Sci Eng Ethics (2014) 20:639–658
DOI 10.1007/s11948-013-9511-y

ORIGINAL PAPER

Protecting Human Health and Security in Digital Europe: How to Deal with the "Privacy Paradox"?

Isabell Büschel · Rostane Mehdi · Anne Cammilleri · Yousri Marzouki · Bernice Elger

Received: 13 July 2013 / Accepted: 28 December 2013 / Published online: 21 January 2014

Abstract This article is the result of an international research between law and ethics scholars from Universities in France and Switzerland, who have been closely collaborating with technical experts on the design and use of information and communication technologies in the fields of human health and security. The interdisciplinary approach is a unique feature and guarantees important new insights in the social, ethical and legal implications of these technologies for the individual and society as a whole. Its aim is to shed light on the tension between secrecy and transparency in the digital era. A special focus is put from the perspectives of psychology, medical ethics and European law on the contradiction between individuals' motivations for consented processing of personal

I. Büschel (✉) · B. Elger
Institute for Biomedical Ethics (IBMB), Universität Basel, Basel, Switzerland
e-mail: i.bueschel@unibas.ch
URL: http://ibmb.unibas.ch/

B. Elger
e-mail: b.elger@unibas.ch
URL: http://ibmb.unibas.ch

R. Mehdi
UMR CNRS 7318 Droits International, Comparé, Européen (DICE), Aix-Marseille University, Aix-en-Provence, France
e-mail: rostane.mehdi@univ-amu.fr
URL: http://www.ceric-aix.univ-cezanne.fr/

A. Cammilleri
Master 2 Sécurité et Défense, Intélligence Stratégique SE-DEFIS, Sciences Po, Rennes, France
e-mail: anne.cammilleri@sciencespo-rennes.fr
URL: http://www.ceric-aix.univ-cezanne.fr/

Y. Marzouki
Laboratoire de Psychologie Cognitive, CNRS, UMR 7290, Aix-Marseille University, Marseille, France
e-mail: yousri.marzouki@univ-amu.fr
URL: http://gsite.univ-provence.fr/gsite/document.php?pagendx=1031&project=lpc

data and their fears about unknown disclosure, transferal and sharing of personal data via information and communication technologies (named the "privacy paradox"). Potential benefits and harms for the individual and society resulting from the use of computers, mobile phones, the Internet and social media are being discussed. Furthermore, the authors point out the ethical and legal limitations inherent to the processing of personal data in a democratic society governed by the rule of law. Finally, they seek to demonstrate that the impact of information and communication technology use on the individuals' well-being, the latter being closely correlated with a high level of fundamental rights protection in Europe, is a promising feature of the socalled "e-democracy" as a new way to collectively attribute meaning to large-scale online actions, motivations and ideas.

Keywords Privacy · Information technology · Health · Security · Fundamental rights · Data protection · Democracy

The relationship between technology and humanity dates back to the beginning of human societies. Humans have been initiating technological change and inversely, technology has been shaping our behaviour, be it on the individual level or that of society. According to Strum and Latour (1999), it is precisely the use of materials and symbols that singles out human societies. For MacKenzie and Wajcman (1999), material resources "are part of what makes large-scale society feasible". Instead of being separate from society, they are constitutive of it. Indeed, information and communication technologies (ICT, European Commission 2001) such as telephones, computers and the Internet facilitate getting and staying connected in conformity with "everyone's fundamental right to communicate".[1] In relation with business activities, ICT ease the communication between economic operators and thus contribute to the development and functioning of markets. Because it increases "electronic gridlock" (European Commission 2010), technological progress may however bear certain risks. Indeed, P. Virilio recalls that it is impossible to disconnect technological progress from ignorance and accidents. According to this author, "inventing the ship amounts to inventing its sinking, inventing the train amounts to inventing its derailment, inventing the plane amounts to inventing its crash" (Gaudriault 2013). New developments in ICT undeniably offer benefits such as faster and more cost-efficient information sharing, including for purposes of human health and security, for example by enabling the delivery of more focussed, purposeful, and lean services, thus facilitating the "promotion of healthy lifestyles and independent living" (Rigby et al. 2013). Regarding individual health care, the use of ICT opens up the perspective "to keep the elderly and the disabled in their own homes rather than in the considerably more expensive hospital or nursing home systems" (OECD 2013). The European Union (EU)'s Early Warning and Response System aimed at fighting the spread of communicable diseases is an example of

[1] This right is being promoted by the International Telecommunications Union: http://www.itu.int/en/about/Pages/overview.aspx. Accessed 2 July 2013.

preventive public health measure. The link between human health and security with regard to ICT may be explained by the occasional correlation between health data and administrative and financial data (OECD 2013). In exceptional circumstances, the processing of such data may serve the investigation, through public bodies, on suspected persons involved in serious crimes, including acts of terrorism.

While offering benefits in terms of individual and public health and security, the use of ICT bears also threats for creeping intrusions into privacy. Hence, it may lead to enhanced vulnerability of individuals especially with regard to their relationship with powerful public and private bodies: the new privacy concerns may "range from modest risks to the privacy of activity data (like data collected by a pedometer) to safety-critical risks (like the integrity of software in an insulin pump)" (OECD 2013).

More generally, the reasons behind the increased vulnerability of individuals' privacy are threefold. First of all, the growing sophistication of ICT leads to more frequent and rapid processing of growing amounts of personal data (European Commission 2010)[2] considered as data enabling personal identification. Secondly, the increased vulnerability of a person with regard to the respect for his/her privacy is directly linked to the diversification of personal data, such as genomic data, laboratory data, diagnostic data, and image data (OECD 2013). Thirdly, vulnerability can be caused by the removal of three types of barriers to data processing: geographical (globalization enhancing the exchange of data for commercial purposes and the fight against international pandemics, terrorism, serious organised crime), operational (through increasing interoperability between ICT systems, Kierkegaard 2012),[3] and technological (through the fusion by multimedia of numerous transmission and expression forms of data and images, Banisar and Davies 1999). On the one hand, enhanced technological sophistication, data diversification and the progressive removal of obstacles to data processing give rise to new threats to privacy. These threats are new because they go beyond the traditional threats to "freedom from intrusion and surveillance" to cover "threats to personal autonomy and personal freedoms, including political freedoms—and […extend] to society at large" (European Commission 2010). On the other hand, social media such as Facebook, Twitter, Tumblr, etc. represent a new promising venue for promoting various societal changes for the better or the worse. Social media can enhance and have enhanced citizen and public empowerment through today's information technologies (IT). With respect to this idea, major social and political changes in the Internet era have largely benefited from online information sharing. Consequently, information privacy is at the heart of this new phenomenon.

Interestingly, the relationship between ICT and privacy reveals a "paradox"[4] in the sense that it combines contradictory features. More precisely, this relationship is

[2] Since the European Commission proposed the first Data Protection Directive in the 1990 s, "[t]he internet has moved out of the university lab into 56 % of European homes and 95 % of OECD businesses".

[3] For example, in the medical field "[i]nteroperability can be defined as the capability for independent and heterogenous health information systems to exchange health-related data for use by doctors, healthcare providers and patients".

[4] According to the Oxford Dictionaries, a "paradox" is "a person or thing that combines contradictory features or qualities": http://oxforddictionaries.com/definition/english/paradox?q=paradox. Accessed 2 July 2013.

characterized by a constant tension between secrecy and transparency. On the one hand, individuals fear threats to their personal autonomy and freedoms stemming from globalized data processing by governments and undertakings, while on the other hand they voluntarily proceed to the disclosure of personal data (e.g. by posting names, photographs, dates of birth, marital status on social networking sites, or medical data on health forums). We intend to shed light on this "privacy paradox" (Norberg et al. 2007; Kaplan 2012) and make suggestions from social, ethical and legal perspectives for dealing with it.

In clinical psychology and medicine, keeping secret one person's medical record, including data related to psychological symptoms, is a key to the therapist-patient confidential relationship (Brosset 2012). Without this safeguard, many persons will choose not to seek the services they need (OECD 2013). At the same time, disclosing medical data is essential for furthering scientific knowledge (e.g. in large-scale clinical research projects where huge amounts of medical data are collected, stored, transferred and analyzed). Even though medical data sharing responds to ethical requirements (e.g. avoid unnecessary repetition of collecting biological samples) and financial constraints, it is subject to limitations (e.g. Verdier-Büschel 2013). Indeed law, while creating the conditions for the development of technological progress (e.g. via the freedom to conduct a business, the right to protection of intellectual property), also limits the use of ICT (e.g. through the rights to protection of private life, and of personal data). Law thus has a double function: it provides support for the transformations of society induced by technological progress and at the same time shapes the latter through its inherent efficiency (Chevallier 1983; Cattan 2012).

Focussing on the study of human behaviour is the object of social sciences such as psychology and sociology. They provide methods that allow identifying the possible existence of links between certain kinds of technologies and specific expressions of human behaviour. In this respect, Beck (1992) argues that progress is not merely a process that happens to societies, but may (or should) become one that is actively and democratically shaped by them. The recent big changes fostered by the Web 2.0 mass communication tools, such as Facebook and Twitter represent a new milestone of the globalization process and for promoting democracy (e.g. Leighninger 2011). An outstanding example witnessed at the sunset of this IT era is the very fast and spectacular unfolding of events triggered by the first Arab spring wave of protest in Tunisia where the youth were given an unprecedented opportunity to spread revolutionary ideas and promote a highly self-organized movement, exclusively made possible by these new IT applications. A psychological study has shown that the use of ICT in the Arab spring movement has "revolutionize[d] revolutions" (Marzouki et al. 2012; Marzouki and Oullier 2012) in the sense that social media provided a tool for exercising political freedoms, public empowerment, and the fundamental right to free speech. Compared to former revolutions, the 2011 Arab revolutions stand as an illustration of political change brought about by the people despite of the absence of a strong leader guiding the movement. The reported study shows that ICT have replaced the role of a paternalistic leader and empowered citizens to fight for a democratic turn on their own by connecting through social media.

In a similar way, the use of ICT in the medical field empowers patients to self-monitor and manage chronic disease conditions (e.g. via recording blood glucose measurements, caloric intake, weight). So-called e-health applications furthermore enable patients to benefit in an effective manner from their right to free movement within Europe. The use of ICT in the medical field also empowers health care professionals to directly and effectively implement public health policy goals by contributing to guarantee an equal access to high-quality and safe health care services (e.g. by resorting to restricted availability of certain health care services in rural areas, Ferraud-Ciandet 2010; Büschel submitted; Fromson 2013), respond to the challenges of a growing demand in health care needs and help save costs linked to increasing health care spending.

In democratic societies, opinions diverge however as to the question whether the processing of personal data via ICT for the purposes of protecting human health and security is legitimate and which should be the legal rules governing it. This article is based on the assumption that the perception by citizens of the risks and opportunities of the processing of personal data reflects a "privacy paradox". Whereas in some circumstances, the disclosure of personal data seems to be accepted as being part of modern life (Hallinan et al. 2012), for example because it may provide individuals with benefits in terms of health and security protection,[5] it is less or not at all tolerated in other circumstances because it is perceived as a threat to privacy inspiring fear[6] (Hallinan et al. 2012). In fact, "[w]ith improved access to health information comes the increased risk of unauthorised access" (OECD 2013). Hallinan et al. (2012) showed in their meta-analysis of public opinion surveys based on a Europe wide sample population (i.e., Special Eurobarometer survey 359, Flash Eurobarometer survey 225, a survey of the Irish Data Protection Commissioner of 2008 and other studies and surveys) that citizens in Europe perceive personal data as not receiving the protection they deserve. They claimed that "an understanding of how the public understand and approach these issues is conspicuously lacking and often appears replaced by superficial assumptions as to what 'the public' want or need", thus leading to "an underevaluation of privacy as a social value". The authors explain that the lack of clarity regarding data processing feeds uncertainty, which in turn explains public fear regarding the consequences of data processing. They observed however that "[d]espite this, the public deterministically accept an increase in the release of data, simply as a necessity and consequence of life in the modern world". They concluded that citizens "are being forced to act in an environment they have little template for approaching".

The aim of this paper is to shed light on the way according to which different disciplines (psychology, medical ethics, European law) deal with the "privacy

[5] For example, medical data being registered on an electronic health insurance card might contribute to better health care performance, as it enables medical doctors, in case of life-threatening emergency, to find out without delay about allergies against drugs of the patient; another example is the registration of personal data of citizens of one country residing in another country with their embassy enabling them to be contacted in case of a major threat to public security.

[6] Citizens especially fear ID fraud and the use of information without knowledge, data sharing with third parties without having consented and, more generally, the use of data for purposes other than those consented for.

paradox". What we consider to be an important new insight is the fact that the privacy paradox is the result of a citizen empowerment process, that is the claim for, and recognition of an effective protection of persons' fundamental rights, including the right to dispose of one's own data. The shift towards enhanced personal autonomy is being boosted by technological advances, such as providing tools for real time monitoring of persons (e.g. personalized care, video-surveillance for purposes of crime prevention). As human health and security are fields that have been traditionally regulated by States in a "paternalistic" manner, new conflicts may arise over the control of personal data.

The Psychological Perspective

Previous studies in interpersonal psychology have shown that sharing a small amount of personal information within dyads of people promotes intimacy reciprocation and increases confidence (Shaffer et al. 1982). It was also revealed that the main predictor of such self-disclosure is the self-monitoring abilities toward other's expectations (Davis 1982). In the new Internet era, such as in blogging behaviours, some empirical studies revealed that self-disclosure is highly influenced by anonymity, self-awareness, and perceived audience size (Okdie 2011). Other studies on social networking platforms showed that choosing whether to disclose or keep secret personal data is a balancing act. A study on information disclosure and control on Facebook by adolescents and young adults shows that despite concerns for privacy induced by the disclosure of personal data, the survey population chose to disclose voluntarily personal data such as birthdays, e-mail addresses, profile pictures, pictures with friends, including pictures at parties (Christofies et al. 2009). The authors state that while Facebook provides an easy information sharing tool, it changes the nature of social relationships. Among the personality factors associated with online information control and disclosure, they identified the need for popularity, self-esteem, trust, as well as a general tendency to disclose. For the study population, "the need to be part of their social group and the need for popularity are key elements in their lives" (Christofies et al. 2009). While stating that different psychological factors are involved in the control and disclosure of personal data, the authors claim that more research is needed especially for explaining what factors lead to control the release of such data (Norberg et al. 2007; Christofies et al. 2009).

Another study shows that views about the use of electronic health records differ according to personal circumstances, such as health status, age, socioeconomic factors, healthcare experiences, specific purpose of the use of the data contained in the electronic health record. For example, while UK adults and young people have expressed concerns about privacy, security, as well as control over access, use and misuse of personal data, they were in favour of using them for public health research and surveillance related to cancer (Luchenski et al. 2012).

A study on the use of mobile phones for increasing mental health and human well-being (mHealth) shows that mobile phone applications specifically associated with behavioural health including "developmental disorders, cognitive disorders, substance-related disorders as well as psychotic and mood disorders" respond to the

shortcomings of conventional assessment procedures, namely difficulties in gathering information from the individual subject during the day (Luchenski et al. 2012). The authors argue that "since the phone is an integrated part of both the individual and the social life", self-monitoring applications allow researchers to record behavioural data in a discrete manner and in real time. For example, *T2 Mood Tracker* is an application which enables patients to self-monitor emotional experiences associated with behavioural health issues like post-traumatic stress, brain injury, life stress, depression, anxiety. However, as Boyce (2012) has pointed out recently, evidence of the effectiveness of such cyberpsychological tools for improving individual health and well-being is still limited. A clinical advisor to diabetes UK has nonetheless stressed that the ability to share peoples' feelings was encouraging to them and that social media were used by patients to get moral support from their peers when they weren't doing so well (Boyce 2012). A major challenge and real threat to the individual's privacy lies in the risk of leaking personal data. In this respect, the use of ICT in the fields of health and security opens up "new vulnerabilities to patients and medical facilities" (Luchenski et al. 2012).

The Medical–Ethical Perspective

In many European health care systems we observe a transition from paper-based to electronic handling of patient records. This technological shift consisting of digitalizing medical data is aimed at improving health care, reducing fraud, reducing medical errors, and saving lives (Mordini and Ottolini 2007; Ferraud-Ciandet 2011; Büschel submitted). Indeed, the quality of health care services may be improved through the tele-monitoring of epidemiological data, seeking expert advice and collaborating on certain medical acts despite of geographical distance. One of the risks for privacy related to this practice consists in fraud about the medical identity of a person. It may however be prevented through genetic fingerprints. Biometric identification may help eliminate or drastically reduce medical errors due to patient misidentification and wrong administration of medication, and save lives in cases of emergency (natural disasters, transportation accidents, acts of terrorism and other mass destruction events). The European Union, "as a political, historical and ethical project, […] endeavours to bring together countries which share and together promote common values, such as […] fundamental rights" (European Parliament 2013). The protection and promotion of these values is strengthened by the instruments adopted and activities carried out under the auspices of the Council of Europe. Therefore, when processing medical data in Europe, fundamental rights and ethical principles such as autonomy and non-discrimination must be observed. Indeed, it should be guaranteed that patients whose data are being processed have given express, free and informed consent. This requirement is specifically critical with regard to minors and patients suffering from mental disabilities. For example, in the context of the Swiss law pre-project on electronic patient records discussions are ongoing about how much autonomy should be given to patients to restrict emergency information release that is in their own interest. The underlying idea is that patient information that is important in a

medical emergency should be accessible by all doctors while other information that is not relevant, for example the fact that the patient is undergoing psychotherapy, is more strictly protected. While it is certainly easier to set a default mechanism about which information should be included in the accessible emergency package, patients could and probably should in addition be asked whether they agree to it and ask for the hiding part of the emergency information. There could be a paternalistic justification not to allow patients to restrict accessibility of emergency information if that will harm them. Even more important in a pluralistic society governed by the harm principle (Mill 1860) are arguments that refer to the fact that patients who hide emergency information could cause harm to the health care system since expensive tests would need to be repeated by doctors although results might have already been available in the electronic records, and time would be lost in the diagnostic and therapeutic process, for example Intensive Care Unit (ICU) beds might be occupied longer than necessary which could harm other patients that are waiting for an ICU bed. While it is is important to protect privacy rights, new technologies create situations where more discussion is needed concerning limits to individual freedoms based on possible harm to others or society.

Furthermore, according to the principle of non-discrimination, "[s]ystems should be designed so that as many people as possible can use them effectively with the minimum of discomfort. Particular attention should be […] paid to avoid any discrimination against ageing […and] patients who cannot provide, permanently or temporarily, the requisite biometric characteristics" (e.g. impossibility to provide fingerprints if the skin is burned, Mordini and Ottolini 2007).

The European Law Perspective

Law in general, and European law in particular—due to ambitious fundamental rights protection instruments,[7] strong Constitutional traditions in the field of data protection (European Commission 2010) and efficient control mechanisms (Mehdi 2012)—has an important role to play in the protection of the individual against breaches of his/her fundamental rights stemming from privacy-intrusive technologies. This is especially true since the revision of the Lisbon Treaty conferring a binding character on the closely related rights to the respect for private and family life and to the protection of personal data (Art. 7 and 8 of the Charter of Fundamental Rights of the EU, European Court of Justice 2010, 2011) and providing for a specific legal basis for adopting privacy laws independently from internal market aspects (Art. 16 Treaty on the Functioning of the EU).

In order to safeguard individual privacy, European law—which prevails over national laws—prohibits the processing of personal data unless the data subject has given his/her express, free and informed consent. However, whether data subjects will give their consent or not depends on their perception of ICT and the trust they

[7] To quote only the most frequently invoked instruments: European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Treaty on the European Union, Treaty on the Functioning of the European Union, Charter of Fundamental Rights of the European Union.

place in the safety of the data processing process. Inversely, the privacy-respecting or -intrusive impact of ICT influences the well-being of the individual (BVerfG 2010),[8] as well as the exercise of political rights by civil society (Marzouki et al. 2012; Marzouki and Oullier 2012). Indeed, in its *Census*-judgment, the German Constitutional Court decided that depriving citizens of knowing "who knows what when about [them] and in which situation […]" and thus, restricting the exercise of their right to informational self-determination "would not only limit the possibilities for personal development of the individual, but also the common good, because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizens" (BVerfG 1983; European Commission 2010). Nyst (2013), Head of International Advocacy at Privacy International, has put the idea in these terms: "privacy is the fundamental barrier that stands in the way of complete State control and domination. […] A citizenry unable to form or communicate private thoughts without the interference of the State will not only be deprived of their right to privacy, they will be deprived of their human dignity". The more citizens are aware about the risks for privacy induced by ICT, the more likely it is that their autonomy is respected and the more effectively their fundamental rights to privacy and data protection are being guaranteed. Under European law, however, the rights to respect for private life and to the protection of personal data are not absolute rights. They must be considered in relation to their function in society (see, for example, the judgments of the European Court of Justice in joint cases *Volker und Markus Schecke and Eifert*, C-92/09 and 93/09, para. 48 and *Deutsche Telekom*, C-543/09, para. 51). According to Art. 52(1) of the Charter of Fundamental Rights of the European Union, the exercise of those rights may be limited, "so long as those limitations are provided for by law, respect the essence of those rights, and, in accordance with the principle of proportionality, are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others" (judgment of the European Court of Justice in the case of *Michael Schwarz v. Stadt Bochum* of October 17th 2013, C-291/12, para. 34).

We chose two concrete examples, electronic prescriptions and passenger name record data to illustrate the privacy paradox in the fields of human health and security and the challenges they pose from the European law perspective.

Processing of Data for Human Health Protection

Health-related data being closely linked to the most intimate elements of the private sphere, that is, a person's body and mind, the processing without prior consent of data concerning individuals' health is in principle prohibited. However, exceptions to this rule may be justified according to Art. 8 para. 3 of Directive 95/46/EC if "required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those

[8] The German Federal Constitutional Court established the link between "the storage of telecommunications traffic data without occasion" and its impact on individual well-being by stating that it "is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas" at para. 212 of this decision.

data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy". Furthermore, the processing of personal data by Member States may be authorized if it is related to an "event posing a health threat, […or] to the health conditions of […] infected persons and of persons potentially exposed to contamination […] within the [Early Warning and Response System]" (European Commission 2012: para. 4). It has been shown elsewhere that ICT provide tools capable of "improv[ing] disease prevention, diagnosis and treatment, facilitat[ing] patient safety and improv[ing] health systems' coordination, us[age] of resources and sustainability and reduc[ing] waiting times and errors" (e.g., Kierkegaard 2012). Expectations towards the use of electronic prescriptions across Europe for improving the quality of health care are high. By enabling a prescriber to send an "accurate, error-free and understandable prescription directly to a pharmacy", but also nurses to administer medicines and pharmacies to review orders and manage the supply of medicines electronically, e-prescriptions are considered to constitute tools that contribute to the development of new higher quality and more cost-efficient health care models. However, by multiplying access points to the medical data of patients (e.g. concerning a specific condition or treatment), the risk for privacy breaches and medical identity theft becomes higher (Joh 2011; Kierkegaard 2012). Possible consequences of medical identity theft may consist in patients receiving the wrong medication, finding their health insurance exhausted, and failing physical exams for employment due to the wrongful presence of diseases in their health record (Mordini and Ottolini 2007). Another concern highlighted by Quinn et al. (2013) is that mHealth services require users to consent on a much more regular basis than needed for conventional medical services, which "may entail a reduction in the attention patients give to such requests".

In order to be compatible with the high standard of fundamental rights protection in Europe, it is important for European laws to provide appropriate safeguards, such as effective mechanisms for controlling the respect data protection principles such as purpose-limitation, necessity and proportionality. With this regard, accountability and liability mechanisms making it possible to obtain compensation for damages caused by data leakage create incentives for guaranteeing the highest possible security level, thus fostering trust in the processing of data.

Processing of Data for Reasons of Public Security

In reaction to the terrorist attacks of 11th September, the United States (US) enacted a new legislation concerning the processing of travellers' data. It obliges air carriers operating flights to or from the US or across US territory to provide the US Bureau of Customs and Border Protection with an electronic access to the data contained in their reservation and departure control systems (so-called "Passenger Name Records" or "PNR data"). Because this legislation also covers data collected by airlines subject to EU law operating flights to or from the US, the question arises as to whether its privacy-intrusive character was compatible with EU data protection rules. What turned out to be particularly problematic is the use, by a US State

authority, for the purposes of public security protection, of data collected by airlines in the course of their commercial activity. Indeed, according to European law, the processing of data for other purposes than those for which they have initially been collected, as it risks violating the fundamental rights to privacy and data protection, is in principle prohibited. However, exceptions to violations of fundamental rights may be justified for reasons of overriding general interest such as the protection of public security, given the respect of procedural safeguards (Labayle and Mehdi 2009). This means that for personal data processing to be legal, a balance needs to be struck between the fundamental rights to privacy and data protection and overriding reasons of individual or general interest. Striking a balance between privacy and security requires reaching a fair distribution of control over personal data. 'Fairness' in this context means that the control over his/her own data must lie with the data subject, unless the sharing of these data is justified by overriding reasons of general interest such as, for example, the investigation and prosecution of terrorist offences and serious crime. In order to be able to keep control over one's personal data, European data protection principles require that each individual whose personal data are being processed be recognized with the rights of access to his or her personal data, as well as the rights of rectification, erasure or blocking of such data (see *infra*).

Following the annulment, on 30th May 2006, by the European Court of Justice, of the Council Decision 2004/496/EC of 17th May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers, new Agreements have been negotiated between the EU and the US, the EU and Canada and the EU and Australia. With respect to the free movement of persons within the Schengen Area, the European Commission adopted a Proposal for a Directive of the Council and the European Parliament on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime of February 2, 2011 providing that PNR data of aircraft passengers may be transferred by air carriers to Passenger Information Units (PIUs) of the Member States (European Commission 2011d). PIUs are national authorities responsible for collecting PNR data from the air carriers, storing them, processing and transmitting them or the result of the processing to other authorities entitled to request or receive such data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. The Proposal provides that Member States ensure that air carriers inform passengers taking flights in a clear and precise manner about the transmission of PNR data to the PIU, "the purposes of their processing, the period of data retention, their possible use to prevent, detect, investigate or prosecute terrorist offences and serious crime, the possibility of exchanging and sharing such data and their data protection rights, in particular the right to complain" (Art. 11, para. 5). In respect of all processing of PNR data pursuant to this directive, it is foreseen that "every passenger shall have the same right to access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress" (Art. 11, para. 1 of the Proposal). Recently however, the European Parliament rejected the proposal for a European PNR system (Peyrou 2013), arguing that evidence was lacking for the effectiveness of collecting PNR data in the fight

against terrorism. Indeed, as the Boston marathon and Merah case in France have shown, the fact that law enforcement authorities had been disposing of data of the responsible persons was not sufficient for preventing or avoiding the attacks against public security. Furthermore, both the European Parliament and European Data Protection Supervisor expressed concerns as to the transparency and proportionality of the proposed measures (Marx 2013).

Opaqueness, jurisprudential instability and weak efficacy of privacy-protecting rules are detrimental to legal certainty. In a democratic society governed by the rule of law, they challenge the requirement of law to be predictable. The quest must therefore be one for privacy protection rules which are transparent, which benefit from judicial guarantees and which are user-friendly.

Jurisprudential Instability Due to a Case-Based Balancing Between Conflicting Rights and Values

While national and European authorities enjoy a wide margin of appreciation for defining health and security policies, it is required in a democratic society governed by the rule of law that exceptions to any legal rule or principle justified by the general interest be foreseen by law and are necessary, proportional and subject to judicial control (e.g., Cammilleri-Subrenat et al. 2012; Verdier-Büschel and Prouvèze 2011). In the *Leander v. Sweden* case, the European Court of Human Rights (1987) stated that "in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse". While this Court confirmed in *Z. v. Finland* (1997) that the protection of medical data is fundamental to a person's enjoyment of his/her right to private life according to Art. 8 of the ECHR, it accepted at the same time that "the interests of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest in investigation and prosecution of crime and in the publicity of court proceedings […], where such interests are shown to be of even greater importance". In the present case, the applicant's health data related to her infection with HIV had been seized at hospital by the police in the framework of investigations being carried out about the applicant's ex-husband, who was accused of attempted manslaughter through rapes, by which he was supposed to have deliberately subjected his victims to a risk of HIV infection. The European Court of Human Rights considered that the "seizure of the applicant's medical records and their inclusion in the investigation file were supported by relevant and sufficient reasons, the weight of which was such as to override the applicant's interest in the information in question not being communicated". More precisely, they served to determine when the husband of the applicant, who refused to give evidence against the latter, had become aware of his HIV infection, as indeed knowledge about the date of infection was crucial for the determination of the penalty. Under these specific circumstances, the Court considered that the measures were proportionate to the legitimate aims pursued. In the *S. and Marper v. United Kingdom* case however, the European Court of Human Rights (2008) decided that the retention for an

unlimited period of time of fingerprint and DNA information in a nationwide database for criminal-identification purposes constituted a disproportionate interference with the right to respect for private life of the applicants, which could not be regarded as necessary in a democratic society. Recently, the question arose before the Luxemburg-based European Court of Justice whether taking fingerprints and storing them in passports constitutes a threat to the rights to respect for private life and the protection of personal data. As fingerprints contain unique information about individuals allowing them to be identified with precision, they constitute personal data. Subsequently, the Court decided that the taking and storing of fingerprints by national authorities constitutes a threat to respect for private life and the protection of personal data. However, it considered that this threat is being justified by an objective pursued by Council Regulation (EC) No 2252/2004 (especially Art. 1(2) read in the light of recitals 2 and 3), which it recognized as being of general interest: preventing the fraudulent use of passports and consequently, illegal entry into the European Union. Indeed, the Court considered that the taking and storing of fingerprints when issuing passports is necessary and appropriate for preventing the falsification of passports and the fraudulent use thereof and, "by extension, […] illegal entry to the European Union" (para. 45). When examining the proportionality of the relevant provision which provides for passports and travel documents to include fingerprints in interoperable formats, the Court stressed that it "does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone" (para. 60). Excluding the centralized storage of data or the use of such data "for purposes other than that of preventing illegal entry into the European Union" (para. 61), it concluded that it is a proportionate measure.

Intrusion into privacy for reasons of public security would be completely "off-limit" for all times under all circumstances when they are not foreseen by law and/or are disproportionate. One could imagine the processing of personal data such as fingerprints in order to investigate on a minor offence, e.g. for tagging or bicycle theft.

Another hurdle to the efficacy of privacy-protecting rules is the balance between technical precision and the requirement of legal rules to be general enough to cover future technological innovations.

A risk for the Efficacy of Privacy-Protecting Rules

With regard to the increasing sophistication of ICT, the legal rules governing privacy protection risk to become the prerogative of a select band of insiders with the consequence of jeopardising legal efficacy (Mehdi 2012). Indeed, the "performance" and quality of law might be affected in the sense that there risks to be a mismatch between the objective of privacy-protective legal rules and their effective implementation. Such an asymmetry might be the result on the one hand, of the lack of indispensable technical knowledge for applying correctly these rules and on the other hand, the necessity for the law to provide for privacy-protective rules which are general enough to cover the widest possible range of rapidly evolving technological innovations. In order to enhance the efficacy of privacy-

protective rules, the EU developed impact assessment and evaluation mechanisms, and has been introducing experts and the public to the legislative process. In its 2011 Strategy for a Corporate Social Responsibility, the European Commission put forward "the responsibility of enterprises for their impacts on society". To fully meet their social responsibility, enterprises "should have in place a process to integrate social, environmental, ethical human rights and consumer concerns into their business operations and core strategy in close collaboration with their stakeholders" (European Commission 2011c). Protecting the individual against illegal processing of personal data should indeed not only be a duty of public authorities, but also of private companies and citizens. The three main features of such a general social responsibility are highlighted in the Proposal for a Charter of Human Responsibilities. This Charter is supposed to constitute a third ethical pillar common to all societies and social spheres completing the two existing pillars which are the Universal Declaration of Human Rights and the Charter of the United Nations (Calame 2003: 99). According to this Charter, responsibility comprises "accepting responsibility for the direct and indirect consequences of our actions; uniting with one another to escape from powerlessness; acknowledging that our responsibility is proportional to the knowledge and power which each of us holds". In the light of this Charter, the exercise of any power is only legitimate "where it serves the common good, and if it is accountable to those over whom it is exercised". Even though the principles contained in the Charter are not binding, we suggest that with regard to the distribution of power on the internet through the detention of digital data (e.g. by undertakings referred to as "GAFAM" for Google, Apple, Facebook, Amazon, Microsoft, but also by individual internet users), they could guide the exercise of responsibilities in a way that more access to information, knowledge and power strengthens the duty to account for data processing.

When surveilling his/her neighbours, the individual should be respectful of their fundamental right to privacy. The intensity of surveillance and thus, risk of intrusion into private life, must be in relation to the severity of the harm which one aims to prevent through surveillance. Judges—if being seized—are in a position to guarantee the effectiveness of the protection of the rights to privacy and personal data by sanctioning unjustified violations of these rights. However, technical hurdles subsist concerning the judicial control of the identity of a data subject on the Internet (especially with regard to age and capacity to give express, free and informed consent), but also concerning interoperability due to different technical standards, as well as the lack of transparency with regard to responsibility allocation between operators of websites and individuals (e.g. the right to erasure and blocking of data, European Court of Justice Opinion of Advocate General Jääskinen 2013 and, more generally, questions related to cloud computing, Peyrou 2013).

Solutions Provided by Law for Dealing with the "Privacy Paradox"

Law offers two solutions for dealing with the "privacy paradox": regulating the design of technology collecting data and the control over the data obtained. Technically, it is possible to achieve at the same time a high standard of privacy protection and a high level of human health and security through the adoption of an integrated approach

(application of the principle of "privacy by design", EDPS 2010; Cammilleri-Subrenat et al. 2012; Cammilleri-Subrenat 2012), that is the development of "privacy enhancing technologies" (PET). Until now, there seem to exist only very few practical examples of PET, mainly due to the costs and restricted possibilities for exploitation of processed data in conformity with a high level of privacy protection (see also Baeriswyl and Rudin 2012). As an example of PET, taking photographs through active imagery—which is a discrete technology using invisible laser light—has to be compatible with health and privacy protection rules. The latter was the key feature of the "IAAIS"-project, which was financed by the French National Research Agency and included representatives of the State Department, Department of Defence and Department of Justice, as well as industrial partners, among which Sagem. Engineers, stakeholders and lawyers have been closely collaborating for 24 months in order to implement the principle of privacy by design, which means to integrate the requirements of protecting privacy and personal data from the earliest phase of design on throughout the whole technological elaboration process. Another example for the application of the privacy by design principle concerns security scanners at airports, which gave rise to concerns about the protection of diverse fundamental rights such as privacy and data protection, but also human dignity and health. Following a European Parliament resolution adopted in response to the proposal for introducing such scanners on the list of eligible methods and technologies for screening persons, the European Commission launched a public consultation and carried out an impact assessment. The legislation, finally adopted in 2011, grants leeway to Member States and/or airports as to the mandatory or optional use of security scanners and prohibits the storage, retainment, copying, printing or retrieval of images, as well as unauthorised access to and use of the obtained images (European Commission 2011a, b). Furthermore, it grants passengers the right to opt out from being subject to security scanners in favour of an alternative screening method (European Commission Scientific Committee on Emerging and Newly Identified Health Risks SCENIHR 2012).

Additionally to promoting PET design, and with regard to the "dramatic expansion of secret and unaccountable surveillance, as well as the growing collaboration between governments and vendors of surveillance technology that establish new forms of social control" (recital 6 of the Madrid Privacy Declaration, 2009), the EU seeks to strengthen transparency, accountability and security. The European Union addresses these issues through the adoption, among other instruments, of a strategy which clarifies the principles that should guide cybersecurity policy in the EU and internationally (European Commission and High Representative for the European Union for Foreign Affairs and Security Policy Joint Communication 2013). At 2.5, the Joint Communication declares that "the EU international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights". Among other measures, this implies the development of new public guidelines on freedom of expression online and offline, monitoring the export of products or services that might be used for censorship or mass surveillance online, the development of measures and tools to expand Internet access, openness and resilience to address censorship or mass surveillance by communication technology.

Within the ongoing EU Data Protection reform, it is planned to generalize the obligation according to which data breaches have to be notified. Indeed, inspired by the personal data breach notification in Article 4(3) of the e-Privacy Directive 2002/58/EC, Articles 31 and 32 of the Commission Proposal for a Data Protection Regulation of January 25 2012, and Articles 28 and 29 of the Commission Proposal for a Data Protection Directive for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data introduce an obligation to notify personal data breaches. In exceptional circumstances, the obligation to notify may be delayed, restricted or omitted. This may be the case if Member States have adopted legislative measures allowing the partial or complete retention of data when this "constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned. For example, (a) to avoid obstructing official or legal inquiries, investigations or procedures; (b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties; (c) to protect public security; (d) to protect national security; (e) to protect the rights and freedoms of others" (Art. 11, para. 4 of the Proposal for a Data Protection Directive; see also Art. 3, para. 5 of Commission Regulation (EU) No 611/2013). Furthermore, "[t]he communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the personal data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it" (Art. 29, para. 3 of the Proposal for a Data Protection Directive; see also Art. 4 of Commission Regulation (EU) No 611/2013).

According to point 5 of the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, "Member States should ensure that operators, together with national competent authorities and civil society organisations, develop new schemes, or apply existing schemes, such as certification or operator self-assessment, in order to demonstrate that an appropriate level of information security and protection of privacy is established in relation to the assessed risks" (European Commission 2009). Whereas this Recommendation has no binding legal effect, the Draft EU Data Protection Regulation of January 2012 provides for a binding impact assessment to be carried out in cases where "processing operations present specific risks to the rights and freedoms of data subjects" (Art. 33 § 1).[9]

[9] Among these specific risks, Art. 33 § 2 lists namely the following: "(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale; (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale; (d) personal data in large scale filing systems on children, genetic data or biometric data; (e)….".

In the currently discussed version of the Proposal for the Regulation, such impact assessments are mandatory. Supervisory authorities are empowered to impose administrative sanctions in case of failure to carry them out.

In order to ensure an effective application of fundamental rights, it is important to provide for the legal framework—including "widely accepted privacy and security standards for personal data collection, analysis and use" (OECD 2013)—as well as judicial remedies (Art. 47 Charter of Fundamental Rights of the EU). With this respect, the Draft EU Data Protection Regulation adopts an approach similar to the one which characterizes European consumer protection regulations, in the sense that it is person-centred. In the field of data protection, this approach is captured by mandatory provisions such as the obligation to obtain informed consent, the rights to revoke, to be forgotten and to ask for personal data to be erased (Kilian 2012). Furthermore, within the ongoing data protection reform, exportation of personal data to another service provider will be facilitated. However, legal guarantees are not sufficient on their own: "equal thoroughness must be given to the development of quality assurance, monitoring of use, identification of potential adverse outcomes or intentional abuses, constructive reporting and analysis of incidents and events, and creation of appropriate controls, mechanisms and regulation" (OECD 2013).

In conclusion, there is no denial that interdisciplinary collaborations taking account of the social, ethical and legal impacts of ICT on human health and security are the *sine qua non* condition for the respect and promotion of individuals' well-being. Closely correlated to a high level of fundamental rights protection, the latter is a promising feature of the so-called "e-democracy" as a new way to collectively attribute meaning to large-scale online actions, motivations and ideas. In order to support better practices and build trust in ICT, more research needs to be done about access controls and audit, encryption, mobile health, as well as identification and authentification (OECD 2013). The added value of this paper consists in bridging an existing theoretical gap, namely adopting a transdisciplinary approach to the "privacy paradox" aimed at furthering the understanding of the phenomenon in order to enable the adoption of a holistic view in future design of ICT and regulation of their use in the fields of human health and security, for better compliance with fundamental rights.

References

Baeriswyl, B. & Rudin, B. (2012). Privacy enhancing technologies (PET) versprechen (zu) viel bei der Umsetzung von neuen Technologien. *digma—Zeitschrift für Datenrecht und Informationssicherheit* (pp. 18–21).

Banisar, D., & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection and surveillance laws and developments. *John Marshall Journal of Computer & Information Law, 18*, 1–98.

Beck, U. (1992). *Risk society: Towards a new modernity*. London: Sage.

Boyce, N. (2012). Maps, apps, and evidence? *The Lancet, 379*(9833), 2231.

Brosset, E. (2012). Brèves observation sur un secret de Polichinelle: l'influence du droit européen sur le droit médical à travers l'exemple du secret médical. In Leca (A.), *Le secret médical,* Cahiers du Sud-Est de droit de la santé, Les études hospitalières.

Büschel, I. (submitted). Télémédecine et droit de l'Union européenne: remède, opportunité, défi. *Journal International de Bioéthique*.

BVerfGE, 1 BvR 256/08, Decision of 2.3.2010 ("Vorratsdatenspeicherung"). http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html. Accessed January 6, 2013.

BVerfGE 65, 1, 44, Decision of 15.12.1983 ("Volkszählung").

Calame, P. (2003). Tools for social and economic responsibility: The charter of human responsibilities. In Council of Europe (2003). Civil society and new social responsibilities based on ethical foundations. http://www.coe.int/t/dg3/socialpolicies/socialcohesiondev/source/trends/trends-07_en.pdf. Accessed November 4, 2013.

Cammilleri-Subrenat, A. (2012). Le privacy by design confronté à la disparition des piliers du Traité de Lisbonne. http://www.ceric-aix.univ-cezanne.fr/fileadmin/CERIC/Documents/manifestations_scientifiques/AnnexeManifestations/Atelier_PbD_23_MarsFin_En_.pdf. Accessed June 28, 2013.

Cammilleri-Subrenat, A., Prouvèze, R., & Verdier-Büschel, I. (2012). *Nouvelles technologies et défis du droit en Europe—L'imagerie active au service de la sécurité globale*. Bruxelles: Bruylant.

Cattan, J. (2012). *Le droit et les communications électroniques*. Ph.D. dissertation, under the supervision of Prof. H. Isar and R. Mehdi, Law School, University Aix-Marseille.

Chevallier, J. (1983). L'ordre juridique. In CURAPP, *Le droit en procès* (p. 34). Paris: PUF.

Christofies, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyber Psychology & Behavior, 12*(3), 341–345.

Council of the European Union Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, 29.12.2004, pp. 1–6.

Davis, D. (1982). Determinants of responsiveness in dyadic interaction. In W. Ickes & E. S. Knowles (Eds.), *Personality, roles, and social behavior* (pp. 85–139). New York: Springer-Verlag.

EDPS (2010). Opinion on promoting trust in the information society by fostering data protection and privacy. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf. Accessed January 24, 2012.

European Commission (2001). Communication to the Council and the European Parliament: Information and communication technologies in development—The role of ICTs in EC development policy, COM (2001) 770 final. http://ec.europa.eu/development/icenter/repository/com2001_0770en01_en.pdf. Accessed July 14, 2013.

European Commission (2009). Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (notified under document number C(2009) 3200), OJ L 122, 16.5.2009, pp. 47–51.

European Commission (2010). *Comparative Study on different approaches to new privacy challenges in particular in the light of technological developments*. http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf. Accessed July 3, 2013.

European Commission (2011a). Implementing Regulation (EU) No 1147/2011 of 11 November 2011 amending Regulation (EU) No 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports, OJ L 294, 12.11.2011, pp. 7–11.

European Commission (2011b). Regulation (EU) No 1141/2011 of 10 November 2011 amending Regulation (EC) No 272/2009 supplementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports, OJ L 293, 11.11.2011, pp. 22–23.

European Commission (2011c). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A renewed EU strategy 2011–2014 for Corporate Social Responsibility, COM(2011) 681 final.

European Commission (2011d). Proposal of 2 February 2011 for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final.

European Commission (2012). Recommendation of 6 February 2012 on data protection guidelines for the Early Warning and Response System (EWRS) (2012/73/EU).

European Commission and High Representative for the European Union for Foreign Affairs and Security Policy (2013). Joint Communication to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Brussels, 7.2.2013, JOIN (2013) 1 final, 20 p.

European Commission Scientific Committee on Emerging and Newly Identified Health Risks SCENIHR (2012). Health effects of security scanners for passenger screening (based on X-ray technology). http://ec.europa.eu/health/scientific_committees/emerging/docs/scenihr_o_036.pdf. Accessed July 11, 2013.

European Court of Human Rights, *Leander v. Sweden*, judgment of 26 March 1987, application no. 9248/81.

European Court of Human Rights, *S. and Marper v. United Kingdom*, judgment of 4 December 2008, application nos. 30562/04 and 30566/04.

European Court of Human Rights, *Z. v. Finland*, judgment of 25 February 1997, application no. 22009/93.

European Court of Justice (2010). Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, Joined Cases C-92/09 and C-93/09. *European Court Reports* 2010 Page I-11063.

European Court of Justice, Judgment of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado*, Joined cases C-468/10 and C-469/10. Not yet published in the *European Court Reports.*

European Court of Justice, Opinion of Advocate General Jääskinen delivered on 25 June 2013, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12. Not yet published in the *European Court Reports.*

European Court of Justice (2013). Opinion of Advocate General Mengozzi delivered on 13 June 2013, *Michael Schwarz c. Stadt Bochum*, Case C-291/12. Not yet published in the *European Court Reports.*

European Parliament (2013). Draft Report on the situation of fundamental rights in the European Union (2012) (2013/2078(INI)) of 18.9.2013, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Louis Michel.

Ferraud-Ciandet, N. (2010). L'Union européenne et la télésanté. *Revue Trimestrielle de Droit Européen, 46*(3), 537–561.

Ferraud-Ciandet, N. (2011). *Droit de la télésanté et de la télémédecine*. Paris: Heures de France.

Fromson, J. A. (2013). Telemedicine: Changing the landscape of rural physician practice. *NEJM Career Center*. Accessed June 25, 2013.

Gaudriault, C. (2013). Interview with Paul Virilio "Inventer l'avion, c'est inventer le crash…". http://www.zigzag-blog.com/spip.php?page=article&id_article=4. Accessed July 3, 2013.

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review, 28*, 263–272.

Joh, E. E. (2011). Ethics watch—DNA theft: Your genetic information at risk. *Nature Reviews Genetics,*. doi:10.1038/nrg3113.

Kaplan, D. (2012). Vie privée à l'horizon 2020. In CNIL, *Cahiers Innovation et prospective*, (Vol. 1, pp. 36–37). http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/Cahier-ip/cnil_cahieripn1/index.html. Accessed July 2, 2013.

Kierkegaard, P. (2012). E-prescription across Europe. *Health and Technology,*. doi:10.1007/s12553-012-0037-0.

Kilian, W. (2012). Personal data: The impact of emerging trends in the information society—how the marketability of personal data should affect the concept of data protection law. *CRi, 6*, 169–175.

Labayle, H., & Mehdi, R. (2009). Le contrôle juridictionnel de la lutte contre le terrorisme: les 'black lists' de l'Union dans le prétoire de la Cour de justice. *Revue Trimestrielle de Droit Européen, 45*(2), 231–265.

Leighninger, M. (2011). Citizenship and governance in a wild, wired world: How should citizens and public managers use online tools to improve democracy? *National Civic Review, 100*, 20–29.

Luchenski, S., Balasanthiran, S., Marston, C., Sasaki, K., Majeed, A., Bell, D., et al. (2012). Survey of patient and public perceptions of electronic health records for healthcare, policy and research: Study protocol. *BMC Medical Informatics and Decision Making,*. doi:10.1186/1472-6947-12-40.

Mackenzie, D., & Wajcman, J. (1999). *The social shaping of technology* (2nd ed., pp. 3–27). Philadelphia: Open University Press.

Madrid Privacy Declaration of 3 November 2009, signed at the annual meeting of the Privacy and Data Protection Commissioners' conference by more than 100 civil society organizations and privacy experts. http://thepublicvoice.org/TheMadridPrivacyDeclaration.pdf. Accessed November 4, 2013.

Marx, M. (2013). The EP Committee rejects the proposal for a European Passenger Name Record System (PNR). http://eafsj.org/2013/05/01/the-ep-committee-rejects-the-proposal-for-an-european-passanger-name-record-system-pnr/. Accessed July 11, 2013.

Marzouki, Y. & Oullier, O. (2012, July 17). Revolutionizing revolutions: Virtual collective consciousness and the Arab Spring. *The Huffington Post US*. http://www.huffingtonpost.com/yousri-marzouki/revolutionizing-revolutio_b_1679181.html. Accessed July 2, 2013.

Marzouki, Y., Skandrani-Marzouki, I., Béjaoui, M., Hammoudi, H., & Bellaj, T. (2012). The contribution of Facebook to the 2011 Tunisian revolution: A cyberpsychological insight. *Cyberpsychology, Behavior, and Social Networking, 15*(5), 237–244.

Mehdi, R. (2012). L'efficacité de la norme en droit de l'Union européenne. In Fatin-Rouge Stefanini, M., Gay, L., Vidal-Naquet, A. (Eds.), *L'efficacité de la norme juridique: nouveau vecteur de légitimité ?* (pp. 295–331). Bruxelles: Bruylant.

Mill, J. S. (1860). *On liberty* (Vol. 25). Harvard: Harvard Classics.

Mordini, E., & Ottolini, C. (2007). Body identification, biometrics and medicine: Ethical and social considerations. *Ann Ist Super Sanità, 43*(1), 51–60.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*, 100–126.

Nyst, C. (2013). Two sides of the same coin: The right to privacy and freedom of expression (English version of an article in the September issue of Cuestión de Derechos). https://www.privacyinternational.org/opinion-pieces/two-sides-of-the-same-coin-the-right-to-privacy-and-freedom-of-expression. Accessed November 4, 2013.

OECD (2013). *ICTs and the health sector: Towards smarter health and wellness models*. Paris: OECD Publishing. Accessed October 4, 2013.

Okdie, B. M. (2011). *Blogging and self-disclosure: The role of anonimity, self-awarness and audience size*. Ph.D. dissertation, Department of Psychology in the Graduate School of The University of Alabama.

Peyrou, S. (2013). De l'accord PNR à Prism, bilan et perspectives sur les malentendus transatlantiques: lutte anti-terroriste versus protection des données personnelles. http://www.gdr-elsj.eu/2013/09/11/droits-fondamentaux/de-laccord-pnr-a-prism-bilan-et-perspectives-sur-les-malentendus-transatlantiques-lutte-anti-terroriste-versus-protection-des-donnees-personnelles/. Accessed October 11, 2013.

Quinn, P., Habbig, A.-K., Mantovani, E., & De Hert, P. (2013). The data protection and medical Devie frameworks: Obstacles to the deployment of mHealth across Europe ? *European Journal of Health Law, 20*, 185–204.

Rigby, M., Ronchi, E., & Graham, S. (2013). Evidence for building a smarter health and wellness future: Key messages and collected visions from a Joint OECD and NSF workshop. *International Journal of Medical Informatics, 82*, 209–219.

Shaffer, D. R., Smith, J. E., & Tomarelli, M. (1982). Self-monitoring as a determinant of self-disclosure reciprocity during the acquaintance process. *Journal of Personality and Social Psychology, 43*(1), 163–175.

Strum, S., & Latour, B. (1999). Redefining the social link: From baboons to humans. In D. MacKenzie & J. Wajcman (Eds.), *The social shaping of technology* (2nd ed., pp. 116–125). Philadelphia: Open University Press.

Verdier-Büschel, I. (2013). Medical data sharing vs. Privacy protection: Where science meets law. In Malerba, A., Massocchi, A., Santosuosso, A. (Eds.), 2012 Law & Science Young Scholars Informal Symposium Book of Papers (pp. 135–153). Pavia: Pavia University Press.

Verdier-Büschel, I. & Prouvèze, R. (2011). L'utilisation des nouvelles technologies de captation de l'image et la procédure pénale. Réflexions de droit français et de droit européen. In RERDH, *Technique et droits humains*, Actes du Colloque organisé du 20 au 23 avril 2010 aux Facultés de droit de Limoges et de Poitiers (pp. 93–118). Paris: Montchrestien Lextenso éditions.