Health Technol. (2017) 7:325–328
DOI 10.1007/s12553-017-0198-y

EDITORIAL

# Privacy matters: updating human rights for the digital society

**Giovanni Buttarelli**[1]

Received: 16 September 2016 / Accepted: 17 May 2017 / Published online: 24 July 2017


**Abstract** Privacy matters because everyone needs some portion of their intimate space - whether it is their bodies, their families and relationships, their property or information about them - to remain hidden and secure from unwanted or unexpected external interferences. Privacy is a prerequisite for the enjoyment of other hard-fought freedoms like free speech and non-discrimination on grounds of sex, race, sexual orientation and political and religious beliefs. This universal truism is being questioned in an age where humans are submitting large quantities of traces of themselves, increasingly unwittingly, and as a by-product or condition of their participation in digital life. However, as participation in digital society and the economy becomes all-pervasive, and in effect compulsory, privacy cannot become the preserve of those who can afford it. As memories of the man-made cataclysms of the twentieth century recede, there has never been a greater need for safeguards against unjustified intrusions into people's personal space by powerful state actors and corporations. Convergence between political malevolence and technological omnipotence is a *'real and present'* danger. This article summarises the case for privacy and emerging legal principles such as accountability and individual control over data about them. It argues for a *Global Friends of Privacy* comprising willing regulators, academics and civil society to patrol more vigilantly and to contest more forcefully attempts to *'salami-slice'* away precious liberties of populations.

This article is part of the Topical collection on *Privacy and Security of Medical Information*

✉ Giovanni Buttarelli
edps@edps.europa.eu

[1] European Data Protection Supervisor, Rue Wiertz 60, B-1047 Brussels, Belgium

**Keywords** Privacy · Data protection · Big data · Confidentiality of communications · Artificial intelligence · Security · Freedom

'I want to be alone': Greta Garbo's weary protest is one of the most memorable lines from Hollywood's Golden Age. It was also an unconscious assertion of the right to privacy elaborated three decades earlier by Louis Brandeis, future associate justice of the Supreme Court in his seminal Harvard Law Review article co-authored with Samuel Warren.[1] Warren and Brandeis argued that a separate 'right to be left alone' might be seen as derived from the right to property, protecting the individual from 'invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sound.' This article in-turn built on the views expressed several years earlier by Thomas M. Cooley, Chief Justice of the Michigan Supreme Court, in his *Treatise on the Law of Torts* [1].

In other words, technological developments in the United States in the latter half of the nineteenth century created new risks to the life and liberty of human beings, requiring more sophisticated legal safeguards than had previously existed. The automation of production and mass urbanisation as part of the industrial revolution brought with it severe social and environmental problems, and in so doing spurred the civil and human rights movements. Now, during the so-called Fourth Industrial Revolution, massive computational power and ubiquitous, high velocity data flows are leading to calls for stronger privacy protections to be globally applicable.

Twentieth century cataclysms inflicted by humanity upon itself represented the spectacular failure of regimes to uphold the freedom and dignity of the outsider, the poor and the

[1] "The Right to Privacy," Harvard Law Review, Vol. 4, No. 5, 15 December 1890

vulnerable. Human rights, like the right to privacy, have been designed to forestall a repeat of this nightmare, of a confluence between political malevolence and technological omnipotence. Some nations in the world have been spared calamities in the past century, including the United States and the United Kingdom. Nevertheless, there are now tendencies everywhere for fragile freedoms to be chipped away in the name of security, 'trust' or anti-corruption. This applies even where public policy drives towards wholly legitimate ends, such as eliminating the threat of terrorism, enabling access to essential social services or ensuring the safety of consumer goods.

History teaches us that once a fragile freedom is compromised it is very difficult to repair the damage. Interferences with rights evince a ratchet effect: an unprecedented surveillance measure is justified on the grounds of an exceptional threat, or in reaction to a terrorist incident; the surveillance measure becomes the new norm until the next incident occurs, which elicit calls for further, deeper intrusions.

For against the idea of inalienable rights and freedoms, there is now a counter-narrative. In a number of countries typically considered part of the liberal democratic tradition, recent political events have pointed towards a surge in a form of isolationist, nation-centric populism. This new wave is linked to a disillusionment with hitherto presumed norms, and has been notably fuelled by instant internet-enabled communications. In an increasingly polarised, and largely online, marketplace for manifestos, there is a turn towards crude *securitarian* solutions. While such solutions may offer comfort in their simplicity, they tend to lack any empirical evidence that they will on making societies safer. New terms have entered the lexicon, such as *'fake news'* and *'post truth',* suggesting that the Enlightenment rationalism, and civility, underpinning the discourse of human rights - may itself be under threat.

What is remarkable is that the civic needs of the early twenty-first century individual, just like those of the early twentieth century, are not simply locally and culturally specific. Privacy, freedom and dignity are universal human values, differently expressed around the world. Privacy is, according to Alan Westin, *'the claim of an individual to determine what information about himself or herself should be known to others'*.[2] It is a negative right, formulated in the 1948 Universal Declaration of Human Rights: the right to expect that something should not be done which affects one's intimate sphere. It thus includes a person's home and family life, as illustrated by the landmark U.S. Supreme Court ruling in Griswold v Connecticut (1965)[3] that a ban on using contraception was contrary to the 'right to marital privacy', in effect, the right of couples to be 'left alone' by the State in the privacy of their bedrooms.

The right to privacy also includes, according to the Charter of Fundamental Rights of the European Union, a person's communications, which was a natural development from the earlier texts, the UDHR and the 1959 European Convention on Human Rights, which referred to correspondence, thus seeking to protect mail from interception by the postal services or anyone else. In the EU, there are rules– shortly to be updated - for ensuring the confidentiality of electronic communications. This includes a prohibition on wiretaps for accessing the content of communications, and a requirement for service providers to obtain first the consent of phone and email users before accessing information regarding whom they have communicated with, when, where and by what means ('traffic' data). Such information is known as metadata, the electronic equivalent of an imprinted envelope. These communications are more and more mediated by machines, or transmitted by machines on behalf of a human being, perhaps even without their knowledge. It may well be that, within a generation, the notion of personal data (as defined in many jurisdictions and in the EU), or of 'personally identifiable information' (in currency in the United States), loses its meaning, because all information, even anonymised, can be tracked to 'any' individual. At such a point, all that will remain is communication between humans and humans, humans and machines, machines and machines.

Regardless of the political winds of change that may or may not be blowing, privacy matters to everyone. The most successful scions of Silicon Valley have in the past proclaimed privacy to be outdated or even dead, despite having built business empires on their prolific ability to monetise enormous volumes of personal data. Yet these very same pioneers have taken extraordinary measures to ensure the confidentiality of their personal and professional lives. Privacy is an integral part of human dignity, and a prerequisite for many other social goods such as free expression and innovation. The protection of personal data, a separate right under EU law, was conceived in the 1970s as a way of compensating the risk that large-scale data processing would erode privacy and dignity. Now, at the beginning of the twenty-first century, people are expected to disclose information that is ever more personal over the Internet so that they may participate in social, administrative and commercial affairs, with ever-less scope for opting-out of any such disclosure.

In the area of privacy and data protection, there is a striking convergence towards common standards as a by-product of globalisation. One hundred and twenty countries across every continent of the globe, now have data privacy laws, and most of them incorporate norms established by the Council of Europe and the European Union, such as the requirement for

[2] Social and Political Dimensions of Privacy, Journal of Social Issues 59(2), April 2003

[3] Estelle T. Griswold and C. Lee Buxton v. Connecticut,381 U.S. 479, 85 S. Ct. 1678; 14 L. Ed. 2d 510; 1965 U.S. LEXIS 2282 [The right of a married couple to privacy is protected by the Constitution.], Cornell University Law School - Legal Information Institute, Ithaca, NY 2017 https://www.law.cornell.edu/supremecourt/text/381/479

processing data only for purposes compatible with those for which they were originally collected, and the right to access data about oneself.

Failure to comply with these rules is in itself liable to sanctions, regardless of whether someone has suffered demonstrable pecuniary harm or emotional stress (or 'moral damage' in European law). This seats the duty to respect the interests of the individuals concerned by the data being processed squarely on the shoulders of those who seek to profit from that processing. In doing so, data protection mirrors the responsibilities incumbent on all commercial entities according to that other globalising area of law - antitrust - to avoid any anti-competitive behaviour, especially where a company is in a dominant position in a given market. Competition rules are enforced by means of an assumption that any anti-competitive behaviour is, by its very nature and notwithstanding certain public interest exemptions bad for the consumer and bad for the efficiency of markets. It is not necessary for enforcement agencies to prove that the anti-competitive conduct has had palpably harmful effects. This is the principle of accountability, newly established now also in the EU's landmark data protection framework, the General Data Protection Regulation, which entered the statute book in May 2016 following perhaps the heaviest corporate lobbying exercise in the history of EU legislation.

Rules on how information is handled have their roots in privacy, but data protection is now a distinct principle in European Union law. Personal information disclosure always affects privacy to a greater or lesser extent, but you can infringe someone's privacy without handling personal information such as by trespassing on their property, or by passing a law that interferes in people's intimate relations. The right to the protection of personal data is becoming more important than ever.

In the past it was difficult to acquire personal information. It tended to be collected mainly with the individual's knowledge and secured, once held, via physical means - such as locks and restricted access. Searching for information in archives and libraries involved travel, time and money. The rapid spread of Internet-enabled technologies in little more than the last two decades has allowed people to communicate and share information instantaneously across the planet. Rapid increases in computing power and decreases in communications and data storage costs led to the expansion of data sets in the late 1980s and the 1990s. Communications and computing technologies, the Internet, and proliferation of sensors have resulted in more data flows globally, and business processes have changed to take advantage of this rapid data expansion. Basic services have moved online, and we now have to share data, usually unknowingly, if we want to participate in contemporary life and enter the workplace.

If you believe, with Erving Goffman, [2] that social interactions can be performative - that we modify what we do to account for other people's expectations and judgments - then we must find new ways for allowing people the space to develop their personalities in the age of *big data*. At present, if you want to *'go dark'* on the Internet you can deploy a plethora of tactics, such as browser extensions, deletion of all but the most essential cookies, or simply giving false information in response to requests from web-based services; but each of these measures almost inevitably denigrates in some way the online experience, making it less convenient or even impossible to make commercial or social transactions. Furthermore, no computer is ever fully secure, and any personal information stored in the *'cloud'* is susceptible to state actors, whether domestic and hostile, and to criminal hackers. Harm to privacy is therefore an externality of the digital space, but so are restrictions on freedom of expression, and the potential for unfair discrimination based on online profiling.

One means of governance is individual control, which is why much emphasis of the new EU regulation is on the purpose of collection and on the meaning of consent. But the accountability principle helps to rebalance the obligations, so that the data controllers, that is, the companies and public bodies who process personal information for profit or other goals must take responsibility for their actions and cannot abuse the weaker position of the individual who does not have the time, or the expertise, to understand and negotiate how data is processed.

Accountable data processing, effective and relevant laws, user control – these are three essential pillars of the data protection digital ecosystem. The fourth pillar is privacy-conscious engineering. Limitations on what personal information is collected and what happens to it must be baked into the design and build of services and products; otherwise, enforcement will be toothless. The notion of the 'Internet-of-Things' heralds a world in which more and more everyday objects, from toys to fridges, from cars to organ implants, are wired up and are/will be able to communicate with anyone and anything. There are too many alarming instances of connected consumer goods on the market already that are insecure, and are prone to hacking on an almost non-trivial scale. This is where data protection literally becomes a matter of life and death.

Software programmers and product designers need to understand and implement basic tenets of data protection law, like purpose limitation and data minimisation. The latter principle appears to fly in the face of the *'big data imperative'* itself: the contention, now commonplace in many commercial and governmental environments, that we must collect more and more data and store it indefinitely in the belief that previously unimagined combinations of data, in addition to the millions of minor improvements to convenience of everyday life increasingly taken for granted, could one day solve modern humanity's most intractable problems - from disease endemics, to climate change. This is where data protection 'applies the brake,' and requires companies and governments to reflect on the need for data processing and the impact that it could have on the individual.

Even as we seek to maximise the benefits for society of rapid technological change, Europe is right to be circumspect about the risks of *big data,* as well as 'knee-jerk' responses to amorphous terror threats. Only a couple of generations ago most Europeans suffered the effects upon categorised and identifiable individuals of information databases which, although initially populated for benign purposes, were put to the service of totalitarian regimes with catastrophic consequences. [3] Safeguarding privacy and the protection of personal data are the means by which individuals in the age of hyper-connectivity can insure themselves against similarly unexpected consequences which are sadly inevitable.

Not since the Second World War has the need been greater for vigilance and for scepticism towards any measure that would erode privacy and the freedoms which it enables. This calls for a global movement of what we might term the *'Friends of Privacy'* among regulatory bodies, businesses, scholars and civil society, a coalition of those willing to pool their ideas and energies to preserve and advance in our artificial future the dignity of real people.

**Compliance with ethical standards**

**Conflict of interest** The author declares no conflict of interest.

**Funding** There is no funding source for this article.

**Ethical approval** This article does not contain any data, or other information from studies or experimentation, with the involvement of human or animal subjects.

## References

1. Cooley TM. A treatise on the law of Torts: or the wrongs which Arise independently of contract. In: Torts CO, editor. 2nd ed. Chicago: Callahan & Co.; 1888.
2. Goffman E. The presentation of self in everyday life. [monograph no. 2]. Edinburgh: Social Sciences Research Centre, University of Edinburgh; 1956.
3. Gotz A, Roth KH. The Nazi Census: identification and Control in the Third Reich. Philadelphia: Temple University Press; 2004.