently increased, leaving citizens without adequate safeguards against threats to their privacy.

The second half of the twentieth century has witnessed the development of legal instruments meant to protect people's privacy against interference by both states and private entities. The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights which specifically protects territorial and communications privacy.[8] Like the other provisions of the Declaration, article 12 was the result of a political compromise struck between the West and the East, chiefly the U.S.A. and the U.S.S.R. This text was not self-executing and needed to be elaborated particularly regarding the definition of the rights thereby proclaimed. The states, as possible sources of threats, are not named in the text of the article which is meant to protect the personal privacy of their citizens. No reference is made either to limitations of this right or to the circumstances in which those limitations may apply. Although important as a first attempt at the global recognition of the right to privacy, the Universal Declaration of Human Rights could not serve as an efficient bulwark against state interferences with the exercise of this right. At a European level, privacy was to be vested two years later in the European Convention on Human Rights (ECHR). Adopted by the Council of Europe in 1950, Article 8 of the Convention states: "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[9]

---

[6] Article 187, New Code Pénal, replaced by articles 226-15 and 432-9 of the New Code Pénal.

[7] *See,* Privacy and Human Rights 2003, An International Survey of Privacy Laws & Developments: Overview, *available at* http://www.privacyinternational.org/survey/phr2003/overview.htm. (last checked May, 25, 2006) (*citing* The Rachel affaire. Judgment of June 16,1858, Trib. Pr.inst. de la Seine, 1858 D.P. III 62.)

[8] *See*, Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A of December 10, 1948, available at http://www.un.org/Overview/rights.html.

[9] *See*, Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11. (2003), *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457 5C9014916D7A/0/EnglishAnglais.pdf.

Article 8 is fundamental as it lays out the right to have one's privacy respected by any entity while simultaneously providing circumstances in which the State is allowed and sometimes entitled to exert certain prerogatives. "National Security, public safety, [and] the prevention of disorder or crime," are among the reasons a state can interfere with this right. Therefore we can say that security outweighed privacy for the drafters of the ECHR. As stated above, privacy was assimilated with freedom from government coercion. Although having a wider conception of private life – the European Commission of Human Rights ("ECHR") found in 1976 that privacy also comprises to a certain degree the right to establish and develop relationships with other human beings, especially emotional relationships which lead to the development and fulfillment of one's own personality.[10] The Convention confirms this aspect of privacy by outlawing states' interference in basic human relationships. In addition, the Convention on Human Rights formally recognizes the contingent character of the right to respect for private and family life as contrasted by the inalienable character of the prohibition against torture.[11] Indeed, contrary to its Article 8, the European convention on human rights does not provide any situation where the state can limit this right, including when the security of its citizens is in peril. While it did not precisely define the scope of privacy in European law, the 1950 ECHR determined how the signatory countries should regard this right and the behavior they should adopt towards it. The Convention is also crucial because, several years later, many of these countries became members of the European Union and have continued to be bound by its provisions.

At the same time as the right to privacy was being developed and formally recognized, a phenomenon with far-reaching consequences was occurring. The growing use of computers for collecting and handling personal information and data led to a major transformation of the legal tools needed to protect privacy. Following the advent of this phenomenon, concern about unfair information practices developed quickly during the latter half of the 1960's. The term "information-intensity" was coined in reference to the increasing scale of human organizations, making them more remote from their clients, and more dependent on abstract, stored data rather than personal knowledge.[12]

Consequently, during the 1970's, many western democratic countries enacted provisions which provided efficient tools to protect their citizens against interferences to their privacy. Legislation in Europe began with the West German

---

[10] *See,* Privacy and Human Rights 2003, An International Survey of Privacy Laws & Developments: Overview, *available at* http://www.privacyinternational.org/survey/phr2003/overview.htm. (*citing* X v. Iceland, 5 Eur. Comm'n H.R. 86.87 (1976)). *See also*, Niemietz v. Germany, 13710/88 ECHR 80 (1992), *available at* http://www.worldlii.org/eu/cases/ECHR/1992/80.html.

[11] *See*, Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11. (2003), at Article 3, *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf.

[12] *See*, Roger Clarke, *A History of Privacy in Australia: Context* (1998), *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/OzHC.html, (last visited May 25, 2006).

Land of Hesse passing the very first Data Protection Act in 1970 which created the first data protection authority: the Datenschutzbeauftragter. This was soon followed by Sweden's Data Act of 1973,[13] which was the first comprehensive legislation at a national level regulating the use of computerized personal information.[14] The main goal of the Data Act was to prevent "undue infringements upon the integrity of registered persons." France followed suit by enacting the Data Protection Act in 1978 to regulate the use and storage of personal information held by government agencies and private entities.[15] The French Data Protection Act also created an agency in charge of regulating the protection and processing of French citizens' personal data; The National Commission on Informatics and Liberties (Commission Nationale Informatique et Libertés).[16] Most European countries created such a body in accordance to the provisions of future European directives. The National Commission on Informatics and Liberties takes complaints, issues rulings, sets regulations, conducts audits, makes reports, and ensures public access to information by acting as a sort of umbrella-agency over data controlling officials. It can also impose sanctions. The Code Pénal provides a 5 years imprisonment sentence and a 300 000 € fine for all fraudulent, unfair or illegal collection of data. [17]

Despite having similar goals, these laws did not exhibit sufficient signs of unity to protect data on a transnational level. Indeed, with the emergence of the information-intensity phenomenon, some countries offered far better protection than others. Moreover, the transborder flow of this data could lead to the transfer of information to a country where no adequate legislation is in place. In order to prevent the appearance of data-havens where legal protection of privacy is not enforced, two crucial international instruments were adopted in the early 1980's; the Organization for Economic Co-operation and Development ("OECD") guidelines governing the protection of privacy and transborder flows of personal

---

[13] *See*, The Data Act (1973), *available at* http://www.bild.net/dataprSw.htm from The Bulgarian Institute for Legal Development as translated by the Sweden Data inspection board.

[14] *See*, Data Inspection board, *available at* http://www.datainspektionen.se/in_english/personal_data.shtml. (stating that the Data Act was replaced by the Personal Data Act in 1998 to comply to the rules provided by the European Union Directive 95/46/EC).

[15] *See*, Commission Nationale De L'Informatique et des Libertes, *Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés*, *available at* http://www.cnil.fr/index.php?id=301.

[16] *See*, Commission Nationale De L'Informatique et des Libertes, *available at* www.cnil.fr.

[17] *See*, Commission Nationale De L'Informatique et des Libertes, *Data Protection Act*, *available at* http://www.cnil.fr/index.php?id=41. See the same page for other fines and sentences. For the detailed procedure followed by the Commission to impose such sanctions, *see also*, Decree No 2005-1309 of 20 October 2005 enacted for the application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties, *available at*, http://www.cnil.fr/fileadmin/documents/uk/Decree_20_October_2005_English_version.pdf.

data and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("CPI").

In 1980, the OECD adopted guidelines governing the protection of privacy and transborder flows of personal data.[18] The OECD guidelines consider protection of personal data as an essential part of privacy.[19] The guidelines delineated specific rules covering the handling of electronic data. In order to avoid legislational disparities among countries which could hinder the flow of data from one country to another, the OECD recommended that member countries enact into their legislation a number of principles meant to protect privacy.[20]

In 1981 the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[21] Like the OECD, the CPI created specific rules covering the handling of electronic data, although it focused specifically on the automatic processing of personal data. Both the CPI and the OECD require that personal information be:

Obtained fairly and lawfully;
Used only for the original specified purpose;
Adequate, relevant and not excessive to purpose;
Accurate and up to date;
Accessible to the subject;
Kept secure;
Destroyed after its purpose is completed [22]

These texts, the Council of Europe's CPI in particular, have had, and are still having, a deep influence on countries across Europe. Meant to promote electronic commerce, the CPI's provisions are enacted, as well as the 1995 European Union Data Protection Directive, by most of Europe and even by some non-European countries.[23] Non-European countries have enacted these

---

[18] *See*, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[19] For a summary of the guidelines' provisions, *see*, CDT's Guide to Online Privacy, *Privacy Basics: The OECD Guidelines*, *available at* http://www.cdt.org/privacy/guide/basic/oecdguidelines.html.

[20] *See*, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[21] *See*, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *available at*, http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.

[22] *See,* Privacy and Human Rights 2003, An International Survey of Privacy Laws & Developments: Overview, *available at* http://www.privacyinternational.org/survey/phr2003/overview.htm. (last checked May, 25, 2006).

[23] *See*, Eva Y.W. Wong, *Data Protection Legislation in Hong Kong: A Practical Perspective, available at*http://www.is.cityu.edu.hk/Research/WorkingPapers/paper/9429.pdf.

provisions because they are eager to join the Union in the near future or are willing to comply with these regulations to facilitate trade. The 1981 Convention was a major breakthrough towards harmonizing different data regulation legislations as it introduced the creation of a data controller in charge of monitoring data handling and punishing privacy infringements. The 1981 CPI provided a series of definitions relating to data protection that are still partly used to define the regulation and protection of personal data today.[24]

Many European countries uphold these principles in their national legislation. After initially rejecting several bills and recommendations, the British Parliament finally adopted a Data Protection Act in 1984, which had been repealed in 1998 to comply with the 1995 European Union Data Protection Directive.[25] The presence of an official agency in charge of monitoring the enforcement of such rules progressively became a common feature throughout Europe because governmental oversight is an essential aspect of any successful data protection regime. Although the powers of these official bodies vary by country, their prerogatives are geared towards similar purposes.

In 1995, the European Union enacted a directive which updated the rules already in force and unified the data protection laws of its Member States. The 1995 Data Protection Directive[26] reinforces the states' obligations and the data controlling agency's prerogatives. Under Article 28 of the directive, all European Union countries must have an independent enforcement body. This body must be consulted by governments prior to the enactment of laws relating to the processing of personal information. It also conducts investigations, hears complaints, issues reports, and can order the destruction of information or can prohibit its processing if necessary. The Directive represented another step towards an unimpeded flow of information throughout Europe. Two years later, it was supplemented by the Telecommunications Privacy Directive[27] which established specific protections covering telephone, digital television, mobile networks and other telecommunications systems. These communications technologies, including Internet generated data, had not been covered by sufficient provisions until the passage of this Directive.

Although the need for greater protection has been recognized by the European Union, rapidly changing standards and technologies complicated the

---

[24] *See*, The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Explanatory Report*, *available at* http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm.

[25] *See*, Data Protection Act 1998, 1998 Chapter 29, *available at* http://www.opsi.gov.uk/acts/acts1998/19980029.htm.

[26] *See*, Directive 95/46EC 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, *available at* http://ec.europa.eu/idabc/servlets/Doc?id=18534.

[27] *See*, Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, *available at* http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf.

situation. Once transformed into a digital mass of abstract information, personal data can be collected, transferred, consulted and used by a growing number of organizations and entities. The use of that information can be diverse. Marketing is the first to come to mind as it is widely used by businesses. For example, the Internet is a major source of consumer-related material. When surfing the Net, a user can reveal much about his identity, habits and interests.[28] Misuses of that data occur frequently whether by individuals or by organizations. Consumer-profiling technology is no longer a distant means of targeting individuals by monitoring websites typically visited by individual Internet users. Nor is it unimaginable for a relatively skilled computer user to enter someone's computer to steal sensitive information. It is even less difficult for a state having access to that information to exert and intensify a new type of surveillance: Dataveillance. Roger Clarke, a professor of computer science at the Australian National University, is the author of the term. He gave this definition as early as 1988: "Dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."[29]

The shift between old-fashioned privacy-related data and the last twenty years' intense digitalization process increased the level of threats incurred by data subjects. Besides the Internet, telecommunications provide a new generation of data generated by merely using a cell phone. An initial materialization of this new data, referred to as traffic and location data, was Caller-ID technology. The 1997 Directive required the incorporation of an option enabling users to block their number's transmission to Caller-ID equipped devices. Mobile communications now pose additional threats as they can provide details of an individual's movements and activities. This location can be combined with other information including telephone calls and search engine requests; the type of information that can be used to develop precise personal profiles. Privacy is not the only human right put at risk by such tools. Freedom of speech and the right of assembly can be jeopardized as well.[30]

Law enforcement authorities were quick to incorporate this "valuable" information into their investigations against organized crime. An Internet Service provider can be highly useful for police and intelligence services because it gives them the ability to monitor a suspect and his/her acquaintances or accomplices by merely consulting a database of their phone calls. It can at the same time prove to be a major source of privacy infringements as, to paraphrase Lord Camden, transactional and locational data are often the dearest property any man can have. In traditional telephony, transactional data consists of telephone numbers, the call metrics (duration of call, time and date), countries involved,

---

[28] *See*, David Banisar, *Letter written to the South African Committee on Justice & Constitutional Development*, (2001), *available at* http://www.privacyinternational.org/countries/south_africa/pi-sa-intercept-letter.html.

[29] *See*, Roger A. Clarke, *Information Technology and Dataveillance*, (1988), *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html.

[30] *See*, Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, (2000), *available at* http://www.gilc.org/privacy/coe-letter-1000.html.

and the types of service which have been used.[31] While this data was stored by providers, it was only available to law enforcement authorities because the content of the conversations were not stored. Wiretapping required a warrant or a court order, but access to traffic data was possible with lower authorization and oversight requirements. Traffic data has been considered less legally sensitive and, as a result, the obstacles for security services to access them were minimal. The same was true for Internet-generated transactional data, although this rivaled substantive communications in the amount and type of information that it could provide about someone.

In fact, there is no single legal definition for connectional data. Connectional data is generally considered to be the technical information (traffic data, location, billing,...) relating to communications transmitted or received by the users of electronic communications networks, including the Internet. This gives information about the caller or the receiver, including the date, the time and the duration of the call or connection, and the identity of the computers used via their IP addresses. Moreover, the geographical or temporal location of the caller can be associated with other data, enabling verification of the communicator's location or identity. The retention of connectional data, broadly speaking, is an embarassing question that must be considered on legal, technical, economical and political grounds.

Data retention laws must be enforced on different levels. First, one has to determine which classifications of data gained from communications can be retained and by whom. Second, the duration and manner of data retention must be defined. Third, limitations on the ability to access retained data must be specific in case of litigation, and especially in case of judicial queries. Finally, rules must be created to define who will bear the economic cost of data retention, especially the financial cost of requiring operators to retain, access and release stored data.

The issue of data retention lies at the forefront of international, European and national news, bringing a new eagerness to a debate which many may consider outdated. The monitoring of communications generated by data retention for the purpose of public safety raises the issue of fundamental personal privacy rights, including the need to strike a balance between concepts of anonymity and governmental control. New standards, including Voice over Internet Protocol, known as VoIP, offer the ability to communicate from one point on the globe to another by using personal computer. These new services are generating large amounts of connectional data which present a potential source of major privacy infringements. Regulating the flow and collection of these new types of personal communications data presents additional challenges to European lawmakers. Consequently, European legislation will once again have to adapt to efficiently address those risks.

[31] *See* Privacy and Human Rights 2003, An International Survey of Privacy Laws & Developments: Overview, *available at* http://www.privacyinternational.org/survey/phr2003/overview.htm.