Project acronym:	PRESCIENT
Project title:	Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment
Project number:	244779
Programme:	Seventh Framework Programme for research and technological development
Objective:	SiS-2009-1.1.2.1: Privacy and emerging fields of science and technology: ethical, social and legal aspects.
Contract type:	Collaborative project
Start date of project:	1 January 2010
Duration:	36 months

Deliverable D1:

Legal, social, economic and ethical conceptualisations of privacy and data protection

Author(s):	Serge Gutwirth, Raphael Gellert and Rocco Bellanova, VUB Michael Friedewald and Philip Schütz, Fraunhofer ISI David Wright, Trilateral Research & Consulting Emilio Mordini and Silvia Venier, CSSC

Dissemination level:	Public
Deliverable type:	Report
Version:	2.0
Submission date:	23 March 2011

Terms of use

Document history

Version	Date	Changes
1.0	10 December 2010	Working paper, discussed at the expert workshop on 16 December 2010
2.0	23 March 2011	Revised version, including the results of the expert workshop

Contents

1 INTRODUCTION – PRIVACY THROUGH THE PRISM

The aim of this deliverable is to provide a state-of-the-art analysis of legal, social, economic and ethical conceptualisations of privacy and data protection, especially in the context of emerging and future technologies.

To that end, this report presents legal, social, economic and ethical perspectives on three major issues: the conceptualisations of privacy and data protection, the balancing and trade-offs between privacy/data protection on the one side and security and other values on the other, and the challenges raised by future and emerging technologies (FETs). The work is divided in three parts, each of them containing the four perspectives.

The final conclusions sketch the contrasts and similarities between the different approaches and draw the necessary lessons.

2 CONCEPTS OF PRIVACY AND DATA PROTECTION

2.1 The legal construction of privacy and data protection

2.1.1 A "legal" approach

The legal concepts of privacy and of data protection differ from their socio-economic and ethical counterparts, since they must be derived from the classical sources of law that bind the legal practice when it states the law through adjudication. Hence, a description of the *legal* construction of privacy and data protection must draw from an analysis of the pertinent case law, as it develops within the pertinent legislative framework, drawing inspiration from the interpretative and systematising work of legal scholars – the "legal authorities" or the "legal doctrine". Given the constraints of this report, we will focus upon legislation and case law, which have directly binding effects, respectively *in abstracto* and *in concreto*.[1] Given the European context in which this report is written, we will focus upon the European legal order, stemming from the EU and, to a lesser extent, from the Council of Europe.

As the overall aim of this section is to spell out the legal significance of privacy and data protection, we will describe the similarities, contrasts, relationships and overlaps of the two rights, both formally and substantially, and with reference to their constitutional framework.

2.1.2 Mapping the legal content of both rights

It follows from the EU Charter of Fundamental Rights (CFR) that there is a *formal* difference between privacy and data protection On the one hand, art. 7 establishes everyone's right to privacy as a right "to respect for his or her private and family life, home and communications" in almost the same terms[2] as art. 8.1 of the European Convention of Human Rights (ECHR).[3] Art. 8 CFR hallows the right to the protection of personal data, stating not only that

[1] The work of legal scholars will only be referred to if it helps in understanding the issues at hand. Moreover, many debates amongst legal scholars are directly linked to ethical, philosophical, social and economic debates, and will be indirectly dealt with later in this deliverable.
[2] The CFR mentions the more up-to-date term of "communications" instead of "correspondence" in the ECHR.
[3] EU Charter of Fundamental Rights, OJ, C 364/10, 18.12.2000; European Convention of Human Rights, www.echr.coe.int.

"Everyone has the right to the protection of personal data concerning him or her", but also that "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." It also says, "Compliance with these rules shall be subject to control by an independent authority." In other words, the Charter distinguishes two rights of which the former concerns the *privacy of individuals* while the latter focuses on the *processing of personal data* and provides that such processing should be surrounded with (constitutional) safeguards.

Privacy. Since art. 7 CFP is a replica of art. 8 ECHR, at European level the *content* of privacy for legal purposes can be securely derived from the pertinent case law of the European Court of Human Rights in Strasbourg (ECtHR), which has ruled that art. 8 ECHR – with its four components of private life, family life, home and correspondence – can cover a wide range of issues such as integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile, protection of personal data, wiretapping, gender, health, identity (i.e., a right to have some control over identity markers such as one's name), sexual orientation, protection against environmental nuisances and so on: the list is not exhaustive. Interestingly, the ECtHR affirmed that it is neither possible nor necessary to determine the content of privacy in an exhaustive way.[4] It also implied that privacy is a relational concept that goes well beyond a mere right to intimacy, with the important consequence that art. 8 rights may also protect visible and public features and conduct of individuals (public privacy).[5] Progressively, the Strasbourg Court also acknowledged the right to make essential personal choices (such as name and sexual orientation) and eventually this has led the Court to state that individual self-determination or autonomy is an important principle underlying its interpretation of art. 8 ECHR.[6] In this sense, the Court seems to favour a "liberty" rather than a "bundle of subjective rights" approach to privacy.[7]

---

[4] *Niemietz vs. Germany* of 16 December 1992, § 29 and *Pretty vs. U.K.,* of 29 April 2002, Judgment: "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. However, it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude there from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."

[5] E.g. *Rotaru vs Romania* of 4 May 2000, § 43; *P.G. & J.H. vs U.K.*, of 25 September 2001, § 57, *Peck vs U.K.,*of 28 January 2003, § 58.

[6] *Pretty vs U.K.,* of 29 April 2002, § 61, Judgment: "As the Court has had previous occasion to remark, the concept of 'private life' is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (X. and Y. v. the Netherlands judgment of 26 March 1985, *Series A* no. 91, p. 11, § 22). It can sometimes embrace aspects of an individual's physical and social identity (Mikulic v. Croatia, no. 53176/99 [Sect. 1], judgment of 7 February 2002, § 53). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (see e.g. the B. v. France judgment of 25 March 1992, *Series A* no. 232-C, § 63; the Burghartz v. Switzerland judgment of 22 February 1994, *Series A* no. 280-B, § 24; the Dudgeon v. the United Kingdom judgment of 22 October 1991, *Series A* no. 45, § 41, and the Laskey, Jaggard and Brown v. the United Kingdom judgment of 19 February 1997, Reports 1997-1, § 36). Article 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, Burghartz v. Switzerland, Commission's report, op. cit., § 47; Friedl v. Austria, *Series A* no. 305-B, Commission's report, § 45). Though no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees. "

[7] Rigaux, F., (ed.), *La vie privée, une liberté parmis les autres?*, Larcier, Brussels, 1992; Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, 2002.

Data Protection. If the fundamental right to privacy is, as seen above, formulated in general terms, the more recent explicit recognition of the fundamental right to data protection in generic terms has been preceded, since the late 1970s, by abundant and detailed international, European and national legislation. At European level, the most important piece of regulation is EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, commonly known as the Data Protection Directive.[8] In art. 7, the Directive establishes a number of quintessential conditions for personal data to be processed legally, amongst which the "unambiguous consent of the data subject" and/or the fact that the processing serves "legitimate interests pursued by private interests". The Data Protection Directive also recognises a number of subjective rights for data subjects (such as the right to receive some information whenever data is collected, to access the data, to have data corrected, and to object to certain types of processing) and imposes some obligations upon data processors, who must guarantee the confidentiality of data against unauthorised access and, in some cases, must notify a specific independent supervisory body before carrying out certain types of data processing. The Data Protection Directive further enacts a number of principles such as the purpose specification principle (the processing and use of data for specified, explicit and legitimate purposes), the fairness principle (all processing must be fair and lawful to the data subject) or the data quality principle (all data must be adequate, relevant and not excessive in relation to the aim for which they are processed). Regarding sensitive data as mentioned in art. 8, the regime is stricter and, in principle, prohibitive.

Other relevant EU instruments include the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters of 27 November 2008[9], the 2002/58/EC Directive (E-Privacy Directive) which actualises the data protection principles to face some of the new challenges raised by the continuing developments in the electronic communications sector[10] and Regulation EC No. 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.[11] This Regulation is particularly important because, inter alia, it created the European Data Protection Supervisor, an autonomous EU institution with the powers of supervision, consultation and co-operation (art. 41). In addition, in art. 16, the Treaty of Lisbon on the Functioning of the European Union (TFEU) enacted a general constitutional provision on data protection[12] and it gave the CFR binding force in the EU.

[8] European Parliament and the Council, 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. OJ L 281, 23.11.1995.

[9] Council Framework Decision 2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350/60, 30.12.2008. This Framework Decision aimed to fill the gap left by the restricted scope of the Data Protection Directive, by providing a regulatory framework for the protection of personal data in the area of police and judicial co-operation, or what was called the "third pillar" before the entry into force of the Lisbon Treaty.

[10] Recital 4 mentions that the aim of the directive is to translate "the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector".

[11] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1, 12.01.2001.

[12] "Everyone has the right to the protection of their personal data" (art.16[1] TFEU).

2.1.3 Interplays

Privacy and data protection are thus different, but they are certainly not unrelated. They are intertwined and overlapping, but their respective scopes and regimes should be distinguished.

As a matter of fact, the ECtHR did effectively look at data protection cases through the prism of privacy (art. 8 ECHR) and it has developed criteria to assess whether an issue of data protection touches or not upon the right to privacy. The Court thus distinguishes between the processing of data that concern the private life and the processing of data that do not. It uses two criteria to make the distinction: the nature of the data processed and the extent of the processing. If the data are intrinsically linked to the private life of the individual, then the processing will fall under article 8 without further doubt. If the data are not "essentially private", one will have to look at the extent of the processing: does it systematically store the data, does it store the data though not systematically, with a focus on the data subject, or could the data subject not reasonably expect the processing? In a number of cases, the Court has condoned data processing with regard to issues pertaining to the privacy of the data subject.[13] Unlike data protection, which directly applies every time "personal data" are processed, privacy protection ex 8 ECHR does not. And that means that not every processing of personal data, covered by data protection legislation, necessarily affects privacy. But it will be protected through data protection nevertheless.

Where the Strasbourg Court has acknowledged that a data protection issue is also a privacy issue because it judged that the data concerned were privacy-sensitive, it has granted some of the guarantees foreseen in data protection legislation: it has acknowledged a right to access to personal files[14], claims regarding the deletion of personal data contained in public dossiers[15] and the correction of "official sexual data" from transsexuals[16]; it has further insisted upon the necessity of having independent supervisory authorities in the context of the processing of personal data[17]; it endorsed the principle of purpose limitation when it ruled that personal data cannot be used beyond normally foreseeable use[18], and the principle that governmental authorities may only collect relevant data based on concrete suspicions[19]. Finally, the Court acknowledged the right to financial redress in the case of a breach of article 8 caused by the processing of personal data.[20] But even if the Court has consecrated some of the data protec-

---

[13] *Amann vs Switzerland* of 16 February 2000, § 65, *Rotaru vs Romania* of 4 May 2000, § 43; *P.G. & J.H. vs U.K.*, of 25 September 2001, § 57. See also De Hert, P., and S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action", in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), *Reinventing data protection?*, Springer, Dordrecht, 2002, pp. 3-44.

[14] ECtHR, *Gaskin v. the United Kingdom*, Application No. 10454/83, Judgment of 7 July 1989; ECtHR, *Antony and Margaret McMichael v. United Kingdom*, Application No. 16424/90, Judgment of 24 February 1995. ECtHR, *Guerra v Italy*, Judgment of 19 February 1998, *Reports*, 1998-I; ECtHR, *McGinley & Egan v. United Kingdom*, Applications nos. 21825/93 and 23414/94, Judgment of 28 January 2000.

[15] ECtHR, *Leander v. Sweden*, Application No. 9248/81, Judgment of 26 March 1987; ECtHR, *Segerstedt-Wiberg and others v. Sweden*, Application No. 62332/00, Judgment of 6 June 2006.

[16] ECtHR, *Rees v UK*, Judgment of 25 October 1986 *Series A*, No. 106; ECtHR, *Cossey v UK*, Judgment of 27 September 1990, *Series A*, No. 184; ECtHR, *B v France*, Judgment of 25 March 1992 *Series A*, No. 232-C; ECtHR, *Christine Goodwin v. the United Kingdom*, Application No. 28957/95, Judgment of 11 July 2002.

[17] ECtHR, *Klass v. Germany*, § 55; ECtHR, *Leander v. Sweden*, §§ 65–67; ECtHR, *Rotaru v. Romania*, §§ 59–60. See in detail: *Gaskin v. the United Kingdom*, Application No. 10454/83, Judgment of 7 July 1989; ECtHR, *Z. v Finland*, Application No. 22009/93, Judgment of 25 February 1997.

[18] ECtHR, *Peck v. the United Kingdom*, § 62; ECtHR, *Perry v. the United Kingdom*, § 40; ECtHR, *P.G. and J.H. v. the United Kingdom*, § 59.

[19] *Amann v. Switzerland*, § 61 and § 75 ff.; ECtHR, *Segerstedt-Wiberg v. Sweden*, § 79.

[20] *Rotaru v. Romania*, § 83.

tion principles in its rulings – inspired also by the CoE Convention 108 and the international development of data protection law – the case-by-case approach, be it only because of its inherent characteristics, could never lead to a result similar to the systematic and general nature of data protection law.

The ECJ is competent to make rulings concerning conflicts based upon the Data Protection Directive. Some of its cases have been permeated by a "privacy logic". It has stated that the processing of personal data can affect the right to privacy. Therefore, provisions of the Directive that might affect this right must be interpreted in the light of art. 8 ECHR,[21] and must pass the threefold threshold test foreseen by the article,[22] although Member States enjoy a wide margin of appreciation.[23] In its first judgment, the Court went even so far as to declare that an unlawful data processing is equal to a breach of privacy.[24] References to the threefold test of the ECHR were also made in other cases.[25] However, in more recent cases, the European Court of First Instance has reminded us that "the mere presence of the name of a person in a list of participants at a meeting does not compromise the protection of the privacy of the person".[26]

Finally, in their conceptual relationship, it is important to underline that data protection is both broader and narrower than privacy. It is narrower because it only deals with personal data, whereas the scope of privacy is wider. It is broader, however, because the processing of personal data can have consequences not only in terms of privacy, but also in terms of other constitutional rights. For example, data processing can impact upon people's freedom of expression, freedom of religion and conscience, voting rights, etc. Most importantly, the knowledge of individuals that can be inferred from their personal data may also bear risks of discrimination.

2.1.4 The relationships between the legal concepts of privacy and data protection

In addition to other fundamental human rights, both privacy and data protection are legal consequences of the political institutionalisation of the private sphere – drawing the limits of state power – in liberal democratic constitutional States. Such a concept of the State is historically rooted in the resistance and rejection of former absolutist and arbitrary economies of power. Henceforth, power is limited and not absolute as the result of a double constitutional architecture. On the one hand, the power of the State is limited and counterbalanced by the power of the individual, holder of inalienable fundamental rights that can be invoked against the State. On the other, the power of the State is subject to constitutional rules holding the government to its own rules and to a system of mutual checks and balances amongst its three powers (trias politica, transparency and accountability). Furthermore, government is dependent on the sovereign polis constituted by the people since it can only be legitimate if it can be considered as an expression of "the people": representation and elections. Such a political architecture is thus not only based upon the assumption that the individual exists as an autochthonous, constitutive and autonomous political actor, but it also constitutionally enforces it. By building a human rights shield against state intrusions around the individual, it consequently institution-

[21] ECJ, Österreichischer Rundfunk, §. 68
[22] ECJ, Österreichischer Rundfunk, §. 83
[23] ECJ, Österreichischer Rundfunk, §. 83
[24] ECJ, Österreichischer Rundfunk, §. 91.
[25] See Opinion of the Advocate General Leger in Cases C-317/04 and C-318/04, §. 229.
[26] ECtFInstance, *The Bavarian Lager Co. Ltd v Commission of the European Communities*, §§. 114-115.

alises a private sphere distinct from – but articulated upon – the public sphere, where government and state power intervention is legitimate.[27]

The *legal* "right to a private life" and the *legal* notion of "privacy" have been construed by judges and, later, enacted by legislators against the background of this "political private sphere" of individual liberty and autonomy. The elaboration and further enactment of the legal right to privacy was an answer to gaps and weaknesses detected in the protection of individual liberty by the older, more classical human rights (such as prohibition of torture, freedom from arbitrary arrest, freedom of expression). This programmed "the right to privacy" to become a residual legal line of defence against illegitimate or disproportionate interferences with and limitations of individual liberty, autonomy and self-determination. In that sense, the "right" to privacy is the ultimate legal defence of liberty.[28]

The fundamental rights to privacy and data protection thus participate in the protection of the political private sphere, although in different ways. Privacy sets prohibitive limits that shield the individual against the State (and other) powers warranting a certain level of *opacity* of the citizen, whilst data protection channels legitimate use of power, imposing a certain level of *transparency* and accountability to power. The logics of opacity and transparency are fundamentally different: *opacity tools (of government)* are prohibitive and normative, they determine whether an interference with individual autonomy is acceptable or not.[29] This is very much the case of the right to privacy in European case law. *Transparency tools*, on the other hand, come into play after normative choices have been made, in order to channel the normatively accepted exercise of power through the use of safeguards and guarantees in terms of accountability and transparency. Data protection legislations obey such logic: they generally do not dispute the fact that personal data might be processed, but they submit the processing to rules and conditions, they empower data subjects by giving them subjective rights and they establish supervisory bodies in order to make sure that data processors don't abuse their powers.

The conclusion is that privacy and data protection, like other human rights, are legal instruments designed to safeguard the "political private sphere", but they have a very different mode of operation: privacy shields the individual, data protection controls and channels the instances that process personal data.

2.2 Why is privacy important from a social point of view?

2.2.1 Defining the social point of view

What is meant by the social dimension of privacy? Here it means that privacy is important to both the individual and to society. Society can be interpreted simply as the collectivity of people living in a country or, even more broadly, living in the EU. A society is more than that, however. A society is composed of people who have some affiliation with each other, notably

[27] Gutwirth, Serge, "De polyfonie van de democratische rechtsstaat", in Elchardus, M. (ed.), Wantrouwen en onbehagen, VUB Press, Brussels, 1998, pp. 137-193; De Hert, Paul, and Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in Erik Claes, Anthony Duff et al. (eds.), *Privacy and the criminal law*, Intersentia, Antwerp, Oxford, 2006, pp. 61-104.
[28] De Hert, P., and S. Gutwirth, "Regulating profiling in a democratic constitutional state", in M. Hildebrandt and S. Gutwirth (eds.), *Profiling the European citizen: Cross disciplinary perspectives*, Springer, Dordrecht, 2008, pp. 271-291.
[29] De Hert and Gutwirth, 2008, op. cit.

through some shared political, social, economic, cultural or other structures, including communications networks and virtual societies, such as the Information Society, promoted by the European Commission. A society will generally support certain shared values, such as those written into the European Charter of Fundamental Rights or the Lisbon Treaty. European society shares values such as dignity, autonomy, privacy, data protection and European solidarity. Some of these values are also rights (e.g., the right to dignity, the right to privacy, the right to data protection).

When we speak about the social dimension of privacy, we imply an interest in understanding the value of privacy to both the individual and society. We signal an interest in understanding the value of privacy in particular societal contexts, of understanding its value in relation to other social values, such as security, free markets and private enterprise. The social dimension of privacy is concerned with issues such as the free flow of information across national borders, the personalisation of services, the ubiquity of surveillance cameras, national ID card schemes, identity theft, loss of personal data, etc.

2.2.2 Privacy as an individual fundamental right

In Europe, privacy is a fundamental right. The protection of individual privacy is enshrined in Article 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe 1950) and Article 7 of the 2000 Charter of Fundamental Rights of the European Union. In addition, data protection in the EU is governed by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive), Directive 2002/58/EC on privacy and electronic communications (the e-Privacy Directive), the Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (the so-called Data Protection Framework Decision)[30], and the Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108).[31]

The right to privacy and the protection of personal data are enshrined in these charters, conventions and directives, because privacy is an important value to the individual and to society and because privacy and personal data are subject to threats and need protection.

Personal data has value, not just to the individual but also to governments, companies and others. Personal data fuels our modern service economy. It enables us to cross borders. It supports our entitlement to government benefits and can be used to check if we are defrauding the State. Privacy, which might have sheltered us from the gaze of others in days gone by, from their knowledge of who and what we are, has become a problematic concept. Governments, companies and others want to know more and more about us, to possess our biometrics and much else that defines our personhood.

---

[30] European Council, Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30 Dec. 2008, pp. 60-71.

[31] "The Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) can be considered as the first European legal framework for the fundamental right to protection of personal data. The right to data protection is closely related but not identical to the right to private life under Article 8 of the European Convention for Human Rights. The right to data protection is recognised as an autonomous fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union. The principles of Convention 108 were refined in Directive 95/46/EC which forms the main building block of data protection law within the EU." Article 29 Working Party, The Future of Privacy, 1 Dec 2009, p. 5.

The dangers to privacy are well understood. Jennifer Chandler, as one among many examples, points out that "A person who is completely subject to public scrutiny will lose dignity, autonomy, individuality, and liberty as a result of the sometimes strong pressure to conform to public expectations. In addition to freedom from the pressure to conform, privacy also protects the individual from another party's use of his or her information to manipulate, outcompete, or otherwise exploit the individual."[32]

In addition to such dangers, some experts have observed that privacy itself has become dangerous, at least to governments concerned about crime and terrorism. To deal with these threats to society, some politicians and policy-makers seem to believe that it is necessary to fuse and mine databases and to surveil the population in many different ways in order to find those who would illegally disrupt our societies and way of life. Thus, says Peter Burgess, the fundamental concept of privacy has changed radically in the last decades.

> While we can still talk of a person's privacy as a kind of relation to knowledge about the person, this knowledge is no longer the sole dominion of that person. The assumption of a right to control knowledge about oneself is no longer reserved to the person. Information about the person is no longer personal, but rather transportable, commercial, marketable…. Information, far more than hard security practices, is seen as the key to European security. Privacy has metamorphosed from being the object of security to a very threat to security. We have moved from a modern society, organized around a legal, economic, social, cultural and moral separation between a private sphere and a public sphere, to a late- or postmodern society where that separation has become the threat to society itself.[33]

Over the last century or so, since Warren and Brandeis wrote their famous *Harvard Law Review* article on the right to privacy[34], jurists, academics, privacy advocates and others have addressed threats to privacy and the need to protect privacy, but with the shock of 9/11, if Burgess is right, we are witnessing a new turn of events, where privacy itself is viewed as dangerous.[35] In addition to law enforcement authorities and intelligence agencies who seek to ferret out those among us who are invidious to social order, the private sector has its own profit incentives to know their customers in intimate detail in order to better target and persuade them to consume their products and services.

---

[32] Chandler, Jennifer, "Privacy versus national security: Clarifying the Trade-off", in I. Kerr, C. Lucock and V. Steeves (eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, Oxford: 2009, pp. 121-138 [p. 124]. Daniel Solove has identified harms to privacy in some considerable depth. See Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge, MA, 2008, pp. 174-179. See also Calo, M. Ryan, "The Boundaries Of Privacy Harm", Berkeley Electronic Press, July 2010. http://works.bepress.com/m_ryan_calo/2

[33] Burgess, J. Peter, "Security After Privacy: The Transformation of Personal Data in the Age of Terror", Policy Brief 5/2008, International Peace Research Institute, Oslo (PRIO), 2008. http://www.prio.no/Research-and-Publications/Publications/?mode=type&type=12

[34] Warren, Samuel, and Louis D. Brandeis, "The Right to Privacy", Harvard Law Review, Vol. 4, No. 5, 15 Dec 1890, pp. 193-220.

[35] Harvard Law professor William Stuntz has described privacy and transparency as "diseases", arguing that "in an age of terrorism, privacy rules are not simply unaffordable. They are perverse." See Stuntz, William J., "Against Privacy and Transparency, Secret Service", *The New Republic*, 17 April 2006. Cited by Solove, Daniel J., "Data Mining and the Security-Liberty Debate", *University of Chicago Law Review*, Vol. 75, No. 1, Winter 2008, p. 343-362 [p. 345].

2.2.3 Privacy as a social value

When discussing the social value of privacy, two schools of thought compete. The first argues that "privacy is dead", whereas the others praises it for its social value.

According to the "privacy is dead, get over it" school, struggling to protect privacy is a futile exercise.[36] In addition to Scott McNealy, various others have made similar comments about the death of privacy. For example, Facebook founder Mark Zuckerberg has been reported as saying that the rise of social networking online means that people no longer have an expectation of privacy and that privacy was no longer a "social norm".[37] Google CEO Eric Schmidt once said of his company's ambitions: "When we talk about organizing all of the world's information, we mean all."[38] A deputy director of the US Office of National Intelligence said that "Too often, privacy has been equated with anonymity… In our interconnected and wireless world, anonymity — or the appearance of anonymity — is quickly becoming a thing of the past."[39] His British counterpart made a similar observation: "Modern intelligence access will often involve intrusive methods of surveillance and investigation, accepting that, in some respects this may have to be at the expense of some aspects of privacy rights."[40] Various government agencies are funding the development of technology to detect brain activity remotely and are hoping to eventually decode what someone is thinking.[41] If such research is eventually successful, it could be fairly said that the "privacy is dead" thesis will have prevailed. Our thoughts are surely the last redoubt of privacy.

The "privacy is dead" thesis serves well those who are desirous of knowing everything about us so they can market new services to us[42] or determine whether we are cheating on the social benefits system, have over-stayed in the country or harbour terrorist aspirations. Companies might try to blur the distinction between personally identifiable information and personally embarrassing information, which might make them seem like they care about their customers' privacy.[43] In reality, the personally identifiable information is more valuable for marketing purposes than pictures that users might share with friends of their revelries last Friday night.

---

[36] Sun Microsystems CEO Scott McNealy has been (in)famously quoted as warning, "You have zero privacy anyway. Get over it." See Sprenger, Polly, "Sun on Privacy: 'Get Over It'", *Wired*, 26 Jan 1999. http://www.wired.com/politics/law/news/1999/01/17538

[37] Johnson, Bobbie, "Privacy no longer a social norm, says Facebook founder", *The Guardian*, 11 January 2010. http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

[38] Stross, Randall, "Google Anything, So Long as It's Not Google", *The New York Times*, 28 Aug 2005. http://www.nytimes.com/2005/08/28/technology/28digi.html?pagewanted=1&_r=1

[39] Pinkerton, James P., "Privacy is a thing of the past", *The Denver Post*, 24 Nov 2007. http://www.denverpost.com/opinion/ci_7535993

[40] Travis, Alan, "Fight against terror 'spells end of privacy'", *The Guardian*, 25 Feb 2009. http://www.guardian.co.uk/uk/2009/feb/25/personal-data-terrorism-surveillance

[41] Farahany, Nita, "The Government Is Trying to Wrap Its Mind Around Yours", *The Washington Post*, 13 Apr 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/04/11/AR2008041103296.html?hpid=opinionsbox1

[42] Story, Louise, "To Aim Ads, Web Is Keeping Closer Eye on You", *The New York Times*, 10 March 2008. http://www.nytimes.com/2008/03/10/technology/10privacy.html?em&ex=1205467200&en=9aba6985f3668765&ei=5087%0A

[43] Microsoft Research's social media expert Danah Boyd argues that the distinctions between private and public are different in the network age. In particular, she contrasts what she calls personally identifiable information with personally embarrassing information and notes that these need to be treated differently because the consequences of exposure are different. Thompson, Bill, "Networks blur the private and public divide", BBC News, 17 March 2010. http://news.bbc.co.uk/1/hi/technology/8570406.stm

Not everyone agrees that privacy is dead, or wants to see it die.[44] Even Google's Schmidt was so upset by the CNET News story about him that Google banned any of its employees from talking to CNET News for a year.[45] The irony could not be greater – Google and many other companies want to know as much about their users as possible, while their executives do not want their users to know so much about them.

No matter how often it has been said that privacy is dead and that we should get over it, most people still believe in the importance of privacy[46] and are not suckered by those who seek to exploit our privacy to their own ends.[47]

This in turn, might lead us to think that privacy is valuable for the society. There are various indicators of the importance privacy has achieved in political, social and cultural terms in the last half century. One indicator is in number of laws, regulations and policies dealing with privacy. Before 1970, virtually no country had privacy and/or data protection legislation. Another indicator is the amount of attention that privacy gets from the news media, academics and other stakeholders. Yet another indicator is privacy's presence in popular culture, in films such as Alfred Hitchcock's *Rear Window* (1954), Francis Ford Coppola's *The Conversation* (1974), Irwin Winkler's *The Net* (1995), Tony Scott's *Enemy of the State* (1998), Andrew Niccol's *Gattaca* (1997), Peter Weir's *The Truman Show* (1998), Steven Spielberg's *Minority Report* (2002) and Florian Henckel von Donnersmarck's *The Lives of Others* (2006).[48]

While privacy as a fundamental right and as a social value can be understood as two separate things, some commentators have made the point that "the conception of privacy as an individual right could be challenged by an emergent recognition of privacy as a social value".[49]

Daniel Solove goes further and argues that "The value of privacy should be understood in terms of its contributions to society."[50] He also rightly says that "when privacy protects the individual, it does so because it is in society's interest."

Aharon Barak goes further still when he states that "The concept of a 'right' derives from the concept of society; without society, rights have no meaning."[51]

While privacy has traditionally been regarded as an individual right and/or value – and still is – a growing number of privacy scholars have begun to consider its importance to society. Priscilla Regan was one of the first to identify why it is important to society. In a section enti-

---

[44] Froomkin, A. Michael, "The Death of Privacy?", *Stanford Law Review*, Vol. 52, May 2000, pp. 1461-1543. "Despite the warnings of information privacy pessimists, all is not lost – yet" (p. 1461).

[45] Stross, op. cit.

[46] A survey by Ofcom in the UK indicates that more people are becoming sensitive to the threats to their privacy. The Ofcom "survey of the internet habits of 1,824 people aged 16 and over, found that since 2007 users have become more savvy about online security and are now more reluctant to provide personal information online". Sweney, Mark, "UK web users 'wary of revealing too much'", *The Guardian*, 17 May 2010. http://www.guardian.co.uk/media/2010/may/17/social-networking-facebook-privacy-ofcom

[47] Clifford, Stephanie, "Two-Thirds of Americans Object to Online Tracking", *The New York Times*, 29 Sept 2009. http://www.nytimes.com/2009/09/30/business/media/30adco.html?hpw

[48] For an insightful discussion of such films, in the context of surveillance and privacy, see Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, UK, 2007, Chapter 7.

[49] Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge MA, 2006, p. 49.

[50] Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge, MA, 2008, p. 173.

[51] Barak, Aharon, "Proportionality and Principled Balancing", *Law & Ethics of Human Rights*, Vol. 4, Issue 1, 2010, p. 3. http://www.bepress.com/lehr/

tled "The Social Importance of Privacy" of her 1995 book, *Legislating Privacy*, she comments that

> Privacy has a value beyond its usefulness in helping the individual maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better off as well when privacy exists. I maintain that privacy serves not just individual interest but also common, public and collective purposes. If privacy becomes less important to one individual in one particular context, or even to several individuals in several contexts, it would still be important as a value because it serves other crucial functions beyond those that it performs for a particular individual.[52]

Regan cites three reasons why privacy has social importance. First it has a *common value*. "Some rights, which protect individual interests, are regarded as so fundamental that all individuals in common have a similar interest in them… in much the same way that people of different religious beliefs have a common interest in a right to free conscience, people of different privacy beliefs or preferences have a common interest in a right to privacy." Second, it has a *public value*. "A public value of privacy, then, is derived from its importance to the exercise of rights that are regarded as essential to democracy, such as freedom of speech and association, and from its importance as a restraint on the arbitrary power of government." Third, privacy has a *collective value*. "No one member of society can enjoy the benefit of a collective good without others also benefiting." Like clean air and national defense, privacy is an example of a collective good.[53]

Arthur Cockfield, the Associate Dean of Queen's University Faculty of Law in Canada, sides with Regan and contends that the social value of privacy and the individual rights aspect of privacy are "critical to the functioning of our democratic state".[54] He adds that "Even if privacy becomes less important to certain individuals…, it continues to serve other critical interests in a free and democratic state (e.g. the need to protect political dissent) beyond those that it performs for a particular person."[55]

Stephen Margulis examines the social dimension of privacy and finds that "Privacy is social in two senses: the social-psychological and the social-political. This duality is a bridge between social-psychological privacy as social behaviour and socio-political privacy as a social issue." He says that from the social-psychological point of view, privacy is social in three ways: "(a) Privacy's foci are interpersonal communication and social interaction. This view of "social" predominates… There are two less frequent referents. (b) How we experience, understand, react to, and enact privacy are products of our social and cultural development… (c) Privacy is an attribute not only of individuals but also of groups and, for some theorists, orga-

---

[52] Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy, University of North Carolina Press*, Chapel Hill, 1995, p. 221.

[53] Regan, ibid., pp. 220-231.

[54] "Judges, lawyers and policy-makers need to take into more explicit account both the individual rights aspect of privacy as well as the social value of privacy, that is, society's interest in preserving privacy apart from a particular individual's interest. Both of these aspects of privacy are critical to the functioning of our democratic state." Cockfield, Arthur J., "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies", *U.B.C. Law Review*, Vol. 40, No. 1, May 2007, pp. 41-68 [p. 41]. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1031964

[55] Cockfield, Arthur J., "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies", *U.B.C. Law Review*, Vol. 40, No. 1, May 2007, p. 42

nizations". From the social-political point of view, he cites Regan and her three reasons why privacy is important as a social value (see above).[56]

Alan Westin, author of the landmark classic, *Privacy and Freedom*, also comments on the social dimension of privacy, e.g., as follows: "The importance of that right to choose, both to the individual's self-development and to the exercise of responsible citizenship, makes the claim to privacy a fundamental part of civil liberty in democratic society. If we are switched on without our knowledge or consent, we have, in very concrete terms, lost our rights to decide when and with whom we speak, publish, worship, and associate. Privacy is therefore a social good in democratic societies, requiring continuous support from the enlightened public."[57]

In line with the aforementioned scholars, Julie Cohen adds her support to the case that privacy is of fundamental value to both the individual and society. Like others, she contends that privacy underpins other values such as autonomy and anonymity:

> A degree of freedom from scrutiny and categorization by others promotes important non-instrumental values, and serves vital individual and collective ends… informational autonomy comports with important values concerning the fair and just treatment of individuals within society…. A realm of autonomous, unmonitored choice, in turn, promotes a vital diversity of speech and behavior. The recognition that anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association—decisions that otherwise might be chilled by unpopularity or simple difference—is part of our constitutional tradition…. The autonomy fostered by informational privacy also generates more concrete collective benefits. Development of the capacity for autonomous choice is an indispensable condition for reasoned participation in the governance of the community and its constituent institutions—political, economic, and social…. Examination chills experimentation with the unorthodox, the unpopular, and the merely unfinished. A robust and varied debate on matters of public concern requires the opportunity to experiment with self-definition in private, and (if one desires) to keep distinct social, commercial, and political associations separate from one another.[58]

Recognising the social value of privacy is very important when we enter the debate about balancing privacy against other social values such as security. Viewing privacy as "only" an individual right or value in the context of security as something that is important to us all creates the distinct risk that privacy will come out the loser in the balance between privacy and security. Cockfield makes this point too. "The traditional understanding of privacy often focuses on the individual rights aspect of privacy by emphasizing privacy as an individual's claim against state interference. This understanding generally leads to legal analysis that sees privacy as an interest which competes with security, sometimes resulting in calls for the need to dilute privacy to protect the public against criminal and/or terrorist activities."[59] And so does Solove: "Privacy is often cast as an individual right and balanced against the greater

[56] Margulis, Stephen T., "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 243-261. http://onlinelibrary.wiley.com/doi/10.1111/josi.2003.59.issue-2/issuetoc

[57] Westin, Alan, "Social and Political Dimensions of Privacy," *Journal of Social Issues*, Vol. 59 No. 2, 2003, pp. 431-453 [p. 434]. http://www.blackwell-synergy.com/toc/josi/59/2

[58] Cohen, Julie E., "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Revie*w, Vol. 52, No. 5, 2000, pp. 1373-1437 [pp. 1423-1426].

[59] Cockfield, Arthur J., "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies", *U.B.C. Law Review*, Vol. 40, No. 1, May 2007, p. 42

social good, which results in privacy being frequently undervalued in relation to many conflicting interests."[60]

Thus, in balancing security and other social values against privacy, it is necessary to take into account privacy's value both to the individual as well as to society.

2.3 The economics of privacy and data protection

In economic discourse, the notion of privacy is mainly understood as informational privacy and therefore almost exclusively limited to the question of using personal (or corporate) data for business purposes.[61] Thus, data protection rather than privacy issues are central to economic analysis. Rarely is the question raised why it might be valuable to protect privacy and personal data. Moreover, mainstream economic theory does not really make a distinction between the protection of an individual's personal data and the protection of confidential corporate data and trade secrets.

The background of this understanding is the concept of "information economics", which is a branch of (neoclassical) microeconomic theory studying how information affects economic decision-making. In our context, information economics mainly deals with two issues: *information asymmetry* and *information goods*.

Information asymmetries are related to decisions in transactions where one party has more or better information than the other. This creates a power imbalance in transactions. For George J. Stigler, one of the key leaders of the Chicago school of economics and the intellectual father of information economics (Nobel prize winner 1982), privacy is a factor that increases information asymmetries because one party can retain (personal) information that might be important for the decision-making of the other party.[62] The existence of such information asymmetries gives rise to problems such as moral hazard[63] and adverse selection[64]. For these reasons, orthodox neoclassical theory rejects data protection as an undesirable market disturbance.

In recent years, *behavioural economics* has extended the understanding of economic decision-making of individuals and institutions beyond the paradigm of rational choice. Building on Herbert Simon's theory of bounded rationality[65], behavioural economics recognises that social, cognitive and emotional factors are important, especially when decisions are made

[60] Solove, *Understanding Privacy*, op. cit., pp. 78-79.
[61] Even though public data controllers are of the utmost importance, representing the largest and most powerful data collectors, they are mainly left out of the economic analysis, because they follow a more complex cost-benefit rationality involving societal benefits which are discussed in chapter 2.2.
[62] Stigler, George J., "An Introduction to Privacy in Economics and Politics", *Journal of Legal Studies*, Vol. 9, 1980, pp. 623-644. Another influential exponent of the Chicago School is the legal researcher and jurist Richard A. Posner. See Posner, R. A., "The Economic Theory of Privacy", *Regulation*, Vol. 9, No. 3, 1978, pp. 19-26.
[63] Moral hazard occurs when a party insulated from risk behaves differently than it would behave if it were fully exposed to the risk. Cf. Arrow, Kenneth J., *Essays in the theory of risk-bearing*, North-Holland, Amsterdam, 1970; Baker, Tom, "On the Genealogy of Moral Hazard", *Texas Law Review*, Vol. 75, 1996, pp. 237-292.
[64] Adverse selection refers to a market process in which "bad" results occur when buyers and sellers have access to different information and the "bad" products or customers are more likely to be selected. See for instance the classic study by Akerlof, George A., "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics*, Vol. 84, No. 3, 1970, pp. 488-500.
[65] Miller, Kent D., "Simon and Polanyi on Rationality and Knowledge", *Organization Studies*, Vol. 29, No. 7, 2008, pp. 933–955.

under risk and uncertainty. In this context, researchers explore empirically the preconditions under which individuals are trading privacy (or rather personal data) for other benefits.[66]

Concentrating on easily quantifiable variables, the economic discourse mainly attends to informational privacy, which deals with disclosing or holding back certain private, personal or sometimes other sensitive information. Whereas information economics as a branch of neoclassical microeconomic theory conceive the protection of personal (private) data –as opposed to corporate sensitive data or organisational privacy (e.g. trade secrets), as an undesirable market distortion, behavioural economics try to include the individual perception of privacy in terms of social, cognitive and emotional factors into their models. This way the classical economic paradigm of informational privacy is decisively widened; taking a concept of privacy into account that is linked to trust.

Although it will be shown later on (3.3) that both sides benefit at least to some extent from the disclosure of personal data, a striking asymmetry, e.g. in awareness of what data is actually processed, in access opportunities of this data and eventually the economic profit resulting from the data collection, seriously harms a sustainable trust relationship not only between consumer and (service) provider but also citizen and state. This asymmetry should be reduced in the interest of both parties.

The other important development in the economic valuation of privacy is that (private) information is increasingly becoming a commodity and the basis of new types of businesses. These include typical information services ranging from search engines and personalised advertising to sophisticated data mining services.

In a nutshell, the economic value of privacy is twofold: Whereas data protection or informational privacy refers to the material value of personal data, the immaterial value of privacy in broader terms can be linked to the importance of trust between data subject and data controller, which becomes forcefully apparent when it is compromised.

2.4 Ethical approaches to privacy and data protection

Ethics is a branch of philosophy that rationally assesses questions about morality; say about issues that can be classified as good (or right) and bad (or wrong). Ethics is a philosophical enquiry about concepts involved in practical reasoning, *viz.* concepts which regard the way in which human beings chose among possible different courses of action. Provided that there are events which are actions, say, events that are controlled, at least in part, by an agent, who contributes to cause them according to some intentions, ethics investigates (1) *the notions involved in actions, say, ethical principles such as good and evil, right and duty, virtues, obligations, free will, etc., their foundation and their rationale*. Ethics also deals with (2) *claims made in these terms, their soundness and consistency*. Finally ethics, when it is applied to a specific social fact or practice, also deals with (3) *practical problems that involve the ethical principles and the assessment of the rationale behind each option of action*.

The modern idea of privacy does not belong primarily to ethics. It is a term originated by the social, political and legal theory to describe what is not public business, notably, which is not business of the law and the government (whatever kind of government it is). The notion of

[66] Acquisti, Alessandro, "Nudging Privacy: The Behavioral Economics of Personal Information", *IEEE Security & Privacy*, Vol. 7, No. 6, 2009, pp. 82-85.

privacy becomes an ethical term when it is framed in terms of right, say, the (a) *right to privacy*, or when it is framed in terms of good, say, (b) *privacy as a value* or as an (c) *instrument to achieve other values (e.g., being free, flourishing, achieving some virtues, affirming his own dignity, etc)*. This opens three main issues, say, 1) the foundation of the notion of privacy as an ethical concept; 2) the ethical and political implications of privacy claims; and, in the specific context of this discussion paper, 3) ethical problems raised by emerging technologies vis-à-vis the notion of privacy, and what actions should be undertaken.

Privacy is an ethically multifaceted concept, being equally a good to be achieved (both a value per se and an instrument which allows to achieve other values) and also a right. Either privacy is conceptualized as a good or as a right, or as both, its value needs to be justified, say, one should provide reasons that explain why privacy deserves to be achieved or/and to be protected. In this first section, the ethical approaches to privacy will provide an overview of the philosophical and ethical discussion around the concept and the value of privacy, will trace the biological, anthropological, and psychological antecedents of the need to privacy, and the notions of private and public spheres in modern political thought, and finally we will discuss the current philosophical perspectives on privacy.

The ethical approach mainly addresses privacy as a result of the tension between two constitutive human polarities, the will to be autonomous and the need to be dependent. The human condition implies the existence of the tension between the individual (his or her particular needs and wills) and the community. Humans are herd and individualistic animals at once: in the western artistic and philosophical tradition, the individual is *homo homini lupus*, as well as a *political animal*. This polarity has biological, anthropological and psychological antecedents, which generate the notions of private and public spheres in political philosophy. The German philosopher Arthur Schopenhauer exemplified such an aspect of the human condition by the so-called hedgehog's dilemma. The dilemma is concerned with the idea that hedgehogs can only get so close to warm one another before they inevitably hurt each other with their spiny backs. Schopenhauer takes this paradox and applies it to the human condition: the closer they become, the greater is the potential for humans to hurt one another. Yet they need to be close to each other in order to get the necessary warmth. The ultimate solution to this dilemma seems to involve locating an optimal distance between the subjects.[67]

The demarcation of a physical and symbolic area around the individual is an inescapable human need, as is the need to be part of a wider human community. Setting the boundaries between these two necessary realms is not, however, an easy task. Each civilization has framed the private-public polarity in different ways, and its current version, which dates back to the 18th century, is only one of the possible versions of this unsolvable opposition.

2.4.1 Foundations for privacy in biology, anthropology and psychology

Taking evidence from different scientific disciplines, ethics provides a rationale for why privacy is important and deserves to be protected.

Biology provides some interesting clues about the origins of the concept of the private sphere in humans, chiefly thanks to studies on the territoriality of animals, and on crowding and isolation. Many studies have indicated that crowding may have effects on individual perform-

[67] Schopenhauer, Arthur, *Parerga und Paralipomena*, 1851, translated by E.F.J. Payne, Oxford University Press, Oxford, 2000.

ance, social behaviour and health.[68] The problem of crowding has gained increasing attention since the industrial revolution, with the migration from rural areas towards cities, with larger numbers of people living in smaller areas. In the contemporary metropolis, environmental stressors, such as heat, noise and air pollution, deeply affect the behaviour of individuals. Many studies provide evidence that overcrowding acts as an intensifier of stressful condition and, under extreme conditions, can itself induce stress reactions or pathological behaviour. Yet from infancy, human beings are acutely aware of their dependence on others. Such dependence lasts long beyond the standard mother-newborn dependence witnessed in other species. Anthropologists use the term "neoteny" to refer to the tendency of mammals to remain dependant on others and to exhibit juvenile characteristics in later stages of life**.** Human beings present a higher level of neoteny*,* which is probably one of humans' greatest resources. Biological research shows that conditions of extreme isolation can be much more pathological than overcrowding, and can generate severe psychological and physiological consequences. Neoteny is also an important cause of tension, conflict and stress. Dependence in the sense of having one's wants correctly anticipated and met may be a pleasant state for a short period of life. But sooner or later, frustrations and obligations entailed by dependence become burdensome.

In anthropological literature, many scholars have claimed that aspects of privacy can be found in every society, since it is "an essential part of human flourishing and well-being"[69]; in other words, privacy is a "cultural universal".[70] The book *Privacy: studies in social and cultural history*[71], written by the American anthropologist and political scientist Barrington Moore Jr., remains one of the most important scholarly contributions on the social and anthropological basis of privacy. "In all forms of civilizations," writes Moore, "the relationship between the individual and the larger society has been a major concern for religious, political and ethical thought." In Moore's analysis, the group always emerges as the source of both security and anxiety. The core of Moore's argument is that social obligations are a fundamental feature of all social organisations, even the most rudimentary ones. Social obligations necessarily imply some limitations to individual freedom. This is the main reason why individuals tend to create private spaces in which they can potentially disobey obligations without being socially sanctioned. According to Moore's conception, the creation of the private sphere ultimately results from the need to transgress social rules in a safe and socially accepted way, which is not disruptive for the whole society.

In psychology, the idea that the private realm could be conceptualised as an escape from the pressure of civilization is present in Freud's account of privacy. According to Freud, the distinction between the private and public realms can be considered as one of the strategies used by human civilization to deal with the burdens of contemporary society. Moreover, Freud believed that the private sphere includes a vast array of experience which goes beyond our awareness: the final result is that we never completely master, as we usually believe, the boundaries between the private and public realms.[72]

---

[68] For a brief overview of the research on crowding, see Epstein, Yakov M., "Crowding Stress and Human Behaviour", *Journal of Social Issues*, Vol. 37, No. 1, 1981, pp. 126–144.

[69] Moore, Adam, "Privacy: its value and meaning", *American Philosophical Quarterly*, Vol. 40, No. 3, 2003, pp. 215-227.

[70] The conceptualisation of privacy as a cultural universal was first provided by the American scholar Alan Westin in his book *Privacy and Freedom* (1967). A cultural universal is an element common to all human cultures worldwide; for a more complete definition, see the work of the French anthropologist Claude Lévi-Strauss, *The Savage Mind*, 1966.

[71] Moore Jr., Barrington, *Privacy: Studies in Social and Cultural History*, M. E. Sharpe, Inc., 1984.

[72] Freud, Sigmund, "Zeitgemässes über Krieg und Tod", *Imago*, Vol. 4, No. 1, 1915, pp. 1-21; Freud, Sigmund,

2.4.2 Foundation for privacy in political philosophy

In political philosophy, the core of the concept of privacy lies in the negotiation of the boundary between the internal and external spheres of human existence. The ways in which privacy is conceptualised and protected can tell us a great deal about the social relations and political structures of a given historical period.

In Western political philosophy, the first conceptualisation of the private sphere as opposed to the public realm dates back to the ancient classical world. The first historical conception of the public in the sense of a generalised notion of other human beings as a source of obligations and authority begin to emerge in ancient Greek democracy.[73] In the Classical period (the period of Pericles's government in Athens), the public realm of the polis was the sphere where a man could flourish as a complete person[74], while the realm of the private, the *oikos* (household), was the focus of the family identity (persons and properties).

The notion of the private sphere, as we understand it, is a product of the 18th century modern liberal thought and refers both to the realm of the family and to the realm of the individual interests and needs, as opposed to the sphere of politics, the place where citizens discuss their common concerns and the activity of public institutions for the administration of the community. In modern liberal thought, the distinction between the private and public spheres mainly derived from the need to balance powers in society. One of the cornerstones of liberal theories is that power corrupts and consequently absolute power corrupts absolutely, and it is to be avoided.

The 20th century totalitarianisms probably represent the most evident example of the total intrusion of the state into the personal space of the individual. In totalitarian states, the control over individual life by the state was perpetuated through the transparency imposed on their lives. Totalitarian regimes are not, however, the sole form of totalitarianism: there is also a "democratic totalitarianism" which is based on the so-called "tyranny of intimacy". In his meaningfully entitled book *The Fall of the Public Man*, Richard Sennett analyses the paramount importance of the passion men put in the *res publica*, and argues that the state of its decay in modern times is rooted in the ages when the public life began to be "corrupted" by the private realm. Sennett deeply analyses the erosion of the delicate balance between public and private life which maintained society in the first flush of its secular and capitalistic existence.[75]

2.4.3 The current philosophical debate on the concept of privacy

Western philosophers have experienced great difficulty in reaching a comprehensive and satisfying definition of privacy. There is a great diversity of opinion in what privacy means, how it might be protected and how it is valued. The contemporary notion of privacy is associated with the concept of *autonomy*, as the capacity to put distance between us and others, to

---

"Das Unheimliche", *Imago*, Vol. 5, No. 5-6, 1919, pp. 297-324.

[73] See Arendt, Hannah, *The human condition*, University of Chicago Press, 1958.

[74] The terminology for privacy in European languages is rich and diverse. Many languages draw on the Latin verb *privare*, meaning "to separate, deprive", while others have developed terminology from other sources. In this etymology arises the sense of deprivation which comes from the word *privatus* ("belonging to oneself", used in contrast to *publicus*, "belonging to the public"), indicating a person standing apart from the public sphere.

[75] Sennett, Richard, *The fall of public man: On the social psychology of capitalism*, Vintage Books, New York, 1978.

develop our beliefs and desires, to maintain a certain level of control over the inner spheres of the self, to exercise a certain degree of individual power to make choices, to limit access to oneself and to be separate from the community. As individuals, we exist to the extent that we are able to make decisions and represent ourselves as autonomous beings. The individual power to be autonomous is the result of the delicate balance between our desire to be independent and our need of the community. The autonomy of the individual is realised against a particular group of others. The community differs according to different cultures and historical forms of public organisation, such as the tribe in pre-literate societies, the *polis* for the Athenian man, the state derived from the social contract in liberal thought.

Another crucial element in the conceptualisation of privacy is the idea of the internal/external boundary negotiation. A completely private life isn't a life inherently human, just as a completely public life disappears from the personal sphere which is crucial for human development. Privacy also refers to the will to protect the intimacy of both a person and a close relationship between individuals. Everyone has the right to be the owner of his self-representation, as well as to be inviolate, invisible and anonymous while protecting his intimacy. Privacy is a concept that has intuitively something in common with terms such as seclusion and solitude (as a choice to be separate from others, in opposition to loneliness), anonymity, confidentiality and secrecy (as the concealment of certain matters from others), modesty, reserve and intimacy (as the respect for one's personality and individuality).

The legal and philosophical debate concerning privacy intensified and became more prominent in the second half of the 20th century. One can distinguish in the literature *descriptive accounts of privacy* (focusing on its meaning) and *normative accounts* (focusing on the defence of its value). One way of understanding the growing literature on privacy is to view it as divided into two main currents of thought, one of which is the category of *reductionism* (which supports the idea that conceptual clarity can be achieved by reducing privacy claims into their basic components)[76] and the other of *coherentism* (defending its fundamental distinctive value)[77]. Arguments to justify privacy's value are either linked to its *consequences* (privacy is valuable because of its desirable consequences), or to the fact that it is a fundamental part of human nature (the *deontological* argument). Discussion of the concept is complicated by the fact that privacy appears sometimes to be valuable because it provides a sphere within which the individual is free from interference by others, and yet it also appears to function in the sense of separation from others. Privacy embodies both the right to freedom from unreasonable constraints (*anti-oppression* argument) and the right to build one's identity (*flourishing* argument). A related conceptual classification in the philosophical and legal debate on privacy is, therefore, the one that differentiates two different functions of privacy, the *separation-based accounts* of privacy that rely on privacy's "negative function" (privacy functions by separating individuals from the others, limiting access to one's body, mind, information) and the *control-based accounts* of privacy that rely on privacy's "positive function" (privacy provides the individual with control over certain aspects of his or her life).

---

[76] See, for instance, Thomson, Judith J., "The right to privacy", *Philosophy and Public Affairs*, Vol. 4, 1975, pp. 295-314. According to the author, privacy is derivative "in its importance and justification", since any privacy violation is better understood in the light of other interests and rights, most properly rights of property and bodily security. See also Posner, R.A., "The economics of privacy", *The American Economic Review*, Vol. 71, No. 2, 1981, in which the author states that privacy is not distinctive because the personal interests it protects are inefficient.

[77] The distinction between reductionists and coherentists was introduced in Schoeman, Ferdinand D., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.

In the second half of the 20th century, scholars have described several aspects of privacy, such as physical (linked to the physical protection of the body), psychological (linked to the autonomy of the spirit, in order to develop as an independent human being), economical (linked to the right of property), informational (linked to the disposal of personal information), as well as decisional (referring to a sort of decisional power). Having a quick look at the extensive literature on the subject, narrow views of privacy defend it as control over information about oneself[78], while others defend it a broader concept required for human dignity[79], or crucial for intimacy[80]. Some scholars consider privacy as an extension of one's personality or personhood[81], while others reduce its meaning to a restricted number of different torts, such as intrusion, private facts, false light and appropriation[82]. During the 1990s and 2000s, the debate on privacy has evolved in order to address the challenges raised by the emergence of new technologies, as well as by the security needs of the post-9/11 world. For the most part, philosophical and legal theorization about privacy has operated within the traditional liberal paradigm. Some authors have also considered the social value of privacy[83], pointing out that privacy issues are related to power relationship between people and the institutions. Other scholars have argued that privacy rights can be detrimental to societal needs[84]. Some other scholars have also warned against the potential for privacy to act as a protector of harmful behaviour: this is the case of the feminist critique[85], that worried about the "darker side" of privacy, referred as a right to protect sexual harassment and domestic violence. More recently privacy has been defined in terms of "contextual integrity"[86], meaning with this expression that several variables, including the nature of the situation and the nature of the information in relation to that context, concur in a violation of privacy. The notion of privacy as contextual integrity helps solving some practical problems, and allows to develop ad hoc algorithms to be applied by electronic systems. Yet from a more theoretical point of view is hardly a novelty, and it does not solve most political and philosophical controversies related to the notion of privacy (e.g., the notion of "contextual integrity" refers to a definition of each context which is not at all neutral and objective. It is apparent that when actors disagree about what a given context entails in terms of privacy rights and distribution of information, the theory cannot be applied any longer).

---

[78] Perhaps the best examples is the definition of privacy given by William Parent, who defines it as "the condition of not having undocumented personal information known or possessed by others". See Parent, W., *Recent work on the concept of privacy*, American Philosophical Quarterly, Vol. 20, No.4, 1983. See also Alan Westin, *Privacy and freedom*, Atheneum, 1967.

[79] Edward J. Bloustein, *Privacy as an aspect of human dignity: an answer to dean Prosser*, 1964

[80] Julie Inness defines privacy as "the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions". See Inness, J., *Privacy, Intimacy and Isolation*, 1992.

[81] Pound, R., *Interests in Personality*, Harvard Law Review, Vol. 28, p. 343, 1915; Fried, *Privacy (a moral analysis)*, 1970; Jeffrey Riemann, *Privacy, Intimacy and Personhood*, Philosophy and public affairs, Vol. 6, No. 1, Autumn 1976.

[82] "One who invades the right of privacy of another subject to liability for the resulting harm to the interest of the other. The right of privacy is invaded by (a) unreasonable intrusion upon the seclusion of another...; or (b) appropriation of the other's name or likeness...; or (c) unreasonable publicity given to the other's private life...; or (d) publicity that unreasonably places the other in a false light before the public..." See Prosser, *Privacy*, California Law Review Vol. 48, No. 3, 1960.

[83] Solove, Daniel, *Conceptualizing privacy*, California Law Review, 2008

[84] As exemplified in Posner, R.A., *The Right to Privacy*, Georgia Law Review 1978, vol. 12, p. 393–422 (that criticizes privacy rights from an economic perspective) and Etienne, A., *The Limits of Privacy*, Basic Books, New York 1999 (that criticizes privacy rights from a communitarian perspective).

[85] See Catherine MacKinnon, *Toward a Feminist Theory of the State*, Cambridge: Harvard University Press, 1989

[86] Nissenbaum, Helen, *Privacy as contextual integrity*, Washington Law Review, Vol. 79, No. 1, Feb 2004.

One can see from an ethical approach to privacy as sketched here that defining its essence and value is a complex task indeed. The complexity of the concept lies in the fact that privacy embodies a set of different values and sometimes conflicting ideas, and that its definition depends on an interaction with the role of the public, in a given society and in a given historical period. Nevertheless, the ethical perspective helps in understanding that the value of privacy lies in the importance of the creation and maintenance of a private sphere, as shown from biological, anthropological, psychological and philosophical evidence.

2.4.4 Data protection from an ethical perspective

The Latin term *datum* (what is given) can be defined as "a piece of evidence considered as fixed for the purpose in hand"[87]. The plural, *data*, is a general term that commonly refers to a set of information that can be used as a basis for reasoning or calculation, while data protection refers to the implementation of a set of measures to guard against the unauthorized access to specific types of data. In Europe, the Data Protection Directive regulates the processing of 'personal data', referring with this expression to any information relating to an identified or identifiable natural person, the 'data subject'. With particular reference to the concepts behind the expression "*personal data protection*", ethics should investigate the moral justifications behind the protection of such information (i.e. explain why should we protect them, what is the rationale of this protection) as well as the modalities in which that protection can be realized (what does this protection exactly mean and how can be realized).

As reported in detail in Moore's anthropological analysis of privacy, all cultures have constrained the access to certain types of data. In the very last decades, the amount of the data collected and the speed of the data exchange have dramatically increased due to advances in information and communication technologies and to globalization. In the contemporary society, information has become one of the most valuable assets, and data – in all their forms – are among the most commonly used types of currency. The main principles governing the data protection practices in Europe are based on the idea that personal data shall be collect with the data subject consent and shall be processed fairly, for specified and lawful purposes, and that data should be kept secure and updated, which implies that data subjects should be allowed to access their data and to make corrections to them. It has to be pointed out that the main aim of the EU Data Protection Directive – and of other previous international legal instruments on data protection – is to regulate the processing of personal data *in order to* support the free flow of such information.

Privacy and Data Protection. Privacy and security of personal data are among the most pressing issues in the analysis of the ethical and social implication of emerging ICTs technologies. From an ethical perspective, privacy and data protection are two different but interrelated notions. From one hand, data protection can be included among the different types of privacy, under the heading of *informational privacy,* which can be defined as the right to keep control over the flow of information about oneself. On the other hand, ethical dilemmas related to the field of data protection can also refer to different issues with respect to those strictly related to the privacy of information, such as the prevention of harm (new vulnerabilities to harm of the digital society)[88], the prevention of informational injustice (injustice done on the basis of information usage), moral autonomy and self determination, data security and accountability for their processing. The potential to use particularly sensitive personal data,

[87] Simon Blackburn, The Oxford Dictionary of Philosophy, Oxford University Press, 1994.
[88] See Jerome Van Den Hoven, Information Technology, Privacy and Personal Data, in *Information technology and Moral Philosophy,* Jerome Van Der Hoven, John Weckert, Cambridge University Press.

such as health data or the information on sexual or religious orientation, raises additional crucial ethical issues.

Data Sensitivity. With reference to the data sensitivity, a case where data subjects are giving up huge amounts of particularly sensitive personal data is represented by the medical context, where patients provide physicians with particular sensitive health information for their own wellbeing. Information plays a crucial role in healthcare: electronic medical record (EMR) systems and databases help managing patient care and supporting research and public health activities. They are enhancing the delivery of cost-effective health care, but are also raising important issues of privacy and confidentiality, concerns about the security of the information or about its secondary uses, or over the use of medical data mining for profiling. The absence of a comprehensive legal framework for electronic medical records does not help to face these problems. We are also experiencing the explosion of web sites offering health services and medical information, with the increasing possibility to place personal medical data on the web. Health related website offer a wide range of information and services and are used by health professionals, patients and the public with increasing frequency. Ethical standards and guidelines for health related websites have been developed and can provide a framework for the use of healthcare data in the hard-to-regulate Internet space.

Personal data as private property. In the current debate surrounding the ethical implications of data protection, one of the biggest issues is related to the increasing emergence of a conception of personal data as a commodity, or to the fact that individuals are already participating in the commodification of their personal data. The idea of a propertization of personal data that would potentially offer a solution to the data protection problems resulting from the Information Revolution had emerged.

The conception of a property rights approach to privacy has originated in America in the late 60s[89], but has been particularly debated after the entry into force of the EU Data Protection Directive, when among the proposed interpretations of the tension between American and European different sensibilities there was the suggestion that "data protection" could be cast as a property right[90]. The main question remains whether property rights in personal data could be an effective means to enhance their protection.

A strong relation between property and personhood emerges in important property theories, such as Locke's labour theory, but also Marxist and Foucault's theories. Locke's theory on property has provided important justificatory strands for granting "Lockean-style property rights" [91], such as intellectual property rights[92], or the suggested allocation of patent rights in human genes and genetically modified crops. In the tension field between privacy and prop-

[89] Alan Westin had already suggested the idea of treating personal information as a property. See Alan Westin, *Privacy and Freedom*, 1967.

[90] "People should own information about themselves and, as owners of property, should be entitled to control what is done with it", Jessica Litman, *Information Privacy/Information Property*, Stanford Law Review, Vol. 52, 2000.

[91] Maureen O'Sullivan, *Lockean style property rights: in land, software and genes*, in *Ethics and Health in the Global Village*, Bioethics, Globalization and Human Rights, Edited by Emilio Mordini, CIC Edizioni Internazionali

[92] It was during the 19th century that the term intellectual property began to be used. Intellectual property rights particularly refers to certain exclusive rights granted for particular creations of the human mind. The concept of *intellectual property* refer something of non tangible e non-rivalrous good that can be treated as a private property resembling them in many ways.

erty lies also the concept of publicity rights[93]. The recent debate on the propertization of personal information included many arguments in favour and against, that are taken from the economical, philosophical and legal disciplines[94]. The rhetorical value of talks on propertization has also been pointed out[95].

Vesting a property right in personal data however results totally not in line with the continental human-rights based approach to privacy and data protection[96]. The idea that the right to privacy could be property-based is completely rejected by who sees a long evolution of the relevant international legal instruments[97] in progressively separating the two rights to data protection and to privacy, and in finally granting data protection the status of an autonomous, fundamental human right. Moreover, a parallel between the art.3 of the EU Charter of Fundamental Human Rights, on the integrity of the body, and art. 8 on data protection has been pointed out[98]: as art. 3 deals with the protection of the physical body, art. 8 aims at protecting the "electronic body", and both these provisions are strongly related to art. 1 on human dignity. According to this view, in the digital age, data protection plays a critical role in supporting the more general principle of the inviolability of the person.

To conclude, data protection include many different aspects, first of all the protection of a fundamental human right, legally separated from the right to privacy, but strongly interconnected with it. The debate on the protection of personal data may include other different aspects, related to issues of individual self-determination, property of personal information, publicity and reputation. The central issue remains how it is possible to best protect personal data, increasingly challenged by both technological advance and political priorities, while satisfying government and business needs of information.

2.5 Contrasts and similarities

Privacy and data protection definitely are important: both are constitutionally embedded and many States have adopted specific legislation in order to better enforce their protection. Indeed, since the Enlightenment, the rise of the liberal democratic constitutional state and the thinking of philosophers such as John Locke and John Stuart Mill, privacy has always been entangled with a principle as crucial as individual liberty. This, however, should not obliterate the fact that privacy is a crucial aspect of the architecture of Western constitutional states as well. Therefore, it must be considered not only as an individual but also as a public good, a part of the general or public interest. As a fundamental right that warrants the political private sphere, it can be considered as one of the cornerstones of an open democracy as it is constitutive of the freedom of expression, association, conscience of choice, and is manifested in the

[93] Publicity rights refer to the right to control the commercial use of unequivocal aspects of one's identity.
[94] See Nadezda Purtova, *Property rights in personal data: learning form the American discourse*, Computer law and security review, 2009, vol. 5, n.6.
[95] "Property talk is just how we talk about matters of great importance […] If you could get people (in America, at this point of history) to see certain resource as property, then you are 90 per cent to your protective goal", Lawrence Lessig, *Privacy as Property*, Social Research: An International Quarterly of Social Sciences, Vol. 69, No. 1, 2002, pp. 247-269.
[96] The first legal conceptualization of privacy, the Warren and Brandeis's "right to be left alone", was also based on the dignitary aspect.
[97] The OECD guidelines, the CoE Convention 108, the EU Data Protection Directive and the EU Charter of Fundamental Human Rights.
[98] Stefano Rodotà, *Data Protection as Fundamental Human Right*, Keynote Speech, International CPDP Conference on "Reinventing Data Protection", Bruxelles 12-13 October 2007. Rodotà points out that "the right to data protection has to do with protecting one's personality, not one's property".

secrecy of ballots. That is the reason why both privacy and data protection can be considered as legal tools (of opacity and transparency) aimed at protecting the political private sphere. Nonetheless, and however socially important it is, privacy is not unalloyed. For example, feminists have criticised it as a veil allowing for domestic violence. It can also cover other illegal activities.

Also, it is important to remember that the legal definition of privacy is problematic: that is the reason why the ECtHR has stated that it is neither possible nor desirable to determine the content of privacy in an exhaustive way. In that sense, it favours a liberty approach. The content of the right to data protection[99] is spelled out in the different pieces of legislation that enforce it, the most important (at least at European level) of which is the EU 95/46/EC Directive. It is important to keep in mind that privacy and data protection are fundamentally intermingled, as is evidenced by the jurisprudence of the ECtHR and ECJ.

Although society considers privacy and data protection as legally enforced rights, it is being put at jeopardy by the practices of government, especially in the field of security. This wouldn't have so much importance if privacy didn't have any social value (as argued by the "privacy is dead" school). Privacy however is valuable to the society as it is instrumental in achieving responsible citizenship, diversity of speech and behaviour.

It is very difficult to quantify the value of privacy in economic terms. Privacy issues are often reduced to issues of the use of personal data for business purposes. Moreover, economic theory makes no difference between data of individuals and that of corporations. The economic understanding of privacy and data protection deals with two issues: information asymmetry and information goods. Information asymmetries relate to economic transaction where one party has more information than the other. This creates power imbalances that give rise to problems such as moral hazard or adverse selection, and privacy increases information asymmetries. Information goods mean that personal data are becoming an economic commodity and the core of new businesses (search engines, data mining, etc.). However, privacy has also a role to play in economic decision-making.

Ethics[100] teaches us that privacy is inherent to the human condition. This condition features a fundamental tension whereby humans are individualistic and social at once. They need the company of others, but only to a certain extent, after which this company becomes troublesome (cf. the hedgehog's dilemma). The solution to this dilemma is to put an optimal distance between individuals. However, the extent of this distance depends upon the periods and civilisations. Evidence from different disciplines shows the value of privacy insofar as it helps in creating a private sphere around the individual. Biology shows evidence of the value of privacy through studies on overcrowding and isolation. Overcrowding of humans can have effects upon individual performance, social behaviour and health (e.g., stress induction or pathological behaviour). Isolation, however, is counter to neoteny, a basic human need to evolve surrounded by others. Anthropology defines privacy as a "cultural universal", i.e., a concept present in every society. One of the explanations put forward is that since society is always a source of obligations (and thus a limitation of individual freedom); citizens need a socially accepted space where they can nurture their freedom without further constraints. A psychological account of privacy sees it as a realm where individuals can escape the vicissitudes of life. Similarly, political philosophy has always greatly valued privacy. Ancient Greek

[99] Endorsed by the 2000 EU Charter of Fundamental Rights.
[100] I.e., the branch of philosophy that assesses questions about morality; say about issues that can be classified as right or wrong.

democracy considered the public sphere (the *polis*) as the sphere where a man could flourish as a complete person, whereas the private sphere focused on family identity. In the liberal tradition, its value is twofold, as a shield against absolute power and as a means for citizens to engage in issues related to the common good. Nonetheless, and in spite of the fact that its ethical value is beyond doubt, the core content of the concept of privacy is extremely hard to grasp, and a comprehensive and satisfying definition of the concept is still lacking, in spite of the fact that many scholars have engaged in taxonomies of privacy.

Finally ethics also points out at challenges related to the processing related to the processing of personal data, such as the processing of so-called sensitive data, or the question of the appropriation of personal data.

3 TRADE-OFFS AND BALANCING

3.1 Balancing from a legal perspective

In the system of the ECHR (and that of all human rights instruments), the right to privacy is not absolute.[101] Interferences with this right are legitimate as long as they meet the conditions laid down in art. 8.2. Therefore, when restricting privacy and data protection (the latter insofar as data protection is also considered as a privacy issue), European states have to take into account that such restriction must be foreseen by law, respond to one of the legitimate aims listed in art. 8.2[102], be necessary in a democratic society and be proportionate to the aim pursued. From a legal perspective, the balancing of privacy against other interests is provided for *in abstracto* by the legislative framework (art. 8 ECHR), but *in concreto*, it occurs during the judicial process of weighing and pondering values within the limits and possibilities devised by this framework, in which the conditions of necessity in a democratic society and proportionality are crucial elements.

However, more generally, the methods and criteria of the proportionality test do not only vary from jurisdiction to jurisdiction, but also from case to case. Beyond the differences between the ECrtHR, the ECJ and national constitutional courts, all seem to apply the test in a strict and in a more lenient way, depending on the case. When dealing with sensitive issues where no common position can be found among the Treaty States, the ECrtHR usually recognises a "margin of appreciation" that implies a greater discretion for the States, and consequently, a lowering, if not suppression, of the proportionality threshold. Regarding security issues, it appears not only that the Court acknowledges the fight and the need to take effective measures against crime and terrorism, but also that it applies a weak version of the proportionality test or avoids it, especially when the litigation mainly concerns privacy, and not other human rights.[103] This explains why the ECrtHR requires the formal presence of

[101] For matters of convenience, we use the terms "trade-off" and "balancing" here given that they are so widely used. However, we would like to emphasise that they bear problematic conceptual implications. Indeed, undertaking a trade-off implies that one value must be upheld at the expense of the other. We contend that such an approach misses a fundamental point, that is, the challenge to "compose with" or "reconcile" the two different values at stake, which, albeit being antagonistic to some extent, are nonetheless both essential to the societies we live in. The challenge, then, is to find a way to enforce or reconcile both values, without loss in either.

[102] i.e., "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".

[103] Vries, Katja de, Rocco Bellanova, Paul De Hert, and Serge Gutwirth, "The German Constitutional Court Judgement on data retention: proportionality overrides unlimited surveillance (doesn't it ?)", in Gutwirth, Serge,

safeguards against abuses of the accepted restrictions of a fundamental right. From that perspective, the Court seems to privilege a transparency above an opacity approach (*supra*), which indeed avoids the making of substantial, normative and prohibitive choices, which explains the often observed tendency of the Court to accept the restriction and to focus on the more formal conditions of the restriction, namely its accessibility, foreseeability and safeguards against abuses.

In addition, a weak proportionality test, consisting of a mere balancing of a fundamental right and another interest – for example, privacy and crime control – does not guarantee the protection of the former, since the approach itself assumes that preserving the one per se weakens the other, and vice versa. It excludes the possibility that both interests can be fostered and protected together. Such a proportionality test is doomed to weigh one interest *against* the other, and makes impossible the search of a *composition* or *reconciliation* in which the different interests at stake are all preserved in an optimal way. Such criticisms, however, do not apply to stronger proportionality tests that include the possibility of deciding that the restrictive measures at stake are unacceptable because they harm the essence of a fundamental right or of the constitutional order, even if it can be shown that this measure can effectively realise another legitimate interest – the exercise known to the Strasbourg court as the "necessary in a democratic state" test. The issue at stake, then, is not a "balancing" between two values, but an answer to the questions "How much erosion of a fundamental right is compatible with the democratic constitutional state in which fundamental rights are a constitutive element?" or "In which society do we want to live?". Another aspect of a stronger proportionality test is indeed the obligation to explore if there are alternative measures that allow for the realisation of the legitimate interest in a way that does not affect the fundamental rights in the same way as the proposed measure. In other words, is there a way to protect and enforce both values without loss of (some measure of) the fundamental rights?

The core of the legal balancing between privacy and other legitimate interests lies in the proportionality and "necessary in a democratic society" tests. However, it appears that in many privacy cases the Court of Strasbourg puts the emphasis upon the legality test. Is it a way for the Court to avoid the value judgement inherently present in any balancing exercise, or is it a strategy to exert a tighter control when States have acknowledged a wide margin of appreciation?[104]

The balancing of data protection rights against other interests is also present in data protection legislation since it expresses the fundamental principle that the processing of personal data in the name of legitimate interests is *by default* acceptable. Indeed, article 1 of the Data Protection Directive spells out the fundamental balancing that lies at its heart: to protect the fundamental rights of citizens whilst at the same time ensuring the free flow of personal data. In the Data Protection Directive, balancing operations can be found in article 7 that formulates (in very broad terms) the "criteria for making a data processing legitimate". Indeed, articles 7 (e) and (f) of the Directive enshrine that a processing of personal data will be legitimate "if the controller pursues a legitimate aim". Furthermore, art. 7 (a) declares a processing legitimate if the data subject has given his unambiguous consent. In practice, however, free consent is hard to achieve. In the power relationship between data controllers and data subjects, the latter are almost always the weakest, and their consent is often a pure formality, as would be the case

---

Yves Poullet et al. (eds.), Privacy and data protection : an element of choice, Springer, Heidelberg/Berlin, 2011, pp. 3-23.

[104] Ibid.

when access to a good requires the disclosure of personal data.[105] Moreover, since articles 7 (e) and (f) do already justify any processing of personal data tending to the realisation of a legitimate aim of the processor, the legitimacy by consent criterion foreseen by art. 7 (a) will often, if not always, seem to be superfluous. So one may wonder if the consent criterion can supersede the legitimate aim criterion, which would perversely imply that consent could legitimise processings for "illegitimate aims", which indeed would be unacceptable.[106]

The fundamental principle of data protection is the purpose specification principle, worded in art. 6 of the Data Protection Directive, which foresees that personal data may only be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes", and that they should be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed and "accurate and, where necessary, kept up to date". Often, these two principles – the purpose specification and the data quality principles – are coined as the data minimisation principle. Even when the aims of a data processing are legitimate according to art. 7, they will only stay legitimate if the data collected and the way they are processed are meeting the needs for realising a specified purpose. In other words, if data protection law foresees that personal data may be processed for a whole range of reasons spelled out in art. 7, such processing must remain proportional, i.e., necessary, adequate, relevant and not excessive. This implies, for example, that if the specified purpose can be reached without the need to process personal data or by processing far less personal data than is the case, such a processing could still be considered as disproportionate and thus illegitimate. So, if, by default, data protection accepts that many interests and the consent of the data subject do justify the processing of personal data – which represents an implicit "balance" in favour of these other interests – such processing, nevertheless must remain proportional (and meet conditions as regards transparency, openness, accountability and the subjects' rights as mentioned in 2.1.2)

Furthermore, the Directive contains other exceptions to this default position. Art. 8 of the Data Protection Directive, as a derogation from its principle, forbids the processing of sensitive data.[107] Here, the legislative balancing turned out in another way, which is linked to the fact that processing sensitive data does not only threaten privacy, it also bears risks of discrimination and might encroach upon the freedoms of religion, conscience and expression. However, the same art. 8 provides for a series of exceptions.[108] The Directive also foresees that "subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions".[109] There is a provision for an exemption if the data subject has given his explicit consent, to which apply the same remarks as its counterpart discussed above. Art. 9 foresees exemptions for the media, so as to enable them to fulfil their journalistic mission.

[105] Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, 2002.
[106] Ibid.
[107] "Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the data concerning health or sex life".
[108] Article 8.2.
[109] Article 8.4.

3.2 Balancing from a social perspective

3.2.1 Balancing privacy against other values

Privacy has often been pitted against other social values, notably security. Policy-makers may curtail privacy for security reasons. After 9/11 and the bombings in Madrid (March 2004) and London (July 2005), policy-makers in the US, the UK, EU and elsewhere took a number of initiatives, supposedly in the interests of making our society safer against the threats of terrorism. For example, the Bush administration in the US engaged in warrantless telephone intercepts. The EU introduced the Data Retention Directive whereby electronic communications suppliers were required to retain certain phone call and e-mail information, though not the actual content, for up to two years. Many critics regarded such measures as an infringement of privacy. Our privacy was being traded off against security (or security theatre, to use Bruce Schneier's term[110]), the effectiveness of which has been called into question.

It is not just our political leaders who engage in the process of balancing privacy against other values, in this case security. Virtually all stakeholders are engaged in this balancing process, often on a daily basis. Individuals make trade-offs when they consider how much personal data they are willing to give to service providers in exchange for a service. Industry players, concerned about trust and reputation, must balance their desire to collect as much personal data of their customers as possible against the potential reaction of their customers to undue intrusion. The same media who rail against the laxity of governments and companies in not preventing data theft or loss are often engaged in reporting on the "private" lives of public figures, sometimes illegally by intercepting mobile calls.[111] Governmental officials share personal data in an effort to counter benefit fraud.

Much has been written in academic journals (and elsewhere) about the trade-offs between privacy and other social values, notably security. Bennett and Raab note that "The conception of privacy as a value to be balanced against competing values, or, indeed, balanced against more mundane 'interests', has become securely entrenched in data-protection policy and its practical implementation over the past thirty years or more."[112] So frequently does the issue of trade-offs or balancing feature in the press, in policy debates and in scholarly articles that one could characterise the social dimension of privacy that way – i.e., the issue of trade-offs or balancing not only dominates discussion in the social dimension of privacy, but is inherent to it.

The notion of balancing and trade-offs has a long history, at least as far back as the US Department of Health, Education and Welfare's report on *Records, Computers and the Right of Citizens* of 1973. That report said, "For any one individual, privacy, as a value, is not absolute or constant; its significance can vary with time, place, age, and other circumstances. There is even more variability among groups of individuals. As a social value, furthermore, privacy can easily collide with others, most notably free speech, freedom of the press, and the public's

[110] Schneier, Bruce, *Beyond Fear*, Copernicus Books, New York, 2003. See p. 38: "Some countermeasures provide the feeling of security *instead of* the reality. These are nothing more than *security theater*. They're palliative at best." [Italics in the original.] And p. 249: "Massive surveillance systems that deprive people of liberty and invade their privacy are never worth it.… Since 9/11… the security we're getting against terrorism is largely ineffective… But it comes at enormous expense, both monetarily and in loss of privacy."

[111] Marsden, Sam, "Phone 'blagging' methods exposed", Press Association, in *The Independent*, 9 July 2009. http://www.independent.co.uk/news/uk/crime/phone-blagging-methods-exposed-1739387.html

[112] Bennett and Raab, op. cit., p. 49.

'right to know.'" [113] In other words, since privacy is not an absolute value, it can "collide" with or be traded off or balanced against other values. In fact, the report also said, "there is nothing inherently unfair in trading some measure of privacy for a benefit, [but] both parties to the exchange should participate in setting the terms."[114]

Privacy experts still employ the notion of trade-offs and balancing. Helen Nissenbaum, for example, has said that privacy may sometimes be at odds with other values such as "free speech and a free press, economic efficiency and profitability, open government, and security… When these values clash with those that support restrictive treatment, we need to pursue trade-offs and balance."[115]

And even more recently, Daniel Solove also talks about balancing privacy against countervailing interests. "In some instances, privacy might outweigh the countervailing interest or vice versa... But this balancing depends upon first identifying privacy interests."[116]

Thus, we can see the notion of trade-offs, of balancing privacy against other values has a long history and continues to have currency. Even the same words "trading" and "balancing" continue to be used. The notion of balancing, of making trade-offs suggests a zero-sum game where an increase in security, for example, automatically means a reduction in privacy (and/or data protection). But is this notion still a valid concept? The answer might seem to be in the affirmative. For example, those who want to use a social network such as Facebook are arguably trading off personal data for use of the network. When government engages in mass surveillance of citizens in attempts to apprehend terrorists, they are intruding upon our privacy, i.e., balancing it (or, at least, some of it) against national security. Examples such as these abound.

This conception of balancing, understood as simply opposing two values, assumes that supporting one interest *ipso facto* weakens the other, that it is only possible to uphold one at the expense of the other. Many critical voices have been raised against this cost-benefit conception of balancing.

Jeremy Waldron argues that we need to subject "the balancing rhetoric" to careful analytic scrutiny for several reasons:

> (i) *Objections to consequentialism*. Talk of balance—particularly talk of changes in the balance as circumstances and consequences change—may not be appropriate in the realm of civil liberties. Civil liberties are associated with rights, and rights-discourse is often resolutely anti-consequentialist….
> (ii) *Difficulties with distribution*. Though we may talk of balancing our liberties against our security, we need to pay some attention to the fact that the real diminution in liberty may affect some people more than others….[J]ustice requires that we pay special attention to the distributive character of the changes that are proposed and to the possibility that the change involves, in effect, a proposal to trade off the liberties of a few against the security of the majority.

---

[113] See Section III. Safeguards for Privacy, US Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July 1973. http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm. This seminal report is noteworthy for its formulation of the so-called fair information principles.
[114] See para 4 of the section "Summary and Recommendations", HEW report, July 1973.
[115] Nissenbaum, Helen, "Privacy as contextual integrity", *Washington Law Review*, Vol. 79, No. 1, Feb 2004, pp. 119-158 [p. 151].
[116] Solove, *Understanding Privacy*, op. cit., p. 76.

> (iii) *Unintended effects*. When liberty is conceived as negative liberty, a reduction in liberty is achieved by enhancing the power of the state…. We need to consider the possibility that diminishing liberty might also diminish security against the state, even as it enhances security against terrorism.
> (iv) *Real versus symbolic consequences*…. [W]e must subject these balancing arguments to special scrutiny to see how far they are based on fair estimates of actual consequences and how far they are rooted in the felt need for reprisal, or the comforts of purely symbolic action.[117]

Equally, Chandler admits that "The need for a trade-off between privacy and security is likely true in certain contexts and with respect to certain aspects of the right to privacy," she argues that

> Framing the issue as a contest between privacy and national security tends prematurely to shut down the debate in favour of security…. the danger with prematurely permitting the needs of national security to trump competing values is that important questions may not be adequately considered. These include
> 1. Whether the contemplated security measure actually delivers any security
> 2. Whether there is a less privacy-invasive manner to achieve the same level of security
> 3. Whether the gains in security are worth the total costs of the security measure, including privacy costs and the opportunity costs of security-enhancing spending on health, education, poverty, and the environment
> 4. Whether the costs are distributed fairly so that the increased security of the majority is not purchased by sacrificing the interests of a minority.[118]

However, this is not to say that we are clueless as to what constitute a stronger, better balancing process.

There are a variety of factors that go into the decision-making process when individuals or policy-makers or other stakeholders attempt to strike a balance between privacy and those other values. Proportionality and necessity are frequently cited as factors to be taken into account. So one might ask whether a particular measure is proportionate, i.e., is the gain in security greater than the loss in privacy? Are there less privacy-intrusive ways of achieving the same increase in security? Is the measure really necessary? Will it achieve what is expected?

In striking a balance between values, one should bring necessity and proportionality into the equation, i.e., any intrusions on privacy in order to improve security should be subject to considerations of necessity and proportionality. Those who aim to improve security in a way that impacts (intrudes upon) citizens' privacy should be obliged to show that the proposed measures are needed and proportional.

Jeffrey Rosen cites a proportionality test put forward by the former Canadian privacy commissioner, George Radwanski, who proposed a "stringent four-part test that is similar to the strict scrutiny test applied by United States courts when a fundamental right is implicated. He would have the courts determine whether the invasiveness of the search is proportionate to the seriousness of the crime, the technology is empirically effective at stopping rather serious crimes, the technology is necessary or closely connected to the stoppage of serious crimes like

---

[117] Waldron, Jeremy, "Security and Liberty: The Image of Balance", *The Journal of Political Philosophy*, Vol. 11, No. 2, 2003, pp. 191-210 [194-195].
http://onlinelibrary.wiley.com/doi/10.1111/jopp.2003.11.issue-2/issuetoc

[118] Chandler, Jennifer, "Privacy versus national security: Clarifying the Trade-off", in I. Kerr, C. Lucock and V. Steeves (eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, Oxford: 2009, pp. 121-138 [p. 122].

terrorism or murder, and it is the least restrictive means of achieving the goal without unduly violating privacy."[119]

In a recent essay on "Proportionality and Principled Balancing", the legal scholar Aharon Barak advocates "the adoption of a principled balancing approach that translates the basic balancing rule into a series of principled balancing tests, taking into account the importance of the rights and the type of restriction. This approach provides better guidance to the balancer (legislator, administrator, judge), restricts wide discretion in balancing, and makes the act of balancing more transparent, more structured, and more foreseeable."[120]

With regard to proportionality, he says it "stricto sensu is a consequential test and requires an appropriate relationship between the benefit gained by the law limiting a human right and the harm caused to the right by its limitation."[121] He adds that "The evaluation of the 'goal' side of the scale should take into account the importance of the goal in view of its content, the urgency of its realization reflected in the harm that would be caused absent the restriction, and the probability of that harm." [122]

He also cautions that "One cannot eliminate value judgment in the process of balancing."[123] Thus, balancing is an inherently subjective process. Which factors go into the balancing process depends on who is making the decision and in what context. Or, as Barak puts it: "What is the proper relationship between human rights and society's interests, and when is the state justified in restricting human rights? There is no universally accepted answer to this question; rather, responses vary from society to society and from era to era."[124]

Kevin Aquilina queries how and to what extent public security interests can be balanced with the human right of privacy. He then goes on to identify certain principles and procedures that should be applied in attempting to achieve such a balance,[125] including the principles of the least privacy intrusive technology, effectiveness, accountability, transparency, proportionality, fairness, purpose specification, informed consent and legality, finality and purpose limitation, accuracy, non-retention of data beyond a certain timeframe, right of access and rectification, security safeguards, technological neutrality, anonymity, pseudonymity, unlinkability and unobservability.

Finally, just as privacy has been an elusive term of define, one should not take politicians' assurances about improving other values, such as security, at face value. Aquilina observes that "National security is… a nebulous and ambiguous term. Reasons of national security have been often used to cover-up for controversial policy decisions."[126] Furthermore, he says, "Public security should not be conceived in absolute terms and limitations should be imposed thereon to ensure that its exercise is fair, legitimate, proportionate, transparent and account-

[119] Rosen, Jeffrey, "The Naked Crowd: Balancing Privacy and Security in an Age of Terror", Isaac Marks Memorial Lecture, in *Arizona Law Review*, Vol. 46, No. 4, 2004, pp. 607-619. http://www.arizonalawreview.org/ALR2004/contentsv46.cfm

[120] Barak, Aharon, "Proportionality and Principled Balancing", *Law & Ethics of Human Rights*, Vol. 4, Issue 1, 2010, p. 2. http://www.bepress.com/lehr/

[121] Aharon, op. cit., p. 7.

[122] Aharon, op. cit., p. 12.

[123] Aharon, op. cit., p. 8.

[124] Aharon, op. cit., p. 4.

[125] Aquilina, Kevin, "Public security versus privacy in technology law: A balancing act?", *Computer Law & Security Review*, Vol. 26, No. 2, March 2010, pp. 130-143 [pp. 140-141].

[126] Aquilina, op. cit., p. 131.

able. Otherwise…, the rule of law within a democratic society might be at risk…. The scales of the balance, if no preventive measures are put in place on the State's law enforcement agencies, would tilt in favour of the creation of a police state, to the detriment of democracy. Moreover, 'public security' should be more narrowly defined with more precision in national, regional and international law whilst the threats to public security should be statutorily identified." [127]

3.2.2 Characteristics of the social context

When balancing from a social perspective, it is important to take into account several elements that are characteristic of this context and that have an influence on how to conduct the balancing.

As Waldron and Chandler indicate, the balancing paradigm is problematic to some extent. Industry and government may be content with the balancing paradigm because, when it comes to pitting individual privacy against economic interests or political drivers (the greater good of society), the individual will almost always lose, partly because privacy will be viewed as "only" an individual value, rather than as a social value, i.e., that privacy has a value to society as a whole. Enabling "free" markets or providing more security against crime and terrorism will usually trump individual privacy. Thus, the balancing paradigm serves law enforcement authorities, intelligence agencies and industry, even if occasionally a court may rule against them or public opinion is sufficiently strongly opposed to an action that its pursuit becomes untenable.

Indeed, Chandler goes on to identify several reasons why, in her view, security is so powerful, and why it seems fairly easily to trump competing values such as privacy.

> The reasons suggested for security's rhetorical power are first that security in the sense of physical survival is a prerequisite for the enjoyment of other values such as privacy. Second, human risk perception may be subject to cognitive biases that cause us to overestimate the risk of terrorism and to have difficulty perceiving the harm of reduced privacy. Third, we are apt to think that it is better to have more rather than less security, while this is not true for privacy. Fourth, to the extent that national security is obtained at the expense of the privacy of a minority, the majority is more likely not to perceive or care about the privacy costs and thus will regard the security measures as reasonable. Fifth, social-psychological reactions of solidarity following an external attack may cause people to be more willing to set aside individual rights claims such as privacy for a perceived collective benefit in terms of national security. Finally, judges tend to defer to governments on matters of national security. [128]

She adds other reasons too why security may trump privacy. "Privacy is an inherently limited value, while security is not. As a result, we are more likely to always want more security, but unlikely to feel the same way about privacy." [129] Another reason: "Security improvement is sometimes bought at the expense of a minority. To the extent that this is true, the majority will either fail to perceive the costs of that security or they will not care sufficiently."[130] In addition, in the aftermath of terrorist attacks, "The surge of patriotism and the desire for social

[127] Aquilina, op. cit., p. 142.
[128] Chandler, op. cit., pp. 125-126.
[129] Chandler, op. cit., p. 128.
[130] Chandler, op. cit., p. 129.

unity may contribute to the willingness with which people sacrifice individual liberties for a perceived collective security improvement." [131]

When the greater good of society prevails against an individual right, some critics might say that it is an instance of the tyranny of the majority, something that John Stuart Mill cautioned against.[132] More recently, social philosopher Ronald Dworkin showed his distaste for the tyranny of the majority and the notion of balancing human rights.

> The balancing metaphor is dangerous [and]… deeply misleading because it assumes that we should decide which human rights to recognise through a kind of cost-benefit analysis, the way we might decide what speed limits to adopt. It suggests that the test should be the benefit to the British public, as Blair declared in his 'Let's talk' speech, when he said that 'the demands of the majority of the law-abiding community have to take precedence'. This amazing statement undermines the whole point of recognising human rights; it is tantamount to declaring that there are no such things… The 20th-century tyrannies have taught us that protecting the dignity of human beings, one by one, is worth the increased discomfort and risk that respecting human rights may cost the public at large.[133]

Thus, for Dworkin, the balancing paradigm is dangerous because one cannot apply a cost-benefit analysis to a fundamental right, that do so is to succumb to the tyranny of the majority.

For some scholars, such as Bennett and Raab, the concept of trade-offs, of achieving a balance is

> problematic both as a verb and a noun (Raab 1999a). It does not discriminate between divergent conceptions of what it means, in practice, *to balance*, nor does it provide criteria for judging when a balance has been achieved. It is therefore not very informative to hear that "a balance must be struck between privacy and the public interest," or that "we have found the right balance" between the one and the other. Different people may go about finding a balance in different ways, and arrive at different substantive points of reconciliation between competing values…. Although the concept is related to the terminology of judicial decision, the achievement of a balance may ultimately be a matter of political negotiation, perhaps arriving at a consensus; or, alternatively, of authoritative assertion.[134]

The Bennett/Raab book refers to an earlier work written by Charles Raab in 1999. In that earlier work, he admitted that "the doctrine of balancing" is likely to remain at the centre of privacy policy for a long time to come, but said he regarded balancing as "an inadequate normative conception" [135], especially because

> Yesterday's balance might not be today's; what is acceptable in one country might not do in another. Data users and data subjects might disagree strongly on whether a particular compromise constitutes a balance between their points of view. Technological change often ren-

[131] Chandler, op. cit., p. 131.
[132] "'The tyranny of the majority' is now generally included among the evils against which society requires to be on its guard." Mill, John Stuart, *On Liberty*, in *On Liberty and Other Essays*, Digiread.com Publishing, 2010 [originally published in 1859], p. 7.
[133] Dworkin, Ronald, "It is absurd to calculate human rights according to a cost-benefit analysis", *The Guardian*, 24 May 2006. http://www.guardian.co.uk/commentisfree/2006/may/24/comment.politics
[134] Bennett and Raab, p. 13.
[135] Raab, Charles D., "From Balancing to Steering: New Directions for Data Protection", in Colin J. Bennett and Rebecca Grant (eds.), *Visions of Privacy: Policy Choices for the Digital Age*, University of Toronto Press, 1999, pp. 68-93 [p. 69].

> ders old balances obsolete. Moreover, there may be many different points of view to be taken into the balance on each issue, not just two…[136]
>
> If 'balancing' is taken literally, it would mean that there is some way of ascertaining whether parity exists between the items being weighed. But there is no ready reckoner for this; it is a matter of judgment, but that judgment may well be open to dispute about the weights that were deemed to attach to the competing claims, or about other considerations that were overlooked. [137]

Raab advocates a somewhat different conception, one that does not reject balancing as such but goes beyond it. Although "steering" was mainly implicit in the balancing modes, a revised paradigm would emphasise it as the essential part of a decision-making process in which balancing is an instrument to be manipulated, rather than an outcome to be sought.[138]

He concludes that "Some combination of regulation and self-regulation, along with better public education and the availability of privacy-enhancing technologies may succeed in steering towards privacy protection. This is not to reject the idea of 'balance' as such, but to find more sophisticated conceptualisations of its role and to embody it in more subtle and creative ways that match the dynamic growth of the 'information age' with dynamic modes of privacy protection that leave bureaucratic limits to intervention behind."[139]

While Raab's proposals are interesting and welcome, they do not solve the problem of "balancing" for many stakeholders in situations that do not involve regulatory intervention. A regulator may be able to "steer" solutions to those that are protective of privacy, but they do not solve the issue for many other stakeholders, including the public, who are confronted between choices that involve giving up some privacy or personal data in exchange, for example, for use of software or services on the Internet or transport operators who must decide whether to install CCTV cameras on trains or governments who favour biometric passports.
In any event, it is important to note that Raab's criticism is not directed at the concept of balancing as such, but rather, at the way it is enforced in the social context. Hence, it is in the light of such a position that his remarks for creating a stronger and better-equipped balancing process must be understood.

3.3 Balancing from an economic perspective

From an economic point of view, there are mainly two relevant actors. The data subject has to choose between disclosing or protecting personal data, whereas the data controller is interested in collecting, storing and exploiting this data.[140] Both face a complex cost-benefit ratio, which is explored further below.

---

[136] Raab, ibid., p. 73.
[137] Raab, ibid., p. 77.
[138] Raab, ibid., p. 83.
[139] Raab, ibid., pp. 88-89.
[140] The EU data protection directive defines the data subject as "an identified or identifiable natural person", whereas the data controller is referred to as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data". Cf.: Article 2 (a) and (d) of the Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995, pp. 0031 – 0050.

3.3.1 Costs and benefits from the data subject's point of view

Costs created by disclosing personal data are extremely hard to quantify empirically, because they are at the core of exactly that essence and complex value of privacy, which is a fundamental part of the essentially contested concept of privacy itself. Frequently, individuals value costs differently. Privacy incidents often do have indirect and long-term effects on the data subject.[141] Consequences are hard to anticipate and it seems that individuals perceive long-term impacts as a rather indirect, controllable and less perilous harm to themselves. That's why the data subject often underestimates or does not consider the long-term risks in giving away personal information.[142]

However, more and more individuals are confronted with privacy problems frequently resulting from their lax attitude towards sharing private information or being forced to disclose personal data. This can result in social sorting or other discriminatory practices by data controllers. There is furthermore an increasing risk of being the victim of online and offline crime such as burglary,[143] identity theft, cyber stalking and bullying, character assassination as well as other forms of harassment.

Another cost factor of sharing voluntarily personal and private data such as photographs may arise when peers, colleagues or prospective employers form an opinion about the data subject based on a one-time superficial and maybe misleading impression. The consequences can go from mere embarrassment to the failure of a job interview. Feeling annoyed by unsolicited advertisement, but also being uncomfortable with ads that reflect too much knowledge about themselves, Internet users suffer more often than expected from the aftermath of continuously disclosing personal and private information.

In many instances, however, they are actually able to choose between disclosing or retaining personal data. Nonetheless, individuals tend to decide in favour of short-term and tangible benefits although being aware that there is a value to privacy. The research of Acquisti and Berendt deals with exactly this gap of stated preferences, i.e., the (partial) awareness of the consequences of giving away personal information and actual behaviour.[144] Lack of information and transparency about the commercial or governmental usage of personal data often eases the individual's decision to disclose personal data.[145]

---

[141] The data subject's perception of these effects heavily depends on the information he/she receives and on previous experiences with privacy intrusions, the latter being called the "life cycle element". See Laufer, Robert S., and Maxine Wolfe, "Privacy as a Concept and a Social Issue: A Multidimensional Development Theory", *Journal of Social Issues*, Vol. 33, No. 3, 1997, pp. 22-42 [pp. 31-32].

[142] Acquisti, A., and J. Grossklags, "Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting", in J. Camp. and R. Lewis, *The Economics of Information Security*, Kluwer, Amsterdam, 2004, pp. 165-186 [p. 11].

[143] The Dutch website PleaseRobMe.com highlights the dangers of sharing too much information on the Internet about your locations. Cf.: Harvey, Mike, "PleaseRobMe website highlights dangers of telling world your location", *The Times*, 19 Feb 2010.
http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7032820.ece.

[144] Acquisti, A., and J. Grossklags, "Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting", in J. Camp and R. Lewis (eds.), *The Economics of Information Security*, Kluwer, Amsterdam, 2004; pp. 165-186; Berendt, B., O. Günther and S. Spiekermann, "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior", *Communication of the ACM*, Vol. 48, No. 3, 2005, pp. 101-106.

[145] Grimmelmann, James, "Privacy as Product Safety", *Widener Law Journal*, No. 19, 2010, pp. 793-827. [p.802]. http://works.bepress.com/cgi/viewcontent.cgi?article=1026&context=james_grimmelmann

Convenience is one of the most important drivers for disclosing personal data.[146] Data controllers offer a plethora of supposed advantages and seemingly free services to the data subject in order to get his personal data. Acquisti characterises the benefits of disclosing personal information as relatively small and short-term rewards.[147] These include direct and indirect monetary incentives such as little gifts or discounts on products in exchange for the customer's personal data. All of these price deductions such as student, senior citizen and even volume discounts are part of a positive price discrimination strategy. But there are also immaterial rewards which can involve social benefits, e.g., when the data subject tries to avoid peer-group pressure (particularly in social networks) by willingly sharing private information.

Furthermore, Lenard and Rubin argue that the very existence of the Internet as we know it today with a myriad of seemingly free services such as search engines, e-mail accounts, social networks, news, etc., depend heavily on consumers' willingness to disclose personal information.[148] Taking these offers for granted, users underestimate the cost-benefit rationality that underlies the business models of many providers. The trade-off between exchanging personal data and services mostly free of charge is based on an asymmetric allocation of information. Not knowing that their personal data is collected and processed, users are often deluded concerning their reasonable expectation. Since knowledge and education about the economic value of personal data plays a decisive role, a new form of digital divide, perhaps a "privacy divide", threatens to develop in society and the long-term need of a privacy e-inclusion of citizens could come into existence.[149]

Nevertheless, from an economic point of view, the increasing demand for privacy and data protection foster the supply and development of new technologies, laws and entrepreneurial codes of conduct as well as new business models which offer new strategies to deal with privacy issues. It must be admitted, however, that there is little empirical evidence for a strong demand response.

In retaining personal information, the data subject bears, of course, the costs of not receiving the benefits for disclosing his/her personal data. In this case, he/she is also part of a negative price discrimination not belonging to the group of preferred customers that enjoys discounts.

Since data protection implies the holding back of certain information, individuals who are reluctant to disclose personal data could be suspected of being loners, freaks or weirdos who have something to hide. In fact, the question why people would need privacy if they have nothing (bizarre or illegal) to hide is one of the classical arguments of data controllers trying

---

[146] Grossklags, J., and A. Acquisti, "When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information", Sixth Workshop on the Economics of Information Security (WEIS 2007), Pittsburgh, PA, 2007, pp 1-22 [p.4].

[147] Acquisti, A., and J. Grossklags, "Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting", in J. Camp and R. Lewis (eds.), *The Economics of Information Security*, Kluwer, Amsterdam, 2004.

[148] Lenard, Thomas M., and Paul H. Rubin, "In Defense of Data: Information and the Costs of Privacy", *Policy & Internet*, Vol. 2, Issue 1, Article 7, 2010, pp. 149-183 [p. 163].
http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf.

[149] Roussopoulos, Mema, Laurent Beslay, Caspar Bowden et al., "Technology-Induced Challenges in Privacy and Data Protection in Europe", A Report by the ENISA Ad Hoc Working Group on Privacy and Technology, Oct. 2008, p. 16.

to camouflage their gain in power and profit by collecting information.[150] Here the classical but wrong statement "If you have nothing to hide…" becomes relevant.[151]

However, communicating, exchanging opinions or sharing information represents an essential part of human behaviour and an important strategy to succeed in society. If you want to pursue a successful career in any field of work, networking belongs to one of the most relevant activities. That is why holding back information at a certain point could be disadvantageous. In the online world, most social networks try to meet this demand of being easily, all the time and everywhere connected. Although most social interactions still take place in the offline world, a trend towards more and more virtual interactions is apparent, especially among young people. Not sharing digital information could therefore lead to an isolation problem which may become even more serious in the future.

As already pointed out, the relevant literature does not specifically identify the economic advantages of maintaining informational privacy for the individual, because the concept of privacy does not generate easily quantifiable factors. Hence, difficult-to-quantify, privacy aspects are often excluded from the analysis.[152]

Nonetheless, what can be seen as a benefit is that privacy serves as a defensive right against intrusions by others as well as a positive right enabling the data subject to exercise control over his/her information. Westin names four functions of privacy:[153]

- First of all, there is personal autonomy, providing the individual with a core sphere where he/she is able to retreat not being controlled, manipulated or dominated by others.
- Second, privacy serves as a safety valve which enables the individual to release his/her emotions not having to fear any embarrassment.
- Third, self-evaluation and reflection can be carried out undisturbed in the private realm in order to develop one's personality and initiate learning processes. Additionally, innovative and creative thinking is spawned so that societies can continue to advance allowing their citizens to explore beyond the mainstream.
- Finally, limited and protected communication leads to an unrestrained exchange of information supporting the right to free speech.

Again, it is obvious that these abstract, highly immaterial and long-term benefits for the individual are difficult to operationalise and quantify. However, they represent a crucial element in our analysis of the costs and benefits of privacy.

[150] In an interview on the CNBC documentary "Inside the Mind of Google" in December 2009 Eric Schmidt, CEO of Google, was asked: "People are treating Google like their most trusted friend. Should they be?" Hitting the nail on the head, he responded: "I think judgment matters. If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time, and it's important, for example, that we are all subject in the United States to the Patriot Act. It is possible that that information could be made available to the authorities." http://www.youtube.com/watch?v=A6e7wfDHzew

[151] Solove, Daniel J., "'I've got nothing to hide' and Other Misunderstandings of Privacy", *San Diego Law Review*, Vol. 44, 2008, pp. 745-772.

[152] Swire, Peter P., "Efficient Confidentiality for Privacy, Security, and Confidential Business Information", Brookings-Wharton Papers on Financial Services, 2003, pp. 273-310.

[153] Westin, Alan, *Privacy and Freedom*, Atheneum, New York, 1967, p. 32.

3.3.2 Costs and benefits from the data controller's point of view

In gathering, storing and exploiting personal data, data controllers are confronted with various costs and benefits, too. Material and personnel costs of collecting, aggregating, storing and processing data are the most important direct expense factors. Although the software and hardware costs of gathering, processing and storing data are constantly decreasing due to technological progress, the amount of data that is being stored and processed is skyrocketing so that data collecting companies face rapidly rising operating costs (e.g., for electric power supply). For this reason, data centres are built close to power plants or in cooler climates.[154] The energy issue becomes a more and more relevant topic, also because there is an apparent tendency towards retention of data, i.e., to collect more data than is actually needed. This increases, additionally, the risk of over-investment.[155]

Especially when one considers private data as a commodity that can be exploited by its owner, property rights should be taken into account as an indirect cost factor.[156] Confronted, moreover, with a complex body of rules and regulations concerning the collection, storage and usage of personal data, data controllers try to comply (at least, to some degree) with these rules to avoid lawsuits and compensation payments. Extra administrative and infrastructural expenses should, therefore, be factored into the cost equation.

Information security represents one of these additional infrastructural cost factors. When storing personal data, most companies are obliged by law to protect the data through technical means (e.g., encryption) and access control measures. Moreover, back-ups and log files which show who accessed which data serve as another safeguard. Staff at all levels have to be trained how to use and manage data in a lawful way. If a company wishes to transfer data to a country outside the EU, there are serious regulatory hurdles to cross, not least of which is ensuring that the data will be adequately protected and respected to the same extent as in the European Union.

In addition, a company may need to respond to requests for access to their data by customers arguing that the data is not correct. The company will need to verify whether the data is correct or not. And when the data is compromised in some way, e.g., through data breaches caused by a hacker attack, or when data is lost, then the data controller will many material and immaterial costs.

Data and privacy breaches can have devastating consequences for data controllers. Immediate costs include the repair or replacement of the broken system while slowing down or even stopping whole business processes.[157] If mandatory, data subjects have to be notified of the data breach, there is negative publicity, which may seriously damage the image and reputation of the data controller. Data protection authorities may require an inspection or audits, and eventually legal actions such as fines, compensations, torts or other liabilities could account for severe financial consequences.

---

[154] Harizopoulos, Stavros, Mehul A. Shah, Justin Meza and Parthasarathy Ranganathan, "Energy Efficiency: The New Holy Grail of Data Management Systems Research", 4th Biennial Conference on Innovative Data Systems Research (CIDR), January 4-7, 2009, Asilomar, California, USA.

[155] Hui, K.-L., and I.P.L. Png, "The Economics of Privacy", in Terrence Hendershott (ed.), *Economics and Information Systems,* Elsevier (Handbooks in Information Systems), Amsterdam, 2006, pp. 471-498 [p. 474].

[156] Volkman, R., "Privacy as life, liberty, property", *Ethics and Information Technology*, Vol. 5, No. 4, 2003, pp. 199-210.

[157] Tsiakis, T., and G. Stephanides, "The economic approach of information security", *Computers & Security*, Vol. 24, No. 2, 2005, pp. 105-108 [p. 106].

Acquisti, Friedman and Telang have shown in their study that companies that experienced a privacy breach not only have to fear the loss of existing customers, but also suffer a statistically significant negative impact on the firm's stock exchange value.[158] (However, surprisingly, they found that share values tend to recover in a rather short period of time.) Ultimately, privacy and data breaches can result in long-term damages for enterprises such as higher insurance premiums, severance of contractual relations and, most importantly, an eventual harm to trust relationships with customers and/or suppliers.

Thus, data controllers need to assess their security investment in relation to the probability of a privacy incident multiplied by the impact the problem will cause. Such a risk assessment is necessary in order to keep the right balance between an adequate level of data protection and an efficient and effective processing of the data.[159] When sanctions are unlikely or the costs of compensations do not surpass the financial benefits resulting from the collection and usage of personal data, data controllers will tacitly accept these incidents and prefer to neglect privacy and data protections measures.

Trying to exploit personal data commercially, companies aim to understand the mechanisms behind individual purchase behaviour in order to increase their profits from better market opportunities. To sell products and services, suppliers need to comprehend what their customers want or need, to stimulate the buyer's interest in their products or services and to be reasonably sure what a consumer (or different groups of customers) is willing to pay for the product or service. For this purpose, many market players have been aggregating data and profiling their customers, regardless of whether personal or non-personal, for a long time. Moreover, enterprises have collected even more data in the field of production and logistics succeeding in making the supply chain more efficient.

This general aim prevails in an age where the collection of more and more data becomes feasible and affordable due to the ever-decreasing costs for sensors, storage and computing power. The data comes from traditional sources such as loyalty cards and data trails on the Internet[160], but increasingly also from other sources such as RFID-tagged products or deep packet inspection.[161]

In selling personal data to third parties, companies run, of course, the risk of losing money if the added sales revenue is smaller than the benefits of providing services based on processing the personal data on their own.

---

[158] Acquisti, A., A. Friedman and R. Telang, "Is there a cost to Privacy Breaches? An Event Story", The Fifth Workshop on the Economics of Information Security (WEIS 2006), Cambridge UK, 2006, pp. 1563-1580 [p. 1573].

[159] Sonnenreich, W., J. Albanese and B. Stout, "Return on security investment (ROSI) - A practical quantitative model", *Journal of Research and Practice in Information Technology*, Vol. 38, No. 1, 2006, pp. 45-56; Anderson, Ross, and Tyler Moore, "The Economics of Information Security", *Science*, Vol. 314, No. 5799, 2006, pp. 610 - 613. http://www.sciencemag.org/content/314/5799/610.abstract

[160] Graeff, Timothy R., and Susan Harmon, "Collecting and using personal data: consumers' awareness and concerns", *Journal of Consumer Marketing*, Vol. 19, No. 4, 2002, pp. 302-318.

[161] Deep packet inspection is, as its name suggests, a form of inspecting, filtering or examining computer network packets, the data they carry and/or the header part of a packet. The packet can be inspected for viruses, spam, tampering, denial-of-service attacks or other criteria to decide if the packet passes inspection and can be sent on to its destination or if it needs to be routed to a different destination. Deep packet inspection can be used in support of different functions or applications including security, data mining, eavesdropping, censorship, anti-piracy – and targeted advertising. A packet can then be redirected, tagged, blocked or reported to some other agent in the network. See Bendrath, R., and M. Mueller, "The End of the Net as we know it? Deep Packet Inspection and Internet Governance", 2010. http://ssrn.com/abstract=1653259.

Numerous companies have founded their business model on the processing of personal data, creating consumer profiles and exploiting the results of their data analyses in order to make a huge profit.[162] Offering seemingly free services such as Internet searches, e-mails, news, games or social interaction, many Internet enterprises are part of an already huge and still rapidly growing online advertising industry.[163]

3.4 Balancing from an ethical perspective

Privacy is the result of a negotiation between the public and the private spheres, which both encompass other individual rights and social values, duties and obligations. This negotiation is influenced both by personal attitudes (subjectivity) and by social and cultural norms, that determine what, in a given context and a given historical period, has to be protected as inherently personal, and what can be seen as a public matter. In this section, we discuss from a philosophical perspective the trade-off model between privacy and other values and rights, such as security, public good, transparency and freedom of speech.

3.4.1 The birth of the trade-off model: balancing privacy vs. public good

The concept of the public has always been privileged as an idea with respect to the concept of the private, at least since the classical period in ancient Greece, where the public realm of the *polis* was the sphere were a man could flourish as a complete person, while the realm of the private, the *oikos* (household), was the focus of the family identity (persons and properties).

The protection of the private from the intrusions of the public was conceptualised by liberal thought in the 18th century. The need to balance powers in society has led liberal thinkers to emphasise the distinction between private and public spheres. In his *Second Treatise on Government* (1690), John Locke argues that in the state of nature all property is held in common by all, and no person has exclusive rights. Each person has a right to his own person, a right to self-preservation and a right to extend his property rights through labour. Those who voluntarily and mutually consent to form a political society and government, thereby use public means to assure protection of their private ends, namely, the protection of life, liberty and property in the broadest sense. In this way, Locke balanced needs and obligations of the public and the private realms.

Liberal theories posed the serious problem of how it is possible to reconcile the two sides of man's nature, the selfish, ambitious, competitive side, and the social, co-operative, creative and loving side. This problem, which has also important implications on the concept of private sphere, was central to 18th century thinkers. At the two extreme poles, Bernard Mandeville's *Fable of the Bees* (1714) and Adam Smith's *Theory of Moral Sentiments* (1759) provided the necessary theory to reconcile private vice and public virtue.

3.4.2 Simmel's group theories: balancing public and private secrecy

The seminal analysis of the German sociologist George Simmel (1858 –1918) about the conflict between individual and society, and his discussion of group geometry, are paramount to frame the public vs. private debate. According to Simmel, there is a direct relation between

[162] Hildebrandt, Mireille, and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008.
[163] Evans, David, "The Online Advertising Industry: Economics, Evolution, and Privacy", *Journal of Economic Perspectives*, Vol. 23, No. 3, Summer 2009, pp. 37–60.

the degree of autonomy of the individual and the dimension of the group itself, which corresponds to increasingly impersonal and distant relations among members of the group. Simmel suggests that the less the group is intrusive, the less it also provides the individual with the necessary "warmth". This leads Simmel to theorise the unavoidability of secrets in groups, and their foremost importance in building human communities. "The secret," writes Simmel, "produces an immense enlargement of life: numerous contents of life cannot even emerge in the presence of full publicity. The secret offers, so to speak, the possibility of a second world alongside the manifest world; and the latter is decisively influenced by the former."[164] These words about secrets could be easily enlarged to include the notion of privacy, as

> the secret is a form which constantly receives and releases contents; what originally was manifest becomes secret, and what once was hidden, later sheds its concealment. One could, therefore, entertain the paradoxical idea that under otherwise identical circumstances, human collective life requires a certain measure of secrecy which merely changes its topics: while leaving one of them, social life seizes upon another, and in all this alternation it preserves an unchanged quantity of secrecy….It seems as if, with growing cultural expediency, general affairs become ever more public, and individual affairs even more secret.[165]

Although in contemporary society, public affairs are very often secret, while individual affairs tend to be more and more public, Simmel's intuition about a zero sum quantity of secrecy that each given human society tends to express by balancing public and private secrecy is still challenging and thought-provoking.

3.4.3 Contemporary models of privacy

During the 1990s and 2000s, the debate on privacy has evolved in order to address the challenges raised by the emergence of new technologies, as well as by the security needs of the post-9/11 world. For the most part, philosophical and legal theorisation about privacy has operated within the liberal paradigm based on the traditional trade-off balancing model. Some authors have also considered the social value of privacy[166], pointing out that privacy issues are related to power relationships between people and institutions. Many scholars have argued that privacy rights can be detrimental to societal needs.[167] Other scholars have warned against the potential for privacy to act as a protector of harmful behaviour: this is the case of the feminist critique[168], which worried about the "darker side" of privacy, which has regarded privacy as a cover for sexual harassment and domestic violence. More recently, privacy has been defined in terms of "contextual integrity"[169], meaning with this expression that several variables, including the nature of the situation and the nature of the information in relation to that context, need to be taken into account in understanding, if not defining, privacy. The notion of privacy as contextual integrity helps to solve some practical problems, yet from a more

---

[164] Simmel, Georg, "The Sociology of Secrecy and of the Secret Societies", *American Journal of Sociology*, Vol. 11, 1906, pp. 441-498 [p. 462]; Simmel, Georg, *The Sociology of Georg Simmel,* Compiled and translated by Kurt Wolff, Free Press, Glencoe, IL, 1950, p. 330.
[165] Ibid., p.468.
[166] Solove, Daniel J., "Conceptualizing Privacy", *California Law Review*, Vol. 90, No. 4, 2002, pp. 1087-1155.
[167] As exemplified in Posner, R.A., "The Right to Privacy", *Georgia Law Review*, Vol. 12, 1978, pp. 393-422 (which criticises privacy rights from an economic perspective) and Etienne, A., *The Limits of Privacy*, Basic Books, New York, 1999 (which criticises privacy rights from a communitarian perspective).
[168] See MacKinnon, Catherine, *Toward a Feminist Theory of the State*, Harvard University Press, Cambridge, MA, 1989.
[169] Nissenbaum, Helen, "Privacy as contextual integrity", *Washington Law Review*, Vol. 79, No.1, Feb 2004, pp. 101-139. http://www.nyu.edu/projects/nissenbaum/main_cv.html

.

theoretical point of view, it is hardly a novelty, and it does not solve most political and philosophical controversies related to the notion of privacy. The notion of "contextual integrity", for instance, refers to an understanding of each context that is not at all neutral and objective. It is apparent that when actors disagree about what a given context entails in terms of privacy rights and distribution of information, the theory encounters difficulty.

To conclude, from the foregoing ethical consideration, we can see that privacy is the result of a negotiation between the public and the private spheres, that both encompass other values and obligations, and both can be seen from point of view of the individual and society. While the trade-off model seems to be alive and well, it is not a simple model and other factors, such as contextual integrity, can be considered, although they too may pose problems.

3.5 Contrasts and similarities in the balancing process

From a legal point of view, balancing data protection and privacy against other interests is at work in two dynamics. The first one is within the legislation (the Data Protection Directive) itself, the goal of which is to ensure both respect for fundamental freedoms (and in particular privacy) and the free flow of personal data. The other dynamic is within art. 8.2 of the ECHR, which foresees the conditions for lawful interferences with the right to privacy. The second one is within the jurisprudence, since courts (and especially the ECtHR) have to sort out conflicts between privacy and other interests.

Some of the provisions of the Data Protection Directive are quite stringent in terms of the protection of the data subjects, such as the prohibition to process so-called sensitive data or the legitimacy principle. However, they are strongly mitigated by co-existing provisions (e.g., that on consent) and long ranging lists of exceptions. The permissive nature of this legislation may lie within its nature as a transparency tool.

For an interference to be lawful, three conditions must be met. A restriction of privacy needs to be foreseen by the law, pursue a legitimate aim and be necessary in a democratic society (that is, it must respond to a pressing social need and be proportionate). The "necessary in a democratic society" condition is the *locus* where the real value choice is made. However, there is a "procedural" tendency from the Court, which tends to include more and more issues of proportionality within the "legality" requirement, partially because of a reluctance to make these hard political choices, but also in order to perform a broader control when States are granted a wide margin of appreciation.

The social perspective is critical towards blunt, cost-benefit analysis. Instead, it argues for a substantial, valued-loaded balancing. However, as such a balancing takes place within a social context, it is important that the issues at hand are fairly framed so that the actors can make enlightened decisions.

From an economic point of view, two perspectives need to be taken into account: that of the data subject and that of the data controller. Whereas the data subject faces the choice of retaining or disclosing his personal information, the data controller is solely interested in collecting and using this data. Nonetheless, all these choices have associated costs and benefits.

The costs attached to the disclosure of personal information entail discriminatory practices by data controllers, being victim of crimes such as fraud or identity theft, unsolicited advertise-

ment, or the possibility for employers, colleagues or peers to know more than what one would like them to know.

There are many short-term benefits such as positive price discrimination strategies (discounts, free gifts), social benefits and seemingly free services (e.g., e-mail accounts, etc.).

Retaining personal information (in addition to the loss of the benefits associated with the disclosure) may lead to some form of social and professional isolation and exclusion. The benefits are hard to quantify but certainly include the control over personal information.

When data controllers process personal information, they face material costs (e.g., power supplies, staff), and possible violations of property rights. Information security represents costs in terms of infrastructure and business (in case of breach).

The benefits lie in the possibility to better understand consumers' purchasing behaviours and thus to increase market shares.

An ethical perspective enables us to understand the rationale underpinning the trade-off model. Privacy is the result of a negotiation between the public and the private spheres that both encompass different values and obligations. The result of this negotiation is influenced by human subjectivity and by the social values and norms existing at different points in history. The trade-off model we still use today dates back to the 18th century. In this model, privacy refers to the spheres of family and of individual interests, as opposed to the political sphere, that where the common good is discussed. The trade-off model exists for two reasons: to create a shield against absolute power (private sphere), and to create a place where citizens devote their energy to the public good (public sphere). This political model of privacy is echoed by Simmel's sociological understanding of privacy, through his analysis of the conflict between individuals and groups (and, to a larger extent, society). Individuals need a close group for the "warmth" it brings them, but they equally need to shield themselves from it in order to preserve their autonomy. In group situations, this is achieved with secrets. In societies, privacy plays an analogue role to that of secrets in groups. Globalisation, international terrorism and crime, the decline of the nation State and technological development pose a number of threats and challenges to the trade-off model. Both privacy and this model are in need of new conceptualisations.

4 CHALLENGES OF EMERGING AND FUTURE TECHNOLOGIES AND APPLICATIONS

4.1 Megatrends and how technology is impacting privacy

Privacy has been an issue of interest in the legal sphere for a long time. It has become of increasing interest more generally with the advent of new technologies. This is leading privacy back to its original roots, the relation between the citizen and the *polis*. Technologies such as biometrics, RFID, smart surveillance systems, body implants, nano devices and the like raise new issues, new contexts and prompt consideration of new concepts. Privacy issues can arise wherever (potentially) personal information is collected and processed.

This can take place on a micro-level which is related to the trend towards tinier, ever more powerful and lightweight sensors that are able to measure any kind of physical values and transmit them either over the Internet to centralised data centres or locally to other nearby

computers.[170] With powerful processing techniques, it is becoming increasingly possible to capture values that cannot yet be measured directly. This concerns most notably psychological properties and conditions. Brain-wave reading is an important long-term goal of neuroscience.[171]

The second trends towards the collection and processing of potentially personal information takes place at the regional and national level with the establishment of databases, their linkages and the capability to process large amounts of data in reasonable time to extract certain patterns, discover knowledge and construct profiles from them. This is the basis of emerging business services in marketing (customer analytics), psephology, mass surveillance (especially in the fight against organised crime and terror).[172]

The third trend challenging privacy is the build-up of global information infrastructures beyond the Internet. This includes positioning technologies, their various applications (ranging from location-based services to traffic control system) and supply-chain oriented systems (such as the RFID-based EPCglobal architecture).[173] Even after years of discussion about privacy issues, the Internet still generates new privacy challenges, for example, from deep packet inspection and the design of a new architecture for the "Future Internet".[174]

These technologies have specific features that make them quite different from traditional industrial technologies. Compared to technologies that drove the industrial revolution, emerging technologies are lighter, decentred, dispersed, and their control and use are largely in the hands of the individuals, citizen groups and small enterprises as well as industry. In addition, they help to reduce the complexity of human (social, biological, political, etc.) interactions and allow the individual to distance himself from his observation.[175]

In the following pages, we consider three developments involving existing and emerging technologies that raise ethical, social and other issues.

4.1.1 The Information Society

There is a great ongoing public debate on how emerging technologies[176] are modifying the values of the contemporary society. Emerging technologies are a vast range of technologies

[170] International Telecommunication Union (ITU), "Ubiquitous Sensor Networks (USN)", ITU-T Technology Watch Briefing Report Series 4, ITU, Geneva, 2008. http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000040001PDFE.pdfI

[171] Kerr, Ian R., Max Binnie and Cynthia Aoki, "Tessling on My Brain: The Future of Lie Detection and Brain Privacy in the Criminal Justice System", *Canadian Journal of Criminology and Criminal Justice*, Vol. 50, No. 3, 2008, pp. 367-388.

[172] Baker, Stephen, *The Numerati: In Which They'll Get My Number and Yours*, Houghton Mufflin, New York, 2008.

[173] Iqbal, Mohammad Usman, and Samsung Lim, "Privacy Implications of Automated GPS Tracking and Profiling", *IEEE Technology and Society*, Vol. 29, No. 2, 2010, pp. 39-46.

[174] Bendrath, Ralf, and Milton Mueller, "The End of the Net as we know it? Deep Packet Inspection and Internet Governance", Paper presented at: Annual Meeting of the American Political Science Association, Washington, D.C., 2-5 September 2010, 2010. http://ssrn.com/abstract=1653259. van Rooy, Dirk, and Jacques Bus, "Trust and privacy in the future internet—a research perspective", *Identity in the Information Society*, Vol. 3, No. 2010, pp. 397–404.

[175] Virilio, Paul, *The Art of the Motor*, University of Minnesota Press, London, 1995.

[176] According to the EU understanding, "current" technologies are those which are mature or are in a deployment phase, "emerging" are those technologies that are in a pre-marketing phase and are expected to be deployed

and processes, progressively developing with fast advances and innovations in various social and economic fields of research, such as energy, transportation, robotics and biotechnologies. Among them, information and communication technologies (ICTs) are playing a critical role by impacting on and modifying our lives, making our ethical understanding of privacy increasingly problematic. The age in which we are living is strongly structured around information and knowledge, and the equal access to information and the freedom of exchange of ideas are among its main challenges. Contemporary and emerging ICTs are facilitating the desire for knowledge and the need to communicate.[177] A new communication system, increasingly speaking a universal and digitised language, is emerging. Many authors[178] are talking about a social revolution, referring to the profound changes in the traditional limits of space, time and the boundaries of the individual body, which are constantly challenged by technological advances. "Society is now constructed around the space of flows."[179] Castells defines ICTs as "de-centred, dispersed and disseminated, controlled by individuals, network-oriented".[180] One of the most distinctive features of the new technological paradigm is thus ICTs' faster capability of being used to reproduce innovation. The contemporary technological, economic and social revolution has spread throughout the world in less than two decades, in a different way than other previous revolutions. Since emerging ICTs are evolving and diffusing increasingly quickly, it is difficult to predict or even describe the social and ethical implications of their development and use.

4.1.2 The surveillance society

Modern societies have been defined as surveillance societies because of their structural need to collect personal and organisational data to operate efficiently. Tolerance to increased surveillance for security purposes is also growing, and mainly derives from the lower disposition of modern societies to accept any kind of risk, as well as to the emergence of new global and less foreseeable threats.[181] The power and capability of governments and private organisations to aggregate and analyse private information is growing. Privacy of people is often sacrificed for convenience or security, in a way in which we are becoming a transparent society.[182] Surveillance systems have become commonplace in our everyday life, and new technologies and applications constantly emerge. The most traditional forms of surveillance, such as closed-circuit television systems or computer databases, are being joined by new identification technologies, such as biometrics, DNA screening and monitoring for insurance and employment, RFID and smart cards; and tracking and monitoring technologies such as mobile phones services, electronic records of financial transactions, automated GPS tracking, Internet monitoring devices such as cookies keep records of what a person has viewed online. New image analysis algorithms and new sensors systems, as well as ICT implants in the human body and

within the next 5-10 years, "future" are technologies which are still in a developmental phase and will not be deployed before 10 years.

[177] Humans tend unavoidably to communicate and exchange information about themselves, even if they don't want to (the desire not to communicate in any case is an expression of something) or they don't realise they are communicating (e.g., non-verbal communication). The word *communication* comes from the Latin verb *communico* which means "to put in common".

[178] Castells, Manuel, *The rise of the network society. The Information Age: Economy, Society and Culture*, Blackwell Publishing Ltd, 1996.

[179] Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy*, MIT Press, Cambridge MA, 2006, p. xvi

[180] Castells, op. cit.

[181] Chandler, Jennifer, "Privacy versus national security: Clarifying the Trade-off", in I. Kerr, C. Lucock and V. Steeves (eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, Oxford: 2009, pp. 121-138.

[182] See Brin, David, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?,* Addison-Wesley, Reading, MA, 1998.

nanotechnologies deployed for surveillance purposes, are posing new ethical and legal challenges. Surveillance is becoming ubiquitous, pervasive and "banalised"[183].

According to many authors, "surveillance presents us with constant ethical paradoxes", as they are "useful but harmful, welcome but offensive, a necessary evil but an evil necessity"[184]. Ethical issues of the information age were first summarised by Richard Mason in the mid-1980s, and included issues such as accuracy, accessibility, property and privacy[185]. In his article "Ethics for the New Surveillance", Gary T. Marx proposed a comprehensive ethical framework "for thinking about personal surveillance and new information technologies"[186]. The author suggests 29 questions to help determine the ethical use of any surveillance systems or practice. The questions address the means of data collection, the context (including, among other things, the principles of consent, data minimisation and data protection), and the uses of surveillance data. According to David Lyon, surveillance today "is a central means of social sorting, of classifying and categorizing populations and persons for risk assessment and management"[187]. Lyon discusses the inadequacy of current metaphors to address the problems raised by contemporary surveillance, based on the image of Orwell's Big Brother[188] and Foucault's analysis of Bentham's Panopticon[189]. These metaphors are less relevant today because they cannot explain new forms of electronic data surveillance that have emerged following the process of computerisation and the possible collection of personal data everywhere. We are now obliged to conceive the space where surveillance occurs as being either physical or figurative (cyber space), as well as to conceive the object of surveillance as being a thought, a desire or need (for instance, online surveillance for personal advertising). Lyon proposes a new ethics for contemporary everyday surveillance that is based on the dignity of the person and that considers the key concept of personhood as central. According to Lyon, a crucial challenge for the years to come appears to be the necessity of finding an agreement on what constitute the human dignity and social justice that may be compromised by surveillance systems.

---

[183] By "banalisation", we mean making surveillance commonplace (banal), so that it becomes something we as a society do not care about. Banalised forms of surveillance enter our daily life without notice, so that they become a common part of our socio-political and economic relations, so that we become acclimatised or accustomed to surveillance in general, even if we are not always aware of the deployment of particularly intrusive forms of surveillance. The term is used to indicate the increasing pervasiveness of surveillance, right down to the level of the individual (parents monitoring their children's whereabouts or taking pictures of what their neighbours are doing). Some examples could be the capture, storage and processing of fingerprints of frequent costumers of sporting complexes, in order to ease their access to and use of facilities, or the processing of large amounts of personal data in social networks for running "small entertaining applications". In the field of law enforcement, it could be represented by the disproportionate retention of DNA in cases involving petty crimes. This idea partially resonates with the concepts of "soft surveillance", developed in Marx, G.T., "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information", in T. Monahan (ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life*, Routledge, New York, 2006, pp. 37-56. For more on banalisation, see Bellanova, R., P. De Hert, and S. Gutwirth, "Variations sur le thème de la banalisation de la surveillance", *Mouvements*, No. 62, 2010.

[184] See Sewell, Graham, and James R. Barker, "Neither good, nor bad, but dangerous: Surveillance as an ethical paradox", *Ethics and Information Technology*, Vol.3, No. 3, 2001, pp. 181-194.

[185] Mason, Richard, "Four ethical Issues of the Information Age", *Management Information Systems Quarterly*, Vol. 10, No. 1, March 1986.

[186] Marx, Gary T., "Ethics for the New Surveillance", *The Information Society*, Vol. 14, Issue 3, August 1998, pp. 171-185. http://www.informaworld.com/smpp/content~db=all~content=a713856357~frm=abslink

[187] Lyon, David, "Facing the future: Seeking ethics for everyday surveillance", *Ethics and Information Technology*, Vol. 3, No. 3, 2001, pp. 171–181.

[188] Orwell, George, *1984*, Mondadori, 1950.

[189] Foucault, Michel, *Discipline and Punish: The birth of the Prison*, Allen Lane, London, 1977.

4.1.3 The future of the Internet

The development of the Internet, perhaps the most revolutionary technology of the Information Age, was essential in the process of innovative creation, decentralised use and distribution of knowledge. The Internet is a platform that gives everyone instant access to a potentially worldwide audience. The Internet was created as a collaborative network for researchers, technological entrepreneurs and scholars in the US.

Since the mid 2000s, the second generation of the World Wide Web (Web 2.0) is supporting a more subjective and participatory approach towards the Web. Blogs, forums, social networking sites represent new forms for the exchange of ideas. The wireless communication revolution, ubiquitous and cloud computing are about making digital information available anywhere for anyone, and at almost no cost. Computers would be invisibly embedded within one's environment (the Internet of things); ubiquitous computing would focus upon interfaces that connect humans to each others, rather than connecting humans with computers. Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects. The rapid growth of Internet forces us to look at a more complex and contemporary definition of public space. Virtual space has become an equally important place for public appearance and political argumentation, as well as for sharing information. The natural tendency of computers to produce and save information raise important ethical issues related to the protection of personal data, as well as to the crucial role that "ephemeral conversation" and the "right to be forgotten" have in social relations.

The Internet is becoming less a *service* used by people, and more a *place* inhabited by its own citizens, the "netizens". This new territory is different from the territory of traditional nation-states: it is virtual (accessible to everyone) and global (everywhere). It is changing our conceptions of the boundaries of the public and private realms: many human activities are done online and shared – not always voluntarily – with other people. New technologies are affecting the amount of data shared and the rapidity of the exchange, impacting our conceptions of what is private and public. Like any space of interaction among humans, some regulation appears to be necessary. Traditional nation-states are trying to apply their regulations to cyberspace, but this often seems not to work so well in the online environment. Some private companies are controlling big parts of cyberspace. Some of those companies are just selling their products, others are putting enormous efforts into building a sort of "cyber-institution" which has impacts on our human rights and basic freedoms.

4.2 Anticipated legal and regulatory challenges

ICT developments, and especially ubiquitous computing scenarios (aka the Internet of things), raise challenges to privacy and data protection understood from a legal perspective, insofar as they threaten the continued existence of the concept and as they resist any attempt at regulation with existing tools.

4.2.1 Challenges

In the following paragraphs, we identify some challenges to privacy and data protection resulting from future and emerging technologies (FETs).

FETs have led to individuals' leaving a huge number of traces that are detectable, (re)traceable and correlatable far beyond their control. Each time individuals use a network,

they leave digital traces. In other words, "today… an individual leaves a vast amount of processable electronic traces in his wake", which cannot be reduced to personal data in the sense of the Data Protection Directive.[190] They become the resources of a very extensive network of profiling devices that generates knowledge concerning and/or affecting the persons who leave these traces. Such practices entail several risks in terms of privacy.

Because of the massive capacities and capabilities of contemporary technologies, a huge amount of information concerning a single individual can be mined, and on the basis of this mining, predictions can be made about the future behaviour of this person. This becomes even more possible with the linkages or fusion of different databases. Contrary to what used to be the case, these predictions are not based upon an initial hypothesis, and consequently they will be teleological. This in turn entails that they depend upon the will and the goal of the person processing the information. The recourse to profiling is at work in almost all sectors of society, and there are now some companies whose core business is to sell these profiles[191]. There lies the danger: normalisation and customisation of people's conduct as a result of the influence over individual behaviour (people act differently if they know that the traces they leave will be processed to build a profile)[192], a loss of control, a sharpening of (informational) power inequalities since users don't know who processes their data and how their data is used by others, and the steering of people's conduct by taking unilateral decisions about them[193]. This is the metaphor of Franz Kafka's *The Trial*. In this epic novel, citizens are at the mercy of a bureaucratised world whose opaque functioning they fail to understand. Not knowing what is happening to them or why, they have no control over their own destinies. Decisions are based upon people's dossier and data and they have no chance to contest. They are helpless.[194] A specific danger in that respect is the development of unsolicited communications and adjustments. Unsolicited communication refers to unsolicited commercial communication through automatic and intrusive means. A good example is spam. Unsolicited communications are not new[195] and are evolving into unsolicited adjustments. Such things already happen, as is the case with Amazon's book recommendation system, which collects information about customers' tastes in order to provide them guidance on which other items to buy. Scenarios involving the Internet of things look even more ominous as it is possible to imagine smart refrigerators making recommendations to buy milk from a new, yet recommended brand.[196]

Furthermore, ambient intelligence technologies blur the division between the digital and physical worlds. They enable us to perform multiple roles (e.g., parent, employee, friend, col-

[190] De Hert, P., and S. Gutwirth, "Regulating profiling in a democratic constitutional state", in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European citizen: Cross disciplinary perspectives*, Springer**,** Dordrecht, 2008, pp. 271-291.
[191] Solove, 2008.
[192] De Hert and Gutwirth, 2008, op. cit.
[193] De Hert and Gutwirth, 2008, op. cit.; Poullet, Yves, "About the E-Privacy Directive: towards a third generation of data protection legislation?", in Serge Gutwirth, Yves Poullet and Paul de Hert (eds.), *Data Protection in a Profiled World*, Springer, Dordrecht, 2010, pp. 3-30.
[194] Solove, Daniel, "The Digital Person and the Future of Privacy", in Katherine J. Strandburg and Daniela Stan Raicu (eds.), *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, Springer, 2006, pp. 3-13.; Pérez-Asinari, M.V., and P. Palazzi, "Défis du droit à la protection de la vie privée - Challenges of Privacy and Data Protection Law", Bruylant**,** Brussels, 2008, pp. 355-365.
[195] And are regulated through Directives 97/7/EC, 97/66/EC, 2000/31/EC, and 2002/58/EC.
[196] González Fuster, Gloria, Serge Gutwirth and Paul de Hert, "From Unsolicited Communications to Unsolicited Adjustments", in Serge Gutwirth, Yves Poullet and Paul de Hert (eds.), *Data Protection in a Profiled World*, Springer, Dordrecht, 2010, pp. 105-118.

league, citizen, etc.) almost simultaneously. Consequently, technology also blurs the boundary between the private and the public sphere.[197]

Finally, ambient intelligence will permit new practices of data mining and profiling. Indeed, "in an environment where every manufactured product is embedded with intelligence, there will be an exponential increase in data"[198] to be mined and profiles to be crafted. This is no wonder as the lifeblood of ambient intelligence, its "core business", is "dataveillance", the massive collection, aggregation and algorithmic analysis of data on everyone and everything.[199] In some way, ambient intelligence features a new generation of profiling: live profiling.

As far as regulation is concerned, we have seen that the scope of data protection concerns all personal data, understood as individuals' *biographical data*[200]. However, just as the ICT world has its own architecture, it also has its own kind of data. Indeed, many of the data left by users on networks are not *biographical*. However, and although they do not lead to the identification of the user, these type of data enable a data processor to track the user and to identify him/her, since they reveal the type, duration of communications, the frequency a user connects to a network, etc. This is the case for cookies, IP addresses or RFID tag numbers, which are associated with a site or an object to which a person connects. Are these personal data? And is personal data the adequate concept since profilers using this kind of data don't need to identify the user behind the traces that he/she has left behind (what is needed is the operations undertaken by the user, which this kind of data reveals, without need to identify the user)[201]. Is data protection able to cope with these changes?

4.2.2 Options at hand

Although FETs present challenges in terms of regulation, they don't necessarily lead to the obsolescence of existing legislation. Indeed, the legal framework consisting of legislation on privacy (cf. opacity tools) and data protection (cf. transparency tools) is sound enough to cope with these mechanisms. For example, it has been argued that the regulation of data mining and profiling can rely upon these instruments[202].

However, relying upon the existing framework shouldn't prevent us from devising new regulations that refine this very framework. The amended E-Privacy Directive was such an initia-

[197] De Hert, P., "Citizens' data and technology, an optimistic perspective", Dutch Data Protection Authority, The Hague, 2009.
[198] De Hert, Paul, Serge Gutwirth, Anna Moscibroda, David Wright and Gloria González Fuster, "Legal safeguards for privacy and data protection in ambient intelligence", *Personal and Ubiquitous Computing*, Vol. 13, No. 6, 2009, pp. 435-444.
[199] "Dataveillance" comes from the juxtaposition of data and surveillance. See Clarke, R., "Information Technology and Dataveillance", *Communications of the ACM*, Vol. 31, No. 5, May 1988, pp. 498-512.
[200] Poullet, 2010, op cit.
[201] Poullet, Yves, "Pour une troisième generation de règlementation de protection des données Défis du droit à la protection de la vie privée - Challenges of Privacy and Data Protection Law", in M.V. Pérez-Asinari and P. Palazzi (eds.), Brussels, Bruylant, 2008, pp. 25-70.
[202] De Hert, Paul, and Serge Gutwirth, "Regulating profiling in a democratic constitutional state", in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European citizen: Cross disciplinary perspectives*, Springer, Dordrecht, 2008, pp. 271-291; Schreurs, Wim, Mireille Hildebrandt, Els Kindt and Michaël Vanfleteren, "*Cogitas, Ergo Sum*. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector" in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European citizen: Cross disciplinary perspectives*, Springer, Dordrecht, 2008, pp. 241-270.

tive.[203] According to its art. 1.2, the Directive particularises and complements the Data Protection Directive in the electronic communications sector.[204] However, in doing so, the Directive adapts data protection principles to the ICT environment. For instance, it introduces two kinds of data that are not personal: traffic data[205] and location data.[206] The Directive shifts from the regulation of the data controller to that of the providers of a publicly available electronic communication service, no matter whether the latter have been involved in operations of personal data processing[207].

Moreover, the intrinsic link between law and technology (law can bind technology, but technology can adapt so as to make the legal framework effective[208] and can help resort to more pragmatic solutions. The latter include privacy-enhancing technologies (PETs) (encryption, anonymisation, etc.), identity management, privacy by design, privacy seals and privacy impact assessments.[209]

The challenges that FETs raise in terms of privacy and data protection remind us how complicated the relationship between the two concepts is. Whereas "data protection" and "privacy" are often used synonymously, data protection in fact does not cover all infringements upon privacy possible in the new ICT environment (let alone the old one). It is thus not without dangers to equate privacy and data protection and to consider that data protection fully represents privacy in the field of ICT, since such a stance does not permit one to see breaches of privacy not linked to the processing of personal data. This is all the more a problem since the two regimes are intrinsically different, and it is essentially the opacity regime of privacy that can set thresholds regarding the principled acceptability or not of new FET-linked practices.

A renewed interest in privacy beyond data protection is thus essential if we want to keep intact the political private sphere of liberty in a world framed by FETs. This is all the more important since we see some practices that affect the privacy of individuals without any processing of personal data. Just as the e-Privacy Directive, from a "privacy mind-set", endorsed the

---

[203] Directive 2002/58/EC on privacy and electronic communications, OJ L 201/37, 31.07.2002, as amended by Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 13.04.2006; and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending, inter alia, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 337 8.12.2009.

[204] Directive 2002/58/EC, art. 1.2: "The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1".

[205] "Any data processed for the purpose of the conveyance of a communication on an electronic communication network, or for the billing thereof".

[206] "Any data processed in an electronic communications network, indicating the geographical position of the terminal equipment of a user of a publicly available electronic communication services".

[207] Rosier, K., "La directive 2002/58/CE vie privée et communications électroniques et la directive 95/46/CE relative à au traitement des données à caractère personnel: comment les (ré)concilier?", in *Défis du droit à la protection de la vie privée*, Cahiers du C.R.I.D. n°31, Bruxelles, Bruylant, 2008, pp. 328-352.

[208] See the Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010. http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm "The legal framework is applicable to those engaged in behavioural advertising, but it does not, however, prescribe how from a technological point of view, such obligations must be complied with."

[209] See Wright, David, Michael Friedewald, Serge Gutwirth, et al. (eds.), *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008, and, in particular, chapter 5.1 where the authors discuss possible technological safeguards in an AmI environment. See also Korff, Douwe, and Ian Brown, Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Final report, prepared for Directorate General Justice, Freedom and Security, Brussels, 2010. http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm

protection of location and traffic data (which are not necessarily personal data), with the emergence of "new" technologies, such as ambient intelligence, the time has come to return to the more normative privacy test, and to invent a new strand of data protection rules that would be triggered when the processing of non-personal data invades the individual's privacy, and more particularly when it steers his/her conduct while invading his/her autonomy.

4.3 Ethical challenges

In contemporary ages, the social agreement on the distinction between what it is private and what is public is constantly changing, and emerging fields of science and technologies are playing a key role in speeding up this process. The re-conceptualisation of privacy from an ethical perspective needs to explore the contemporary institutional and cultural capacities to shape technological change without endangering fundamental rights, freedoms and social values.

Critical ethical, social and political issues are indeed emerging. The ICT-related ethical challenges we are facing in contemporary times are mainly about making choices that preserve our wellbeing, our security and privacy, as well as this revolutionary ability to quickly innovate. The crucial privacy-related issue seems to be one of control, say, the risk for individuals to accept automatically the loss of control about themselves, their bodies, their minds, their personal information. Awareness and genuine consent on the part of the subjects is lacking in many circumstances. The issue of control is crucial also in consideration of the constant emergence of new powerful embedded technologies, ubiquitous surveillance techniques and cloud computing services that deeply affect the autonomy and freedom of choice of individuals, as well as the control over their personal data. At the same time, modern technologies often also provide new means to prevent older risks. There are many technologies that may be used to protect the privacy of our information and online activities.[210]

New ICTs have become a central part of our day-to-day existence, our family and community relations. ICTs can be used to study, work, play and interact with other people. New ICTs have a profound impact on the basic relationships between individuals, such as those among friends, family members and partners. The emergence of new information technologies forces us also to re-examine the definition of what is intimate, with people giving up important parts of their private life just because new technologies make it possible. There are also concerns over the emergence of new physical[211] and mental[212] health problems arising from the intensive usage of new technologies, such as complex forms of paranoia and obsessive compulsive disorder. On the other hand, researchers have also documented positive impacts on mental

[210] Privacy enhancing technologies (PETs) can be divided into two main groups, those allowing anonymous interactions, such as proxy servers, and those providing data minimisation services, such as the privacy-by-design approach.

[211] Sitting a long time in a static position can cause musculo-skeletal complaints; there is some evidence that intensive computer usage can contribute to passive lifestyle and obesity, as well as deteriorated sleeping habits. See Punamäki, Raija-Leena, et al., "Use of information and communication technology (ICT) and perceived health in adolescence: The role of sleeping habits and waking-time tiredness", *Journal of Adolescence*, Vol. 30, No. 4, 2006, Aug 2007, pp. 569-585.

[212] Research has confirmed that the use of interactive media may turn some adolescents into addicts and place them at risk of losing control over their behaviour. See Eppright, T., M. Allwood, B. Stern and T. Theiss, "Internet addiction: A new type of addiction?", *Missouri Medical Journal*, Vol. 96, No. 4, 1999, pp. 133-136.

health, in children's behaviour[213] and family relations[214]. Additional ethical issues refer to the digital divide, the possibility that computer technologies have increased the socio-economic gap between those groups of people with power and wealth and historically disadvantaged socio-economic, racial and gender groups. This is also true in a global context: there are large areas of the world, and considerable segments of population, cut off from the new technological revolution. In the Information Society, digitally illiteracy has taken over from traditional illiteracy.

The philosophical interest in the ethical implications of computer technology that emerged during the 1980s has three central lines of inquiry[215], i.e., the ethical challenges to social, moral and political values raised by changes in society and individual lives (information ethics), the nature of computer ethics itself (meta-ethics) and the ethical obligations of professional experts (professional ethics). According to the philosopher Helen Nissenbaum, the ethical dimension of information technologies that are changing the ways in which we communicate and the amount of information we share relies on the fact that they are challenging previous commitments to values and principles. Even the questions that may address only the system's technical character are often "rooted not in an interest in the technology alone, but in a concern – and usually a dispute – over values"[216]. In Nissenbaum's view, we urgently need to synchronise our technological progress with the principles upon which our societies rely. Among the most problematic issues is the re-framing of the private sphere, through replacing the actual with the virtual, face-to-face communication with mediated communication, intimate interactions with chat rooms. Nissenbaum wonders whether this new way of communicating deprives us of our essentially human character, and consequently of meaningful opportunities for emotional, spiritual and social growth.

The foregoing ethical considerations of emerging ICTs raise three core groups of issues:

- Upon which values does the global network society rely? In which cases are emerging ICTs eroding or enhancing the right of an individual to have a private space? How can the individual be empowered in controlling his/her right to privacy? Have particular groups of people special privacy needs? How and by whom can they be protected?
- What degree of control (balance between censorship, crime control, security and freedom of speech, anonymity, privacy) do nation-states exert over the Internet? Can a state maintain sovereignty over the Internet? Must the Internet be conceived as a special political zone? When is Web 2.0 a public space and when a private space?
- Do companies have social responsibilities of a government-like nature towards their users? Are they accountable only in relation to their shareholders or should they be accountable to the netizens who use their services? How can profit-oriented interests be reconciled with fundamental human rights and freedoms?

[213] For instance, ICTs appear to have a positive impact on children's cognitive skills and school achievements. See Subrahmanyam, K., P. Greenfield, R. Kraut and E. Gross, "The impact of computer use on children's and adolescents' development", *Journal of Applied Developmental Psychology*, Vol. 22, No. 1, Jan 2001, pp. 7–30.
[214] See Hughes, R., Jr., and J.D. Hans, "Computers, the Internet, and families. A review of the role new technology plays in family life", *Journal of Family Issues*, Vol. 22, No. 6, 2001, pp. 778–792.
[215] See Nissenbaum, Helen, "Information Technology and Ethics", *Berkshire Encyclopedia of Human-Computer Interaction*, Berkshire Publishing Group, Great Barrington, MA, 2004, pp. 235-239
[216] Nissenbaum, Helen, "How computer systems embody values", *IEEE Computer*, Vol. 34, No. 3, March 2001, pp. 1120, 118-119.

4.4 Social and economic challenges

From a social viewpoint, it is interesting to note that social actors have resorted to new strategies towards threats, acute and potential, against privacy. These strategies can be framed in terms of risk governance.

Risk governance consists in understanding the threats to privacy and the vulnerabilities in systems that could make them a target for evil-doers. Identifying and treating threats and vulnerabilities and the risks they pose is what risk managers do. In fact, many utilities, critical infrastructure operators, insurance companies and other publicly traded companies listed on stock exchanges take risk management very seriously indeed. They scan the horizon for emerging threats and probe the vulnerabilities of their companies, maintain risk registers and plan ways to eliminate, mitigate or avoid unacceptable risks. Some stock exchanges, such as the London Stock Exchange (LSE), require that companies state in their annual reports their views on the most serious risks facing the company and what steps they are taking to treat those risks.[217]

Many companies recognise privacy presents risks or, rather, not ensuring adequate protection of personal data presents risks. If personal data are lost or stolen or compromised in some way, they may be obliged to inform regulators as well as the individuals concerned. If they are playing too "fast and loose" with personal data, they may suffer a loss of trust by their customers and damage to their reputation which could harm the prospects for growing a market or providing a service. In fact, some companies already include privacy in their risk management schemes. Businesses increasingly take privacy seriously, hiring chief privacy officers and chief information security officers.[218] The International Association of Privacy Professionals (IAPP)[219] has been growing rapidly and now has more than 8,000 members, most of whom are based in industry, which reflects even industry's concern not to overstep the boundaries of what is socially as well as politically acceptable.

Although the balancing paradigm has been the subject of many column inches in the media and in scholarly journals, almost nothing has been written about privacy risk management in academic journals as an alternative paradigm even though the privacy risk management paradigm is already embedded in the activities of many companies. While there is almost nothing in the academic press, the issue has drawn the attention of data protection authorities or, at least, that of Ontario's Information and Privacy Commissioner. Ann Cavoukian gave a presentation in September 2008 following which, she explains, many participants approached her to express their interest in better understanding the relationship between privacy and risk management. To that end, she assembled a working group of privacy and risk management

[217] Companies listed on the LSE are expected to comply with the Combined Code on Corporate Governance, Section C.2 of which states that "The board should, at least *annually*, conduct a review of the effectiveness of the group's system of internal controls and should *report to shareholders* that they have done so. The review should cover all material controls, including financial, operational and compliance controls and *risk management systems*." [Italics added.] The Combined Code is published by the Financial Reporting Council. The quote is from the June 2006 version of the code. A footnote on p. 14 suggests that the Turnbull guidance be consulted on how to apply this part of the code. The Turnbull guidance, named after Nigel Turnbull, chairman of the committee that prepared the guidance, was originally published in 1999. It provides guidance for listed companies on risk management and reporting. www.frc.org.uk/corporate/internalcontrol.cfm

[218] Schwartz, Paul M., Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment, A Report from the Privacy Projects.com, 2009, p. 24 et seq. http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf

[219] https://www.privacyassociation.org/

professionals in early 2009, which was the genesis of a publication with the title *Privacy Risk Management*.[220]

The 27-page publication is essentially a guidance for companies. It notes that personal information is an asset, the value of which needs to be protected by a formal risk management discipline. Privacy can be managed like any other area of risk such as those posed by technology, economic factors or the environment. The guidance cites an example of the "staggering" cost of a data breach. A survey of US companies in 2009 yielded an average cost of $204 per compromised record; one breach of 100,000 records cost $31 million to resolve.[221] Individuals also bear significant costs.

The Ontario guidance on privacy risk management (PRM) builds on the ISO 31000 Risk Management Framework and consists of six main steps, which are paraphrased here as follows:[222]

1. *Establishing context* – involves scanning and assessing factors from an organisation's external context that can affect privacy risk, e.g., the social, legal, technological, competitive environment, drivers and trends in privacy issues, perceptions and expectations of external stakeholders regarding privacy. It also involves evaluating the internal context, e.g., the organisation's governance structure, operational and strategic objectives, roles and accountabilities, policies, information systems and data flows, decision-making processes, relationships with and perceptions of internal stakeholders, as well as the organisation's culture.
2. *Identifying privacy risks* – so that they may be eliminated or mitigated. Privacy risks may cause direct or indirect loss resulting from inadequate or failed internal processes and systems, staff issues, external events and risks related to a company's outsourced service providers. In addition to traditional risk identification processes, such as privacy impact assessments (PIAs) and privacy audits, other techniques can be leveraged to identify privacy risks, such as developing a culture of privacy protection, listening to employee and business partner feedback, enhancing security measures, following the flow of the organisation's information, examining key business processes, embedding a formal change management program, reviewing third party processes, performing self-assessments, establishing privacy committees and engaging internal audit.
3. *Analysing and evaluating risks* – involves ranking each of the identified risks. Each privacy risk must be considered within the context of an organisation's existing technological, process and physical controls. Residual risk is the level of risk remaining after internal controls. Those with the greatest residual risk are identified as the highest priority. Identified risks may be subject to qualitative analysis[223], semi-quantitative analysis[224] and/or quantitative analysis.

---

[220] Information and Privacy Commissioner of Ontario, *Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed*, Toronto, April 2010. www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf

[221] http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1379486,00.html#

[222] *Privacy Risk Management*, op. cit., pp 8-17.

[223] The Office of the Privacy Commissioner of Canada offers an example of the qualitative approach in its "PIPEDA Self-Assessment Tool". http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.cfm

[224] This approach is used by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA) in their "Privacy Risk Assessment Tool" which measures an organization's performance against the Generally Accepted Privacy Principles (GAPP). http://www.cica.ca/service-and-products/privacy/gen-accepted-privacy-principles/item10677.pdf

4. *Treating risks* – includes a variety of techniques to mitigate risks and enhance opportunities, ranging from risk avoidance by limiting the amount and type of data collected (data minimisation), to privacy risk reduction by using data protection controls and other preventative measures, to risk transfer by making use of third party remedies, like purchasing internet liability insurance.[225]
5. *Monitoring for continuous improvement* – privacy risks are continuously evolving. Monitoring will uncover the need to revisit or introduce new strategies.
6. *Communication and consultation* – involves communicating with staff, reporting to management and Board on the effectiveness of privacy measures, establishing a response plan for communicating in the event of a privacy breach, and creating mechanisms for providing feedback and consultation on privacy issues.

The guidance concludes by saying that risk and privacy professionals need to work together to develop practices to manage the opportunities and risks posed by the management of personal information. It says there are "undeniable" competitive advantages to be realised by being perceived by customers as the "best" at protecting personal information, but the bottom line is that the potential for significant damage to the organisation and irreversible harm to the individual is simply too great to be dismissed.[226]

While the Ontario publication provides detailed and useful guidance on privacy risk management, the term was, however, coined earlier. It was used by the Treasury Board of Canada in its privacy impact assessment e-learning tool in 2003[227] and PricewaterhouseCoopers was using the term since at least the year 2000.[228]

Adopting the privacy risk management paradigm is a way of changing the playing field from the balancing paradigm in which privacy will almost always lose to a risk-based paradigm wherein stakeholders identify and consider the risks to privacy, what is at stake in particular situations, what are the consequences and what actions can be taken to address, avoid, eliminate or mitigate the risks and their the consequences. Good risk management (or risk governance) practices are well established.[229] Good risk governance follows a continuous cycle of identifying, analysing and assessing risks and engaging stakeholders in the process to find solutions.

Advocates of privacy impact assessment (PIA) have been migrating to this privacy risk management paradigm even if the terminology has yet to gain wide currency. Almost all of the privacy impact assessment manuals and handbooks, published by Australia, Canada, New

[225] *Privacy Risk Management*, op. cit. See p. 14 for additional treatment strategies.
[226] *Privacy Risk Management*, op. cit., p. 18.
[227] Dated 26 Sept 2003. http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/assistant/mod23/mod23-1-eng.asp
[228] A PWC press release on the appointment of Dr Lawrence Ponemon to the US Federal Trade Commission's Privacy Committee describes him as having founded PWC's Privacy Risk Management and Compliance practice. See "PricewaterhouseCoopers' Ponemon Named To FTC Privacy Committee", 31 Jan 2000. http://www.thefreelibrary.com/PricewaterhouseCoopers%27+Ponemon+Named+To+FTC+Privacy+Committee.-a059088078
[229] See, for example, Ortwin Renn's modern classic *Risk Governance*, Earthscan, London, 2008. Renn says (pp. 8-9) that risk governance "includes, but also extends beyond, the three conventionally recognized elements of risk analysis (risk assessment, risk management and risk communication). It requires consideration of the legal, institutional, social and economic contexts in which a risk is evaluated, and involvement of the actors and stakeholders who represent them."

Zealand, the United Kingdom and the United States, encourage organisations to include privacy in their risk management activities.[230]

5 CONCLUSIONS

In the following paragraphs, several points will be discussed. First, and maybe the most important finding that can be made from this multidisciplinary approach, is the fact that each discipline constructs its own notion of privacy. Secondly, it is equally interesting to note that each science values privacy differently, and therefore balances it sometimes differently against competing values. Finally, and maybe more difficultly, is the question of how to articulate these different conceptions within sound decision making process?

5.1 A relative mode of existence

This section will focus on the different constructions of privacy. Indeed, because of its multiple and shifting dimensions that stem from the different disciplines that study the concept, it is impossible to grasp the essence of privacy, the ontological core of the concept, assuming that such a core exists (which we don't).

Law distinguishes between privacy and data protection. Law understands the legal right to privacy as protecting the intimacy as well as the autonomy of citizens, whereas data protection is seen as a legal tool that regulates the processing of personal data.[231] Ultimately, both rights are considered as instrumental tools in order to protect the political private sphere, which hallows the autonomy and self-determination of the individual. Whereas the legal right to privacy determines which actions from the government (or private parties) are deemed to be lawful in relation to citizens' autonomy, the legal right to data protection surrounds such practices with safeguards, transparency and accountability wise.

The social approach to privacy does not make the distinction between privacy and data protection. It seems to include issues that other disciplines (e.g., law, ethics) would frame in terms of data protection within privacy matters. Indeed, as a matter of fact, it appears to conceptualise privacy mainly in terms of informational control (current social practices of governments or corporations consist in the processing of huge amounts of information), and hence in terms of intimacy. However, more emancipatory dimensions are not totally absent from the social discourse (i.e., dignity, autonomy, individuality, and liberty).

Economics resort to quantification in order to operate properly, and there is no exception for privacy, which is quantified as personal data. However, the notion of personal data used within this framework is broader than the legal notion of personal data.

---

[230] For example, the Australian guide says "PIA information feeds into broader project risk management processes." Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, 2006, revised May 2010, p. vii. http://www.privacy.gov.au. [On 1 November 2010, the Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner (OAIC).] The ICO PIA handbook states that "A PIA is part of good governance and good business practice. A PIA is a means of addressing project risk as part of overall project management. Risk management has considerably broader scope than privacy alone, so organisations may find it appropriate to plan a PIA within the context of risk management." Information Commissioners Office (ICO), Privacy Impact Assessment Handbook, Version 2.0, Wilmslow, Cheshire, June 2009, p. 5.

[231] Understood as *biographical* data, cf. next footnote.

Indeed, the data protection directive only covers so-called *biographical* data, i.e., data that relate to an identified or identifiable natural person.[232] The economical approach instead refers to personal data not only when *biographical* data are concerned, but also when any information belonging to an individual (but which doesn't necessarily lead to his/her identification) is concerned. On the other hand, another important development of economics in relation to privacy has been the further quantification of the latter, resulting with the commodification of private information and its use as the change in commercial transactions. Does this have an influence on how economics value privacy (cf. *infra*)?

When thinking in ethical terms about privacy, one has to remember that ethics is a branch of philosophy that assesses questions about morality; say about issues that can be classified as good (or right) and bad (or wrong) (cf. *supra*, 2.4). This implies that ethics will only be mobilized when there is the necessity to assess (or judge from a moral viewpoint) a course of action, undertaken by an autonomous agent. In our case, ethics thus relates to actions involving the privacy of individuals. Hence, ethics appears to be a procedural tool that provides guidelines in order to assess[233] a selected course of action, but whose scope is not about giving a substantial definition of a notion. In other words, it can only assess actions relating to a pre-existing concept. Consequently, the scope of ethics lies more in trying to value the notion of privacy,[234] rather than trying to substantiate it. Therefore, and in order to grasp this concept, ethics, as a branch of philosophy, naturally turns towards this discipline in order to provide a definition of privacy. Beyond the different taxonomies that exist, such a philosophical approach mainly associates privacy with the concepts of autonomy[235] and intimacy. Equally, as far as data protection is concerned, ethics concern moral justifications and modalities regarding the processing of such data. Indeed, ethics envisage data protection independently from privacy, because it raises other types of issues that are independent from the ones raised by privacy related actions. The concept of data protection however, is defined according to the relevant legal instruments (as opposed to privacy, which is defined from a philosophical viewpoint).

What can be concluded from these different conceptualisations of privacy? It appears from our analysis that although the different disciplines envisage privacy from different viewpoints, they nonetheless all seem to refer privacy in terms of either autonomy or intimacy.[236] In this sense, there is a strong similarity between the four approaches. But this similarity can be taken one step further if one thinks about the concepts of autonomy and intimacy. Ultimately, intimacy can be thought of as a form of autonomy, centred however around the individual. Autonomy should indeed include the possibility for one's self-development both before and away from the eyes of others. Autonomy, in the end, should, and does, include the faculty to shy away from others. Such an ultimate analysis is also worth from an economical viewpoint, since, as will be seen in the next paragraph, economically valid operations entail balanced

[232] Article 2(a) states that "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".
[233] In terms of good or bad, i.e. morally.
[234] And according to this value, trying to determine the morality of an action that is articulated upon the concept.
[235] From an ethical perspective, this is coherent, given that, in order to take actions that can be ethically assessed, one has to be an autonomous agent with a capacity of volition.
[236] Privacy as intimacy and autonomy as well as privacy and data protection as a means to protect the political private sphere from a legal perspective; privacy as (mainly, but only) information control from a social viewpoint; privacy as autonomy and intimacy from an ethical perspective; and privacy as informational control in economics.

operations power wise, which in turn entails that a degree of autonomy be entitled to the different concerned market actors. Interestingly enough the four disciplines at hand ultimately conceptualise privacy in terms of autonomy of the individual.

One might however ask if this is really of help: what is the added value of switching a concept whose definition eludes us, with an equally hard to grasp notion? First, although indeterminate, autonomy as a concept is more precise than privacy. It is fundamentally entangled with the concept of liberty (one might say they are two different words for the same notion), which is negatively defined; in other words indeterminate! Second, it might be that the several disciplines appropriate themselves the concept of autonomy (i.e., liberty) and substantiate it differently. For instance, economic autonomy might not be the same as social autonomy. However, in this respect, it is interesting to notice that the four disciplines refer to the same taxonomies in order to delineate more accurately the concept from their disciplinary viewpoint.[237]

One might argue that being exhaustive (i.e., finite, determinate) by nature, taxonomies might not be able to fully substantiate a concept that is indeterminate by nature (i.e., indefinite), and that therefore, some shadow zones remain. In such a situation, it is important to adequately articulate the different disciplines. Now, as abovementioned, the scope of this paper is the European legal order. This entails that it only considers activities that take place within this order, and which thus have to comply with the touchstone values of such an order. In other words, intersubjective or economical autonomy may at some point be trumped by political autonomy, understood as a touchstone principal of the social contract that grounds the European order.

5.2 Different disciplines, different values of privacy

Whereas the previous section showed in what way the four disciplines at hand conceptualise the notion of privacy, this section will be dealing with how theses different discipline value privacy.

In order to understand the value that law attaches to privacy, it is necessary to keep in mind the framework within which the law is operating: the democratic constitutional State. Within this framework, both the legal rights to privacy and data protection are seen as protecting the political private sphere, which in turn, is seen as one of the cornerstone principles of such a kind of State. Within such a constitutional mindset, great importance is attached to privacy, although its value is not absolute, as it may conflict with other values and rights that are of equal importance to the democratic constitutional State (e.g., security).

Equally, it follows from our analysis that privacy is of great value for the society. Privacy is critical to the functioning of democracies it is argued, because autonomy is instrumental in achieving responsible citizenship, diversity of speech and behaviour. However, just like the legal discourse, a social approach to privacy acknowledges the non-absolute nature of privacy

[237] The legal approach does not refer to such authors, because it relies upon the premise that it is up to the judge to substantiate the concept of privacy, and has thus undertaken to describe the relevant case-law, cf. *Supra*, 2.1. However, and as indicated in 2.1 as well, judges may build upon legal authors (the "doctrine") when it is deemed helpful and relevant. Such authors that might have influenced the judges are amongst the authors whose taxanomies are being used by the other disciplines of this paper, e.g., Solove, Daniel J., "Conceptualizing Privacy", *California Law Review*, Vol. 90, No. 4, 2002, pp. 1087-1155; Nissenbaum, Helen, "Privacy as Contextual Integrity", *Washington Law Review*, Vol. 79, No. 1, 2004, pp. 101-139.

and the dangers that might follow from such an absolutist conception (e.g., the feminist critique), and hence, the need to balance it with other values.[238]

The economical perspective on the value of privacy is quite ambivalent. What seems clear is that markets rely upon transparency in order to work properly. Indeed, in the context of markets, the opacity that is enabled by privacy leads to informational asymmetries, i.e., the situation whereby a party cannot make a fully informed choice because of lacking information and/or because the other party is better informed. In this respect the concept of trust is pertinent (i.e., the more transparency, the more trust between parties, the better economical transactions). The question might then be asked as to what kind of information does economically driven transparency strives to disclose? On the one hand, orthodox neoclassical theory rejects privacy as an undesirable market disturbance, which entails that markets should reach full transparency (i.e., there is nothing that should not be known from a market agent). Others would argue that transparency is needed insofar as it contributes to reduce power imbalances between actors that is made possible by informational asymmetries, and should therefore target information that is instrumental in achieving a market that works as smoothly as possible, i.e., a market that discloses information that contributes to have balanced economic operations. Therefore, the point of economic (and market) transparency, it can be argued, lies less in disclosing all the information available concerning a market actor, than in featuring all the information that is necessary in order to have balanced (in terms of powers) economic transactions.[239] Thus, such a point of view implicitly relies upon a conception of autonomous market actors endowed with some capacity of informational control.

In order to value privacy, ethics resorts to a multidisciplinary set of arguments. What is clear from these arguments, is that privacy –or rather, the need for privacy- is an essential element of the human condition, both from a biological, anthropological, or even political viewpoint. Ethics however, tells us too that privacy is not absolute, and its scope depends upon cultures, societies and times, but also maybe from the focus selected (i.e., ontological, biological, intersubjective, or political). In this respect, ethics does also point at the "dark side" of privacy, e.g., the feminist critique.

What follows from this is that all disciplines value privacy, only to different extents. The legal and the social perspectives are relatively close in their valuing as it is tested against the background of the democratic constitutional State. The ethical valuation, although relying to some extent upon political theory, is complemented by a biological analysis that insists upon the critical necessity for privacy. Finally, economics seem to *a priori* trump transparency at the expense of privacy for the sake of well functioning market. However, a more in-depth analysis seems to infirm such a conclusion, and instead, considers that transparency does not concern all personal information, but only the one that is indeed instrumental to reaching this aim, i.e., balanced economical transactions; the latter also relying to some extent upon some privacy.

5.3 Substantial or cost-benefit balancing ?

Balancing covers different operations according to each discipline: Many similarities are to be found in the way balancing is envisaged from a legal and a social viewpoint. Both discipline

[238] Even if such a balancing should be undertaken according to the principles for a "strong balancing", cf. *supra*, 3.2.1.

[239] Balanced economical transactions entail both the disclosure of necessary information and the protection of actors' autonomy.

point at the need to undertake so-called "strong balancing", that is, a balancing that goes beyond a mere proportionality/cost-benefit analysis, and make a fully-fledged substantial test. Such a value-loaded test takes into account the broader context within which such choices operate: the democratic constitutional State, and its touchstone values (among which liberty, but also security). This doesn't mean however, that legal and social balancing totally equate. Whereas judges will perform legal balancing, social actors and stakeholders will undertake social balancing. Thus, when performing balancing in a social context, it is important to take into consideration the characteristics of this context that stem from the nature of the actors that constitute it. This in turn entails some discursive ethics, i.e., framing the debate in a fair way so that social actors can make their choices in the least possible biased, and best-informed way.

From the perspective of economics, balancing is conceived as a straightforward trade-off, a "mere" cost-benefit analysis concerning the disclosure of personal information,[240] which is framed in terms of long and short term cost and benefits from the point of view of the data subject (disclosing information) or the data controller (processing information). Such a balancing would be qualified as "weak" in a social or legal framework. One explanation that might be put forward lies in the fact that economic actors are only (or mainly) driven by economic interests and, there is thus no broader referential in terms of values as is the case in the legal or social perspective. Another explanation might lie in the fact that in many cases market actors act as individual actors, preoccupied by their own interest, which therefore means that the balancing will be undertaken according to different parameters.[241]

Finally, from an ethical viewpoint, the concept of balancing is, one could argue, nearly self-evident as it derives from the concept of privacy whose scope has been ethically defined as non-absolute. Therefore, one needs to draw the limits of the concept, eventually, by balancing it against other values, as is the case in a political and societal, or intersubjective contexts. One has to assume however, that the characteristics of the balancing will vary depending upon the context within which it is performed. In a purely intersubjective setting balancing might draw upon "economical balancing", whereas more political and/or societal settings might draw from our legal and social analysis.

In addition to that it is enlightening to see that all disciplines share the same analysis as to the risks that ICTs bear for the privacy (and hence the autonomy) of individuals. Ethics encompasses broader challenges that include physical and mental problems, or the need to reconceptualise the private sphere. The legal and social approaches on the other hand, focus on narrower issues, but make attempts at providing solutions: the former by advocating a better use of the existing legal framework (which entails a renewed interest in the right to privacy), the latter in advocating for new social strategies aimed at the management of risks.

5.4 How to make sense of a multidisciplinary approach: articulating the perspectives

In the preceding paragraphs, we have undertaken an in-depth analysis of four dimensions of privacy. In doing so, we have outlined the contrast and similarities that exist among the various disciplines.

[240] Which is broader than *biographical* information in the sense of data protection, cf. *supra*.
[241] From which stems the question of the status of public authorities when they are acting as market actors.

The question remains however, as how to make sense of this, especially in the framework of European policy and decision-making.

The key for doing so lies in the valid articulation of the perspectives. Indeed, sound policy-making relies upon analyses of issues that are as comprehensive as possible, and which must therefore grasp the full complexity and dimension of the latter, and must also take into account the viewpoints of all relevant stakeholders (economic, social, civil society, etc.). Consequently, all the four concerned disciplined must be taken into the equation, because they all have their own level of validation.

Therefore, when taking decisions pertaining to the privacy of individuals, policy-makers should respect a discursive ethics that enables all the relevant stakeholders to participate in an enlightened manner (social dimension), and should measure the biological, physiological, and economical consequences (ethical and economical dimension) of their decisions to be. Furthermore, their decisions will be materialised in law, which uses its own notion of privacy. Such a deconstruction of the decision making process is not merely theoretical, even though we have seen that ultimately all four dimensions think of privacy in terms of autonomy, and are therefore quite similar on this point. Indeed, the fact of resorting to the same conceptual matrix should never obliterate the fact that this very matrix is indeterminate, and might receive a different substantiation in precise circumstances. Taking into account these potential differences contributes to achieving better decision-making, *inter alia* because it permits to better understand the concept, within its different constructions.

Finally, it is important to always keep in mind that the legislative instruments that are the outcome of such a decision-making process are bound by the constitutional principles that ground the European legal order, which considers the political private sphere as one of its cornerstone and inalienable principles.

APPENDIX: TYPES OF PRIVACY, BENEFITS & HARMS

Table 1: Types of privacy

Types of privacy	Definition / scope	Trade-offs , limitations	Examples of threats[242]
Privacy of person	People have a right to keep private bodily functions (excreting, making love, picking their nose) and body characteristics, including their DNA (genetic code) and other biometrics.	In the interests of its safety and security, society should be able to establish a database of offenders' DNA in order to help identify and apprehend criminals. Some medical research needs access to the genetic fingerprints (DNA) of many people in order to minimise the threat of disease or illnesses that may afflict society.	Government DNA bases in the US, UK and elsewhere include the DNA of many law-abiding citizens. The ubiquitous prevalence of surveillance cameras are making incursions into the privacy of persons. Old people suffering from dementia are monitored all the time.
Privacy of thought and feelings	People have a right to not share their thoughts or feelings and to not have their thoughts or feelings revealed.	Employers need to understand whether their employees are mentally stable and will be able to perform their jobs satisfactorily. This is especially important re jobs in critical infrastructures.	Research is being conducted that would help read people's minds.[243]
Privacy of location and space	People have a right to go wherever they want without being tracked or monitored. They have a right to the privacy of their personal space, including their home, car, office. They have a right to solitude.	Some areas (such as nuclear power plants) are off-limits to most people. If a person is in a car crash, automatic position determination can help get ambulance services or police to the scene of the accident quickly. Parents feel they have a right to know where their children are.	Companies may use location information generated from the user's mobile phones or other web services to bombard the individual with "special offers" from nearby shops. Knowing that an individual is not at home may help evil-doers in knowing when to break in and burglarise the individual's home.

[242] Regan (1995) also observes that politicians and the public agree that the important threats to privacy have arisen from organization-individual relationships, hence are in the public (societal) realm, and not from informal social relationships that are in the private (individual) realm. Cited in Margulis, Stephen T., "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 243-261 [p. 249].

[243] Macrae, Fiona, "Mind reading comes a step closer as scientists map people's brains", *Daily Mail*, 14 March 2009. http://www.dailymail.co.uk/sciencetech/article-1161652/Mind-reading-comes-step-closer-scientists-map-peoples-brains.html. Farahany, Nita, "The Government Is Trying to Wrap Its Mind Around Yours", *The Washington Post*, 13 Apr 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/04/11/AR2008041103296.html?hpid=opinionsbox1

Types of privacy	Definition / scope	Trade-offs , limitations	Examples of threats[242]
Privacy of data and image	People have a right to control over their personal data and image.	Governments may need some personal data for a range of purposes such as taxation, census, the provision of certain social services. Employers may want to see the academic records of prospective employees. Companies and governments can provide more personalised products and services, which should result in efficiency gains for the economy. If one is walking down a street, it is not possible to control someone who takes your photograph or from being captured by closed circuit television (CCTV).	Governments and companies may repurpose personal data, i.e., to use it for purposes beyond those for which the data was originally collected.[244] The paparazzi may pursue a celebrity relentlessly in order to profit from photos even though the person has made strenuous efforts to shield him or herself from such pursuit.
Privacy of behaviour (and action)	People have a right to behave as they please and do what they want without being monitored or having their behaviour controlled by others.	Some people's behaviour and actions may put others at risk – yobs may beat up law-abiding citizens.	Companies may try to manipulate people's behaviour so that they do what the companies want (e.g., to buy their products or services).
Privacy of communication	People have a right to keep their communication with others private and not monitored by others.	Law enforcement authorities and intelligence agencies may need to monitor some people's communication in order to apprehend evil doers.	Governments may monitor everyone's communications and engage in "fishing expeditions", i.e., to identify trouble-makers and dissidents.
Privacy of association, including group privacy	People have a right to associate with whomever they want without being monitored	Someone's association with terrorists or criminals is of legitimate societal concern.	Surveillance cameras and other technologies may be used to determine who meets with whom.

[244] "Facebook, MySpace and several other social-networking sites have been sending data to advertising companies that could be used to find consumers' names and other personal details, despite promises they don't share such information without consent." Steel, Emily, and Jessica E. Vascellaro, "Facebook, MySpace Confront Privacy Loophole", *The Wall Street Journal*, 21 May 2010. http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html

Table 2: Privacy benefits and harms

Types of privacy	Benefits in protecting privacy		Harms arising from compromising privacy	
	To individual:	To society:	To individual:	To society:
Privacy of person	People do not need to feel inhibited if they can perform bodily function in private. Privacy of person is conducive to feelings of individual freedom.	Enabling and supporting privacy of person is conducive to a healthy, well-adjusted society.	People will feel inhibited. It leads to a Big Brother syndrome.	Society will become dysfunctional if it is populated by inhibited citizens.
Privacy of thought and feelings	People can contemplate whatever they like, which will help them grow their creativity and self-expression. People may feel accountable for many of their actions, but they can at least feel as free as a bird in their own minds.	Society benefits from the creativity of free-thinking individuals. Privacy of thought helps society avoid a Huxleyan Brave New World.	People will feel truly enslaved and repressed. They will become dysfunctional. They may lash out at society.	Society will put social order at risk if it is populated by repressed individuals. Social order through "thought control", enforced by "thought control police" is illusory.
Privacy of location and space	Being free to go wherever one wants without others knowing where contributes to the individual's overall sense of living in a democracy, of feeling free.	Freedom of movement is a feature of a trusting, well adjusted democracy.	If our movements and location are monitored all the time, we will suffer from Big Brother syndrome. We will not feel as if we are living in a democracy.	If individuals' locations are monitored all the time, people will feel they live in an exploiting, Big Brother society. There will be a chilling effect. Some people will attempt to undermine the social order. Society puts itself at risk.

Types of privacy	Benefits in protecting privacy		Harms arising from compromising privacy	
	To individual:	To society:	To individual:	To society:
Privacy of data and image	If individuals have control of their personal data, they will feel empowered. It builds self-confidence and a sense that we have real choices.	Democracy benefits from a society of individuals who believe they are in control of their own data (their own destiny).	Individuals will be relentlessly exploited by governments and companies. Personal data enables more precise targeting of individuals. Who wants to be a "target"?	The nature of society will be harmed if governments and companies are continually using personal data to exploit its citizens.
Privacy of behaviour and action	The individual feels free to do what he/she likes without interference from others.[245] People can benefit from solitude, from tranquillity arising from solitude. "Insofar as privacy… frees us from the stultifying effects of scrutiny and approbation (or disapprobation), it contributes to… the development and exercise of autonomy and freedom in thought and action."[246]	Society holds freedom as an important value. Democratic society is composed of individuals who feel free to do what they like. Democracy fosters social cohesion and solidarity.	The individual feels constrained in what he/she can do. The individual feels others watching him, judging him constantly. The individual feels oppressed, subjugated, disempowered, resentful, dysfunctional.	Society is composed of angry, oppressed citizens, who will most likely attempt to vote out, subvert or overthrow the ruling government. They will not be law-abiding because they disagree with the law.

[245] From Westin's (1967) perspective, privacy provides opportunities for self-assessment and experimentation. It is a basis for the development of individuality. It protects personal autonomy. It supports healthy functioning by providing needed opportunities to relax, to be one's self, to emotionally vent, to escape from the stresses of daily life, to manage bodily and sexual functions, and to cope with loss, shock, and sorrow. In sum, privacy is important because it is posited to provide experiences that support normal psychological functioning, stable interpersonal relationships, and personal development. Cited in Margulis, Stephen T., "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 243-261 [p. 246].

[246] Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford CA, 2010, p. 82.

Types of privacy	Benefits in protecting privacy		Harms arising from compromising privacy	
	To individual:	To society:	To individual:	To society:
Privacy of communication	The individual feels free to say whatever he or she likes to whomever he likes. The individual feels free to express his unvarnished views, to express his opinions freely.	Society is composed of people who do not feel inhibited in what they say or the need to be on constant guard re what they say, by phone, e-mail, the Internet, mobile or any other form of communication, including face-to-face communication. Society will benefit from free discussion of a wide range of views, opinions. There is more likely to be growth in communication services if users feel they can use them freely without being monitored. Some companies will benefit from the sale of eavesdropping or monitoring equipment and services.	The individual will need to be careful in what he or she says. There will be a chilling effect. People will feel the effect of Big Brother as well as many little brothers. The person may feel fearful, possibly subdued, possibly angry.	There will be a lack of trust in society, as individuals do not know who will be listening in on their communications and using what is said against them. People will avoid use of certain services especially social networks, which will thus have a chilling effect on the economy.
Privacy of association, including group privacy	The individual will be able to associate with anyone he or she feels like. [247]	Society will benefit by being composed of more social citizens. A wide variety of groups will spring up, some of whom will press for more democratic political or economic change.	The individual will feel more withdrawn. He / she is less likely to associate with certain people or groups.	Social vitality will be sapped as fewer groups will form. Some groups, even innocuous ones, will feel they need to go "underground".

[247] At the socio-political level, in political democracies, privacy provides opportunities for political expression and criticism, political choice, and freedom from unreasonable police interference; it provides opportunities for people and organizations to prepare and discuss matters "in private"; it allows non-political participation in family, religion, and in other forms of association (Westin, 1967). Cited in Margulis, Stephen T., "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 243-261 [p. 246].

LITERATURE

Acquisti, Alessandro, "Nudging Privacy: The Behavioral Economics of Personal Information", *IEEE Security & Privacy*, Vol. 7, No. 6, 2009, pp. 82-85.

Acquisti, Alessandro, Allan Friedman, and Rahul Telang, "Is there a cost to Privacy Breaches? An Event Story", in), *The Fifth Workshop on the Economics of Information Security (WEIS 2006)* Cambridge UK, 2006, pp.

Acquisti, Alessandro, and Jens Grossklags, "Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting", in Camp, L. Jean, and Stephen Lewis (eds.), *The Economics of Information Security*, Kluwer, Dodrecht, 2004, pp. 165-178.

Akerlof, George A., "The Market for "Lemons": Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics*, Vol. 84, No. 3, 1970, pp. 488-500.

Anderson, Ross J., and Tyler Moore, "The Economics of Information Security", *Science*, Vol. 314, No. 5799, 2006, pp. 610 - 613.

Aquilina, Kevin, "Public security versus privacy in technology law: A balancing act?", *Computer Law and Security Review*, Vol. 26, No. 2, 2010, pp. 130-143.

Arendt, Hannah, *The human condition*, University of Chicago Press, 1958.

Arrow, Kenneth J., *Essays in the theory of risk-bearing*, North-Holland, Amsterdam, 1970.

Baker, Stephen, *The Numerati: In Which They'll Get My Number and Yours*, Houghton Mufflin, New York, 2008.

Baker, Tom, "On the Genealogy of Moral Hazard", *Texas Law Review*, Vol. 75, 1996, pp. 237-292.

Barak, Aharon, "Proportionality and Principled Balancing", *Law & Ethics of Human Rights*, Vol. 4, Issue 1, 2010. http://www.bepress.com/lehr/

Bellanova, R., P. De Hert, and S. Gutwirth, "Variations sur le thème de la banalisation de la surveillance", *Mouvements*, No. 62, 2010.

Bendrath, Ralf, and Milton Mueller, "The End of the Net as we know it? Deep Packet Inspection and Internet Governance", Paper presented at: Annual Meeting of the American Political Science Association, Washington, D.C., 2-5 September 2010, 2010. http://ssrn.com/abstract=1653259.

Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge MA, 2006.

Berendt, B., O. Günther and S. Spiekermann, "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior", *Communication of the ACM*, Vol. 48, No. 3, 2005, pp. 101-106.

Blackburn, Simon, *The Oxford Dictionary of Philosophy*, Oxford University Press, 1994.

Bloustein, Edward J., „Privacy as an aspect of human dignity: an answer to dean Prosser", *New York University Law Review*, Vol. 39, pp. 1000-10071964

Brin, David, The *Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?,* Addison-Wesley, Reading, MA, 1998.

Burgess, J. Peter, "Security After Privacy: The Transformation of Personal Data in the Age of Terror", Policy Brief 5/2008, International Peace Research Institute, Oslo (PRIO), 2008. http://www.prio.no/Research-and-Publications/Publications/?mode=type&type=12

Calo, M. Ryan, "The Boundaries Of Privacy Harm", Berkeley Electronic Press, July 2010. http://works.bepress.com/m_ryan_calo/2

Castells, Manuel, *The rise of the network society. The Information Age: Economy, Society and Culture*, Blackwell, Oxford, 1996.

Chandler, Jennifer, "Privacy versus national security: Clarifying the Trade-off", in I. Kerr, C. Lucock and V. Steeves (eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, Oxford, 2009, pp. 121-138.

Clarke, R., "Information Technology and Dataveillance", *Communications of the ACM*, Vol. 31, No. 5, May 1988, pp. 498-512.

Clifford, Stephanie, "Two-Thirds of Americans Object to Online Tracking", *The New York Times*, 29 Sept 2009. http://www.nytimes.com/2009/09/30/business/media/30adco.html?hpw

Cockfield, Arthur J., "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies", *U.B.C. Law Review*, Vol. 40, No. 1, May 2007, pp. 41-68. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1031964

Cohen, Julie E., "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Review*, Vol. 52, No. 5, 2000, pp. 1373-1437.

De Hert, P., "Citizens' data and technology, an optimistic perspective", Dutch Data Protection Authority, The Hague, 2009.

De Hert, Paul, and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action", in Gutwirth, Serge, Yves Poullet et al. (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 3-44.

De Hert, Paul, and Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in Claes, Erik, Anthony Duff et al. (eds.), *Privacy and the criminal law*, Intersentia, Antwerp, Oxford, 2006, pp. 61-104.

De Hert, Paul, and Serge Gutwirth, "Regulating profiling in a democratic constitutional state", in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European citizen: Cross disciplinary perspectives*, Springer, Dordrecht, 2008, pp. 271-291;

De Hert, Paul, Serge Gutwirth, Anna Moscibroda, David Wright and Gloria González Fuster, "Legal safeguards for privacy and data protection in ambient intelligence", *Personal and Ubiquitous Computing*, Vol. 13, No. 6, 2009, pp. 435-444.

Dworkin, Ronald, "It is absurd to calculate human rights according to a cost-benefit analysis", *The Guardian*, 24 May 2006. http://www.guardian.co.uk/commentisfree/2006/may/24/comment.politics

Eppright, T., M. Allwood, B. Stern and T. Theiss, "Internet addiction: A new type of addiction?", Missouri Medical Journal, Vol. 96, No. 4, 1999, pp. 133-136.

Epstein, Yakov M., "Crowding Stress and Human Behaviour", *Journal of Social Issues*, Vol. 37, No. 1, 1981, pp. 126–144.

Etienne, A., *The Limits of Privacy*, Basic Books, New York, 1999

Evans, David, "The Online Advertising Industry: Economics, Evolution, and Privacy", *Journal of Economic Perspectives*, Vol. 23, No. 3, Summer 2009, pp. 37–60.

Farahany, Nita, "The Government Is Trying to Wrap Its Mind Around Yours", *The Washington Post*, 13 Apr 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/04/11/AR2008041103296.html?hpid= opinionsbox1

Foucault, Michel, *Discipline and Punish: The birth of the Prison*, Allen Lane, London, 1977.

Freud, Sigmund, "Das Unheimliche", *Imago*, Vol. 5, No. 5-6, 1919, pp. 297-324.

Freud, Sigmund, "Zeitgemässes über Krieg und Tod", *Imago*, Vol. 4, No. 1, 1915, pp. 1-21

Fried, Charles, Privacy (a moral analysis), *Yale Law Journal, Vol. 77, No. 3, 1970,* pp. 475-493.

Froomkin, A. Michael, "The Death of Privacy?", *Stanford Law Review*, Vol. 52, May 2000, pp. 1461-1543.

González Fuster, Gloria, Serge Gutwirth and Paul de Hert, "From Unsolicited Communications to Unsolicited Adjustments", in Serge Gutwirth, Yves Poullet and Paul de Hert (eds.), *Data Protection in a Profiled World*, Springer, Dordrecht, 2010, pp. 105-118.

Graeff, Timothy R., and Susan Harmon, "Collecting and using personal data: consumers' awareness and concerns", *Journal of Consumer Marketing*, Vol. 19, No. 4, 2002, pp. 302-318.

Grimmelmann, James, "Privacy as Product Safety", *Widener Law Journal*, No. 19, 2010, pp. 793-827. http://works.bepress.com/cgi/viewcontent.cgi?article=1026&context=james_grimmelmann

Grossklags, J., and A. Acquisti, "When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information", *Sixth Workshop on the Economics of Information Security (WEIS 2007), Pittsburgh, PA*, 2007, pp 1-22.

Gutwirth, Serge, "De polyfonie van de democratische rechtsstaat", in Elchardus, M. (ed.), *Wantrouwen en onbehagen*, VUB Press, Brussels, 1998, pp. 137-193.

Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, 2002.

Harizopoulos, Stavros, Mehul A. Shah, Justin Meza and Parthasarathy Ranganathan, "Energy Efficiency: The New Holy Grail of Data Management Systems Research", *4th Biennial Conference on Innovative Data Systems Research (CIDR), January 4-7, 2009*, Asilomar, California, USA.

Harvey, Mike, "PleaseRobMe website highlights dangers of telling world your location", *The Times*, 19 Feb 2010. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7032820.ece.

Hildebrandt, Mireille, and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008.

Hughes, R., Jr., and J.D. Hans, "Computers, the Internet, and families. A review of the role new technology plays in family life", *Journal of Family Issues*, Vol. 22, No. 6, 2001, pp. 778–792.

Hui, K.-L., and I.P.L. Png, "The Economics of Privacy", in Terrence Hendershott (ed.), *Economics and Information Systems,* Elsevier, Amsterdam, 2006, pp. 471-498.

Information and Privacy Commissioner of Ontario, *Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed*, Toronto, April 2010. www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf

Information Commissioners Office (ICO), *Privacy Impact Assessment Handbook, Version 2.0*, Wilmslow, Cheshire, June 2009.

Inness, Julie, *Privacy, Intimacy and Isolation*, Oxford Uniersity Press, Oxford, 1992.

International Telecommunication Union (ITU), "Ubiquitous Sensor Networks (USN)", ITU-T Technology Watch Briefing Report Series 4, ITU, Geneva, 2008. http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000040001PDFE.pdfI

Iqbal, Mohammad Usman, and Samsung Lim, "Privacy Implications of Automated GPS Tracking and Profiling", *IEEE Technology and Society*, Vol. 29, No. 2, 2010, pp. 39-46.

Johnson, Bobbie, "Privacy no longer a social norm, says Facebook founder", *The Guardian*, 11 January 2010. http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

Kerr, Ian R., Max Binnie and Cynthia Aoki, "Tessling on My Brain: The Future of Lie Detection and Brain Privacy in the Criminal Justice System", *Canadian Journal of Criminology and Criminal Justice*, Vol. 50, No. 3, 2008, pp. 367-388.

Korff, Douwe, and Ian Brown, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, Final report, prepared for Directorate General Justice, Freedom and Security, Brussels, 2010. http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm

Laufer, Robert S., and Maxine Wolfe, "Privacy as a Concept and a Social Issue: A Multidimensional Development Theory", *Journal of Social Issues*, Vol. 33, No. 3, 1997, pp. 22-42 [pp. 31-32].

Lenard, Thomas M., and Paul H. Rubin, "In Defense of Data: Information and the Costs of Privacy", *Policy & Internet*, Vol. 2, Issue 1, Article 7, 2010, pp. 149-183. http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf.

Lessig, Lawrence, Privacy as Property, *Social Research: An International Quarterly of Social Sciences*, Vol. 69, No. 1, 2002, pp. 247-269.

Litman, Jessica, Information Privacy/Information Property, *Stanford Law Review*, Vol. 52, 2000.

Lyon, David, "Facing the future: Seeking ethics for everyday surveillance", *Ethics and Information Technology*, Vol. 3, No. 3, 2001, pp. 171–181.

Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, UK, 2007.

MacKinnon, Catherine, *Toward a Feminist Theory of the State*, Harvard University Press, Cambridge, MA, 1989.

Macrae, Fiona, "Mind reading comes a step closer as scientists map people's brains", *Daily Mail*, 14 March 2009. http://www.dailymail.co.uk/sciencetech/article-1161652/Mind-reading-comes-step-closer-scientists-map-peoples-brains.html.

Margulis, Stephen T., "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 243-261. http://onlinelibrary.wiley.com/doi/10.1111/josi.2003.59.issue-2/issuetoc

Marsden, Sam, "Phone 'blagging' methods exposed", Press Association, in *The Independent*, 9 July 2009. http://www.independent.co.uk/news/uk/crime/phone-blagging-methods-exposed-1739387.html

Marx, Gary T., "Ethics for the New Surveillance", *The Information Society*, Vol. 14, Issue 3, August 1998, pp. 171-185.

Marx, Gary T., "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information", in T. Monahan (ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life*, Routledge, New York, 2006, pp. 37-56.

Mason, Richard, "Four ethical Issues of the Information Age", *Management Information Systems Quarterly*, Vol. 10, No. 1, March 1986.

Mill, John Stuart, *On Liberty, in On Liberty and Other Essays*, Digiread.com Publishing, 2010 [originally published in 1859], p. 7.

Miller, Kent D., "Simon and Polanyi on Rationality and Knowledge", *Organization Studies*, Vol. 29, No. 7, 2008, pp. 933–955.

Moore, Adam, "Privacy: its value and meaning", *American Philosophical Quarterly*, Vol. 40, No. 3, 2003, pp. 215-227.

Moore, Barrington Jr., *Privacy: Studies in Social and Cultural History*, M. E. Sharpe, Inc., 1984.

Nissenbaum, Helen, "Privacy as Contextual Integrity", *Washington Law Review*, Vol. 79, No. 1, 2004, pp. 101-139.

Nissenbaum, Helen, "How computer systems embody values", *IEEE Computer*, Vol. 34, No. 3, March 2001, pp. 1120, 118-119.

Nissenbaum, Helen, "Information Technology and Ethics", in *Berkshire Encyclopedia of Human-Computer Interaction*, Berkshire Publishing Group, Great Barrington, MA, 2004, pp. 235-239

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford CA, 2010.

O'Sullivan, Maureen „Lockean Style Property Rights in Land, Software and Genes", in E. Mordini, R. Chadwick et al. (eds.), *Ethics and Health in the Global Village, Bioethics, Globalization and Human Rights*, CIC Edizioni Internazionali, Rome, 2009.

Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, 2006, revised May 2010, p. vii. http://www.privacy.gov.au.

Ortwin Renn, *Risk Governance*, Earthscan, London, 2008.

Parent, W., „Recent work on the concept of privacy“, *American Philosophical Quarterly*, Vol. 20, No.4, 1983.
Pinkerton, James P., “Privacy is a thing of the past”, *The Denver Post*, 24 Nov 2007. http://www.denverpost.com/opinion/ci_7535993
Posner, R. A., “The Economic Theory of Privacy”, *Regulation*, Vol. 9, No. 3, 1978, pp. 19-26.
Posner, R.A., “The economics of privacy”, *The American Economic Review*, Vol. 71, No. 2, 1981.
Posner, R.A., “The Right to Privacy”, *Georgia Law Review*, Vol. 12, 1978, pp. 393-422
Poullet, Yves, “About the E-Privacy Directive: towards a third generation of data protection legislation?”, in Serge Gutwirth, Yves Poullet and Paul de Hert (eds.), *Data Protection in a Profiled World*, Springer, Dordrecht, 2010, pp. 3-30.
Poullet, Yves, “Pour une troisième generation de règlementation de protection des données“, in M. V. Pérez-Asinari and P. Palazzi (eds.), *Défis du droit à la protection de la vie privée - Challenges of Privacy and Data Protection Law*, Brussels, Bruylant, 2008, pp. 25-70.
Pound, R., „Interests in Personality“, *Harvard Law Review*, Vol. 28, 1915, p. 343.
Prosser, William L., Privacy, *California Law Review* Vol. 48, No. 3, 1960, pp. 383-424.
Punamäki, Raija-Leena, et al., “Use of information and communication technology (ICT) and perceived health in adolescence: The role of sleeping habits and waking-time tiredness”, *Journal of Adolescence*, Vol. 30, No. 4, 2006, Aug 2007, pp. 569-585.
Purtova, Nadezda, „Property rights in personal data: learning form the American discourse“, *Computer law & security review*, Vol. 5, No. 6, November 2009, pp. 507-521.
Raab, Charles D., “From Balancing to Steering: New Directions for Data Protection”, in Colin J. Bennett and Rebecca Grant (eds.), *Visions of Privacy: Policy Choices for the Digital Age*, University of Toronto Press, 1999, pp. 68-93.
Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, 1995.
Riemann, Jeffrey, Privacy, Intimacy and Personhood, *Philosophy and public affairs*, Vol. 6, No. 1, Autumn 1976, pp. 26-44.
Rigaux, F., (ed.), *La vie privée, une liberté parmis les autres?,* Larcier, Brussels, 1992.
Rodotà, Stefano. „Data Protection as Fundamental Human Right“, Keynote Speech, International CPDP Conference on “Reinventing Data Protection”, Bruxelles 12-13 October 2007.
Rosen, Jeffrey, “The Naked Crowd: Balancing Privacy and Security in an Age of Terror” *Arizona Law Review*, Vol. 46, No. 4, 2004, pp. 607-619. http://www.arizonalawreview.org/ALR2004/contentsv46.cfm
Rosier, K., “La directive 2002/58/CE vie privée et communications électroniques et la directive 95/46/CE relative à au traitement des données à caractère personnel: comment les (ré)concilier?”, in *Défis du droit à la protection de la vie privée*, Cahiers du C.R.I.D. n°31, Bruxelles, Bruylant, 2008, pp. 328-352.
Roussopoulos, Mema, Laurent Beslay, Caspar Bowden et al., “Technology-Induced Challenges in Privacy and Data Protection in Europe”, A Report by the ENISA Ad Hoc Working Group on Privacy and Technology, Oct. 2008.
Schneier, Bruce, *Beyond Fear*, Copernicus Books, New York, 2003.
Schoeman, Ferdinand D., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.
Schopenhauer, Arthur, *Parerga und Paralipomena*, 1851, translated by E.F.J. Payne, Oxford University Press, Oxford, 2000.
Schreurs, Wim, Mireille Hildebrandt, Els Kindt and Michaël Vanfleteren, “Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profil-

ing in the Private Sector" in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European citizen: Cross disciplinary perspectives*, Springer, Dordrecht, 2008, pp. 241-270.

Schwartz, Paul M., *Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment*, A Report from the Privacy Projects.com, 2009. http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf

Sennett, Richard, *The fall of public man: On the social psychology of capitalism*, Vintage Books, New York, 1978.

Sewell, Graham, and James R. Barker, "Neither good, nor bad, but dangerous: Surveillance as an ethical paradox", *Ethics and Information Technology*, Vol.3, No. 3, 2001, pp. 181-194.

Simmel, Georg, "The Sociology of Secrecy and of the Secret Societies", *American Journal of Sociology*, Vol. 11, 1906, pp. 441-498.

Simmel, Georg, *The Sociology of Georg Simmel*, Compiled and translated by Kurt Wolff, Free Press, Glencoe, IL, 1950, p. 330.

Solove, Daniel J., "'I've got nothing to hide' and Other Misunderstandings of Privacy", *San Diego Law Review*, Vol. 44, 2008, pp. 745-772.

Solove, Daniel J., "Conceptualizing Privacy", *California Law Review*, Vol. 90, No. 4, 2002, pp. 1087-1155.

Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge, MA, 2008.

Solove, Daniel, "The Digital Person and the Future of Privacy", in Katherine J. Strandburg and Daniela Stan Raicu (eds.), *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, Springer, 2006, pp. 3-13.

Sonnenreich, W., J. Albanese and B. Stout, "Return on security investment (ROSI) - A practical quantitative model", *Journal of Research and Practice in Information Technology*, Vol. 38, No. 1, 2006, pp. 45-56

Sprenger, Polly, "Sun on Privacy: 'Get Over It'", *Wired*, 26 Jan 1999. http://www.wired.com/politics/law/news/1999/01/17538

Steel, Emily, and Jessica E. Vascellaro, "Facebook, MySpace Confront Privacy Loophole", *The Wall Street Journal*, 21 May 2010. http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html

Stigler, George J., "An Introduction to Privacy in Economics and Politics", *Journal of Legal Studies*, Vol. 9, 1980, pp. 623-644.

Story, Louise, "To Aim Ads, Web Is Keeping Closer Eye on You", *The New York Times*, 10 March 2008. http://www.nytimes.com/2008/03/10/technology/10privacy.html?em&ex=1205467200&en=9aba6985f3668765&ei=5087%0A

Stross, Randall, "Google Anything, So Long as It's Not Google", *The New York Times*, 28 Aug 2005. http://www.nytimes.com/2005/08/28/technology/28digi.html?pagewanted=1&_r=1

Stuntz, William J., "Against Privacy and Transparency, Secret Service", *The New Republic*, 17 April 2006. Cited by Solove, Daniel J., "Data Mining and the Security-Liberty Debate", *University of Chicago Law Review*, Vol. 75, No. 1, Winter 2008, p. 343-362.

Subrahmanyam, K., P. Greenfield, R. Kraut and E. Gross, "The impact of computer use on children's and adolescents' development", *Journal of Applied Developmental Psychology*, Vol. 22, No. 1, Jan 2001, pp. 7–30.

Sweney, Mark, "UK web users 'wary of revealing too much'", *The Guardian*, 17 May 2010. http://www.guardian.co.uk/media/2010/may/17/social-networking-facebook-privacy-ofcom

Swire, Peter P., "Efficient Confidentiality for Privacy, Security, and Confidential Business Information", *Brookings-Wharton Papers on Financial Services*, 2003, pp. 273-310.
Thompson, Bill, "Networks blur the private and public divide", *BBC News*, 17 March 2010. http://news.bbc.co.uk/1/hi/technology/8570406.stm
Thomson, Judith J., "The right to privacy", *Philosophy and Public Affairs*, Vol. 4, 1975, pp. 295-314.
Travis, Alan, "Fight against terror 'spells end of privacy'", *The Guardian*, 25 Feb 2009. http://www.guardian.co.uk/uk/2009/feb/25/personal-data-terrorism-surveillance
Tsiakis, T., and G. Stephanides, "The economic approach of information security", *Computers & Security*, Vol. 24, No. 2, 2005, pp. 105-108.
Van Den Hoven, Jeroen, „Information Technology, Privacy and Personal Data", in Jeroen Van Der Hoven, John Weckert (eds.), *Information technology and Moral Philosophy*, Cambridge University Press, Cambridge, 2008.
van Rooy, Dirk, and Jacques Bus, "Trust and privacy in the future internet—a research perspective", *Identity in the Information Society*, Vol. 3, 2010, pp. 397–404.
Virilio, Paul, *The Art of the Motor*, University of Minnesota Press, London, 1995.
Volkman, R., "Privacy as life, liberty, property", *Ethics and Information Technology*, Vol. 5, No. 4, 2003, pp. 199-210.
Vries, Katja de, Rocco Bellanova, Paul De Hert, and Serge Gutwirth, "The German Constitutional Court Judgement on data retention: proportionality overrides unlimited surveillance (doesn't it ?)", in Gutwirth, Serge, Yves Poullet et al. (eds.), *Privacy and data protection: an element of choice*, Springer, Heidelberg/Berlin, 2011, pp. 3-23.
Waldron, Jeremy, "Security and Liberty: The Image of Balance", *The Journal of Political Philosophy*, Vol. 11, No. 2, 2003, pp. 191-210. http://onlinelibrary.wiley.com/doi/10.1111/jopp.2003.11.issue-2/issuetoc
Warren, Samuel, and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5, 15 Dec 1890, pp. 193-220.
Westin, Alan, "Social and Political Dimensions of Privacy," *Journal of Social Issues*, Vol. 59 No. 2, 2003, pp. 431-453. http://www.blackwell-synergy.com/toc/josi/59/2
Westin, Alan, *Privacy and freedom*, Atheneum, New York, 1967.
Wright, David, Michael Friedewald, Serge Gutwirth, et al. (eds.), *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008.