23. A BEHAVIOURAL ALTERNATIVE TO THE PROTECTION OF PRIVACY*

Dariusz KLOZA**

1. INTRODUCTION

The frankest and freest and privatest product of the human mind and heart is a love letter; the writer gets his limitless freedom of statement and expression from his sense that no stranger is going to see what he is writing. Sometimes there is a breach-of-promise case by and by; and when he sees his letter in print it makes him cruelly uncomfortable and he perceives that he never would have unbosomed himself to that large and honest degree if he had known that he was writing for the public.

Mark Twain (c. 1906)¹

I.

On 7 February 2016 Joseph ceased to use what had once been his private e-mail account. He has never used any of the mainstream e-mail providers such as

* I have discussed 'behaviour' as an alternative privacy protection with many of my mentors, colleagues and friends around the world and I am indebted to all of them. In particular, I thank – in alphabetical order – Irina Baraliuc, Marcin Betkier, István Böröcz, Roger Clarke, Michał Czerniawski, Paul De Hert, Philippa Druce, Raphaël Gellert, Jake Goldenfein, Graham Greenleaf, Barry Guihen, Mireille Hildebrandt, Lucas Melgaço, Marit Moe-Pryce, Vagelis Papakonstantinou, Cristina Pauner Chulvi, Dan J.B. Svantesson, Matt Szafert and Nigel Waters for their extensive comments on an earlier version of this chapter. I am grateful for an exchange of views on a dedicated seminar *Encryption and other 'behavioural' alternatives for privacy protection*, held at the Swinburne University of Technology, Melbourne, Victoria, Australia on 19 April 2016, and in particular to Claudy Op den Kamp and Monika Žalnieriūtė. I thank two anonymous peer-reviewers for their suggestions. Finally, I am grateful to the Faculty of Law of Bond University, Gold Coast, Queensland, Australia for providing me time and space that allowed me to research and write this chapter. I further gratefully acknowledge financial support for that purpose received from the Fonds Wetenschappelijk Onderzoek – Vlaanderen (FWO).

** Research Group on Law, Science, Technology and Society, Vrije Universiteit Brussel; Peace Research Institute Oslo. E-mail: dariusz.kloza@vub.ac.be.

¹ *The Autobiography of Mark Twain*, Vol. 1, ed. H.E. SMITH (2010); <<http://www.marktwainproject.org>>.

Google, AOL, Apple or Yahoo. Instead, he opened this particular e-mail account at one of the major nationwide providers in the country Y, situated in Europe, where he was born and where he lived at that time. That particular e-mail account required a paid subscription, though its annual fee was rather negligible. In return, it offered a mailbox free from annoying advertisements, which – in the early years – came attached to the bottom of each message. Joseph trusted this provider that his e-mail account would be free of any commercial spying and similar practices, which – from Joseph's point of view – were unwanted. (He could not recall ever buying anything suggested by any advertisement, no matter how persuasive they were.)

Back in 2006 it was a conscious choice dictated by an idealistic desire to avoid dominant multinational companies, fuelled largely by the cyberpunk literature and movies of Joseph's childhood. Although Joseph has never been a 'digital native' – i.e. someone who grew up already surrounded by emerging technologies, and thus having acquired, almost automatically, high-tech literacy skills – he has quickly become 'tech-savvy' and these technologies have fascinated him ever since. When he was around ten years old his parents bought him his first personal computer and this way he has witnessed the most of the technological progress of 1990s. His fascination, at that stage, was rather romantic: his enthusiasm grew with each new own discovery. (To the extent that he too was initially captivated by Barlow's *Declaration of the Independence of Cyberspace*,² which – Joseph claims – for him shed new light on Schiller's '*deine Zauber binden wieder*').³ In his elementary school he learned to code a couple of computer programming languages. Some 20 years later, he claims, he can 'speak fluently only HTML' (Hyper Text Markup Language). In the golden age of cyberspace, together with a fellow student at the university, he even had run a blog devoted to the intersection of law and technology. The web archives nowadays have 'thankfully forgotten it'.

Yet his fascination for technology has never been unconditional. He certainly has never blindly trusted technology. For instance, being a frequent traveller, he always carries with him some cash in a 'hard currency', because credit cards might unexpectedly stop working. He always covers the keyboard of the terminal while typing in his personal identification number (PIN). While travelling, some of his credit cards once or twice were skimmed and his bank blocked further transactions on its own initiative. Joseph was glad that his money was safeguarded, but also equally annoyed that he was deprived of access to his funds until he came back to his country of residence and received a new card in a

² J.P. BARLOW, *Declaration of the Independence of Cyberspace*, Davos, 8 February 1996, <<https://www.eff.org/cyberspace-independence>>.

³ A passage from Friedrich Schiller's *Ode to Joy (An die Freude, 1795)*. In the majority of translations to English interpreted as 'your magic binds again [reunites]'.

bank branch. Having, under social pressure, once signed up to a major social networking site and having kept it for a few years, he quit after falling victim to a data breach.

With the passage of time, Joseph has changed his desktop computer for a laptop and a dial-up connection to broadband wireless. He was using his private e-mail account predominantly for casual discussions with family and friends, sporadic online shopping and travel reservations. Sometimes his e-mail conversations would concern intimate facts concerning himself or his family and close friends. From time to time he exchanged views on delicate subjects and politics, sometimes explored in a very sarcastic way. However, these conversations have never amounted to anything illegal or otherwise illicit. Nevertheless, Joseph assumed his private communications were secure enough and – in the early years – he did not employ any extra layers of protection such as encryption or anonymisation. The only exceptions to this were services encrypted by default, e.g. online banking. He would make sure his anti-virus software and its database were up-to-date. In general, he had been using relatively strong passwords, changed periodically, so – at the end of the day – he had been sleeping rather well.

As the technology progressed and the equipment became more affordable, Joseph increasingly accessed his e-mails on multiple devices, e.g. on home and office computers. Put simply, it was both convenient and useful. Technically speaking, this involved subscribing to the IMAP (Internet Mail Access Protocol) communication protocol, which allows for synchronisation among these devices, yet keeping copies of all e-mails not only on each device, but also on the server. At a certain point, using the IMAP protocol became beneficial further for backup purposes. There was a time when backup was of little concern for Joseph. At home, he has had in his possession an external hard drive and he would make a backup copy once in a while. At work, he would avoid any cloud computing services and he would access his professional Dropbox account – demanded by his employer – solely via a website, thus avoiding the need to install a specific application on his laptop and avoiding any accidental upload. However, once while boarding a plane, his backpack accidentally dropped onto the ground, causing significant damage to his laptop, including a permanent loss of some data.

In the meantime, Joseph has progressively become aware and conscious of both the benefits and drawbacks of innovation and emerging technologies, of their impact on his life and the lives of others in society. Eventually, dealing with these technologies has become a part of his professional life. He called it *la déformation professionnelle*. Joseph is not a conservative, quite the contrary, but he sees that a tiny number of things were better in the past and he views some reasonable degree of 'offline-ness' as one of those.

Joseph would use his mobile phone until the device ceases to function. (His last mobile phone served him for six years and – while obtaining a new one – he lamented that nowadays his options were limited almost entirely to smart phones.) Determined to make do, he decided not to enable any 'smart'

functionality and would use his phone solely for calling and texting. With the phone he currently possesses, he is still able to take out its battery while attending important meetings. (For such meetings, he leaves his tablet in the office.) He would put a removable sticker on the laptop built-in camera. He would reject the majority of loyalty programmes, short of those of airline alliances, his guilty pleasure. In his web browser, he would enable a do-not-track functionality, install a blocking application for advertisements and an add-on to blur his Internet Protocol (IP) address. He would use unorthodox search engines and erase his browsing history and cookies every few days.

He would prefer reading on paper than on his tablet. Each year, on holidays, he would disconnect entirely for a couple of weeks. He would not even touch a keyboard of any device. He calls it a 'digital detox'. While travelling, he would decline to use any navigation device and instead would consult a pocket map or ask someone for directions. (He once lamented that the generation just a decade younger than him had lost the sense of directions and 'these days they cannot find their way without Google Maps'.)

On 7 February 2016 a new surveillance law entered into force in country Y. This piece of law constituted a part of a broader reform process pursued by a new far-right government, elected just a few months earlier. Not going into details, certain law enforcement agencies of that government became empowered to read too much – in Joseph's opinion – of his communications, without any concrete reason or adequate safeguards. In particular, due to deliberate vagueness of legal provisions, these agencies became allowed to access any data stored at any server within the borders of the country Y. Because Joseph was using the IMAP protocol and because a copy of his data was kept on a server, these agencies could access *de facto* the entirety of his e-mail communication. While Joseph would assume, even dangerously, that similar practices debated or introduced in truly democratic countries would be genuinely used to fight against serious crime and terrorism, there exists a critical threat that these new surveillance powers in country Y, the country of his passport, could be used also to undermine the political opposition, now or in the future. Even though Joseph no longer lives there – together with many of his fellow citizens, also those living abroad – he finds what this new government does is pretty much undemocratic. Being born in Eastern Europe and being aware of atrocities committed in the past by the Gestapo, NKWD, Bezpieka, Securitate or Stasi – just to name a few – many of these with the aid of information collected by these security services, Joseph felt 'cruelly uncomfortable'.

When in 2013 Edward Snowden revealed spying practices carried out by the US National Security Agency, Joseph was rather glad his e-mail provider was not compromised. However, a few of Joseph's friends have used mainstream providers such as Google, and this way some of his e-mails could have been spied on. However, he had nothing to do with American politics and actually not that much correspondence has been exchanged that way. Thus this did not trouble him greatly. Yet both these developments – in the US and, subsequently,

in the country of his passport – eventually convinced him he needed some extra steps to protect his interests.

On 7 February 2016 Joseph therefore ceased to use this particular private e-mail account. He did not think he had any other choice. The law in country Y has been used instrumentally to legitimise the abuse of power. First, the ‘cost’ of going to a constitutional court to challenge the law, assuming it was possible and that it would make any change, constituted an entry barrier. Second, he could not encrypt for himself his e-mails already stored on the server. In practice, he changed the modern IMAP to the old-fashioned Post Office Protocol 3 (POP3) and downloaded all the e-mails to his own device, automatically deleting the totality of their copies from the server. Still, this has not been a perfect solution: he cannot exclude backup copies, kept by the provider in the course of normal business practice, finding its way to the wrong hands. (In point of fact, this e-mail account still remains active as some of his relatives, colleagues and friends might not yet know his new e-mail address. He intends to close down the old one within a year or so.)

He has not abandoned the idea of having an e-mail account for purely private purposes; quite the contrary. Some ideas came by word of mouth and – after some market research – he opted for a provider offering end-to-end encryption, no ‘back doors’, ‘key escrows’ or similar practices, whose servers are located in a jurisdiction believed to be free from the peeping eyes not only of businesses but also of governments. Even with a lawful court order, such a service provider could hand over only encrypted data that cannot be read without a key. Even if the data were hacked or leaked, they would reveal a string of meaningless zeros and ones. And it would be difficult to compel him to hand over the decryption keys. He has eventually trusted that this provider would actually do what it claims. Joseph likes to believe he partakes in a bigger movement. With his friends and colleagues, who are well-read in information and communication technologies, he has begun looking for effective means to protect privacy. Such debates recently concern alternatives for secure cloud storage of data or instant messaging. They still have not found what they are looking for.

II.

The story of Joseph is true and I know him personally.⁴ His story has inspired me to ponder on the gradual failure of existing arrangements – i.e. modalities (like

⁴ The name has been changed. ‘Joseph’ was chosen because ‘J’ in ‘Edward J. Snowden’ stands for ‘Joseph’. It was Mireille Hildebrandt with her chronicle of Diana’s ‘onlife world’ (M. HILDEBRANDT, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Cheltenham 2015, pp. 1–7) who inspired me to start too with a story. The concluding sentence is adapted from U2 and their song ‘I still haven’t found what I’m looking for’ (Clayton/Evans/Hewson/Mullen; 1987). I particularly thank Barry Guihen for his advice in giving account to Joseph’s story.

the law), actors and dynamics between them – to *adequately* protect individual and collective interests, including privacy.

In our world, that is to say, the Western world, it is expected that the tripartite foundation of our societies – democracy, fundamental rights and the rule of law (in the Anglo-Saxon world) or *Rechtsstaat* (in continental Europe)⁵ – would *adequately* protect individuals, the society and their respective, and sometimes contradictory, interests against abuse. This duty to protect adequately has multiple aspects. It first and foremost requires establishing a dedicated system of protection. It further includes drawing a 'thin red line' whenever these various interests diverge or conflict. It includes holding the state accountable for its own actions and inactions. It requires the state to ensure relevant actors within its jurisdiction partake in providing this adequate protection and to hold these actors accountable for that.⁶ Some forms of protection are exclusive for the state, e.g. criminal justice or national security. Some others are 'shared', i.e. the state offers some protection in a form of e.g. enforceable legal rights, but a lot of room for manoeuvre is nevertheless left for individual choice. According to the belief of individual's freedom, she is to choose whether, when and how to be protected, thus complementing the system of protection. It is further expected that democracy, fundamental rights and the rule of law (*Rechtsstaat*) would ensure that both the public authorities (governments at all levels, independent regulatory authorities, etc.) as well as private actors, this including organisations and other individuals, would not interfere or invade, unless strictly necessary yet with some safeguards offered, with individual and collective interests. It is also expected that public authorities would operate on the basis of the law and within its limits, far from arbitrariness, while realising their public mission, including the provision of prosperity, safety and security, among others. This ideal is applicable to the entirety of political life. It includes both individual and collective interests and privacy is one of them. In some instances, the existing arrangements do their job excellently. In some other instances, these arrangements do not live up to the expectations vested therein. Put simply, in those instances the existing arrangements – i.e. modalities, actors and dynamics between them – have failed to *adequately* protect diverse interests and the protection of privacy is one of them.

⁵ Drawing boundaries between these four concepts lies beyond the scope of this chapter. Cf. further e.g. J. WALDRON, 'The Rule of Law and the Importance of Procedure' in J. FLEMING (ed.), *Getting to the Rule of Law*, New York University Press, New York 2011, p. 3.

⁶ This is a reference to the concept of 'system responsibility'. Cf. e.g. P. DE HERT, 'Systeemverantwoordelijkheid Voor de Informatiemaatschappij Als Positieve Mensenrechten-verplichting' in D. BROEDERS, C. CUIJPERS and J.E.J. PRINS (eds.), *De Staat van Informatie*, Amsterdam University Press, Amsterdam 2011, pp. 33–95; P. DE HERT, 'From the Principle of Accountability to System Responsibility? Key Concepts in Data Protection Law and Human Rights Law Discussions' (2011) *Proceedings of the Data Protection Conferences 2011 Budapest*, Budapest, pp. 95–96.

The protection of interests such as privacy is to a large extent achieved by means of regulation and the key modality of regulation is that of law. However, the law may sometimes be unable to offer any protection, the protection offered might be insufficient, the law might simply lack common sense or, worse, might be used instrumentally to approve an undemocratic practice. Resorting to other means to fill in the gap often brings only moderate consolation. As a result, people have less and less trust in the existing arrangements as well as in those who regulate (e.g. parliaments), execute these regulations (e.g. governments) and – sometimes – adjudicate (e.g. courts of law). The story of Joseph's private e-mail account illustrates this perfectly: initially, the law offered him no practical, effective or efficient protection from the peeping eyes of multinational companies, but he was still free to *choose* another e-mail provider, with a different business model, in another country with a different set of laws. For some years such a solution was acceptable to him as – even though later on the National Security Agency (NSA) in the United States (US) could have read these few e-mails extracted from his friends' accounts – he did not perceive it as an invasion crossing his own 'thin red line'. The main reason was that he had nothing to do with US politics. However, when the law in more and more countries, including the country of his passport, has been used to sanction the almost unlimited and warrantless searching powers of law enforcement authorities, this was too much for him. This threat – that someone could be reading his e-mails without his knowledge, sometimes without really good reason and that this might be used against him, now or later – touched upon him, his identity and dignity and he *chose* to cease using that particular e-mail account. Instead, he *chose* to subscribe to a provider offering encrypted services, accepting all consequences of his choice.

What Joseph did is to resort to his own *behaviour* to protect his interests, including his privacy. He chose to undertake certain actions or inactions to protect – when he was aware of threats and he understood them – those of his interests he considered vital and directly relevant to his personhood, even though his choice did not make his life easier. (He faced the truth that the more secure, the less available and less easy to use the service is.)

The use of behaviour to protect own interests is nothing new. In this setting, behaviour has a long history. For example, when trust in a messenger could not be sustained, it is Julius Caesar who has been credited with inventing perhaps the first, simplest and most widely known cryptography technique: in his private correspondence he would use a substitution cipher. He would write 'three letters back', i.e. replace the letter D by A, E by B, etc. However, the way in which behaviour is used nowadays to protect privacy, the reasons for that and their implications are rather new and thus merit academic attention. In this contribution I would like to explore the phenomenon of *behavioural means of privacy protection* as a reaction to the failure of the existing arrangements to offer *adequate* protection thereof.

III.

The structure of this chapter is rather simple. Section 2 overviews contemporarily available privacy protections and these could be of a regulatory (and in particular legal), organisational and technological nature. Section 3 analyses the inadequacies of these protections. I start with the underlying problem of the protection of privacy – i.e. the irreversibility of harm – and I next discuss main reasons for such inadequacies in each category of protections. In particular, I argue that contemporary regulatory protections are inadequate because they do not offer practical, effective and efficient protection; they do not keep pace with the ever-changing nature of the society, their needs and desires, on the one hand, and of innovation and technology, on the other; they are often used instrumentally to pursue specific political goals; and such a usage leads to the diminishment of public trust. These early parts give a succinct overview of the many avenues available to protect privacy. They subsequently argue that despite this multiplicity of ways, in some instances, contemporarily available privacy protections do not live up to the expectations vested therein. (I use a lot of examples and a reader in a hurry might safely omit them.) Therefore section 4 introduces the notion of behavioural means of privacy protection as a response to these inadequacies. Based on my own experience, lengthy discussions and observations, I overview their history, offer an early typology thereof and spell out their characteristics, conditions for their successful application and problems they might cause. Section 5 concludes this chapter by arguing for the recognition of behavioural protections as a standalone and legitimate means of privacy protection. It further speculates on side effects these protections might cause (e.g. chilling effect and social exclusion) and on the boundaries between their use and abuse. So far as possible, this chapter is accurate to end of November 2016.

In this chapter, I refrain from defining what 'privacy' and 'personal data protection' (or 'data privacy') are or what they do. I also refrain from distinguishing one from the other.⁷ For the sake of ease for the reader, I use

⁷ The distinction between 'privacy' and 'data protection' is based on the *method* by which they perform their function in the society. As Gutwirth and De Hert put it, 'the history and the practice of democratic constitutional states ... always reveal the use and articulation of two distinct constitutional or legal tools. On the one hand, there are tools that tend to guarantee non-interference in individual matters and the *opacity of the individuals*. On the other hand ... tools that tend to organise and guarantee the *transparency and accountability of the powerful*. These two instruments have the same ultimate objective, namely the limiting and controlling of power, but they realise this ambition in a different way, from a different perspective' (S. GUTWIRTH and P. DE HERT, 'Regulating Profiling in a Democratic Constitutional State' in M. HILDEBRANDT and S. GUTWIRTH (eds.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, Dordrecht 2008, p. 275; emphasis in original). The former is conceptualised as 'privacy', the latter – 'personal data protection' or 'data privacy'. Cf. further e.g. G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Dordrecht 2014.

'privacy' to signify both. Instead, I discuss solely the *means* of their protection, as I have axiomatically assumed that both merit protection. The reader would nevertheless see I that tend to understand 'privacy' as a human right in the European sense, but this does not exhaust its other possible meanings. I use the term 'protections' (in plural) to denote the wide range of regulatory, organisational, technological and behavioural means (modalities) available for keeping privacy 'safe from harm and injury'.⁸ After introducing Christopher Hood's theory of governance in section 2, 'protections' are interchangeably used with 'tools'. Conversely, by using 'protection' (in singular) I deploy its natural meaning.

2. TOOLS FOR PRIVACY PROTECTION

2.1. REGULATORY TOOLS

2.1.1. *Legal tools*

What means are currently available for the protection of privacy? In other words, what means the various stakeholders – from a layman on the street to those who regulate, to those who handle information, to those who oversee compliance – have at their disposal to protect privacy, either their own, either of others? Here I am not interested in what the object of protection is (I have named it 'privacy' and refrained from defining it but already assumed it is worth protecting), I am least interested in who has to protect (it shall suffice for my purposes to assume each of the above-listed stakeholders has to play some role) or where the protections originate from (e.g. formal political arenas),⁹ but rather I am interested in the mechanisms of protection; in other words: how? I have been inspired by the classic *The Tools of Government* by Christopher

⁸ Oxford Dictionary of English.

⁹ In order to get the most complete understanding of any theory of regulation, many commentators argue that not only the ways how regulation is achieved matter, but also those who regulate (actors) and relations (dynamics) between them (cf. e.g. C.D. RAAB and P. DE HERT, 'Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood' in R. BROWNSWORD and K. YEUNG (eds.), *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, Oxford 2008, pp. 263–285). Other commentators supplement these with processes of regulation (constituent steps or tasks) and venues ('institutional locations where authoritative decisions are made') (cf. e.g. J.R. TURNPENNY, A.J. JORDAN, D. BENSON and T. RAYNER, 'The Tools of Policy Formulation: An Introduction' in A.J. JORDAN and J.R. TURNPENNY (eds.), *The Tools of Policy Formulation: Actors, Capacities, Venues and Effects*, Edward Elgar, Cheltenham 2015, pp. 8–12; F.R. BAUMGARTNER and B.D. JONES, *Agendas and Instability in American Politics*, University of Chicago Press, Chicago 1993, p. 32). An analysis of the many theories of regulation from these perspectives lies outside the scope of this chapter.

Hood, who was interested in the 'tools' – 'such as tools for carpentry and gardening' – that government has at its disposal for governance, i.e. for 'shaping our lives'. His systematisation is useful to make sense of the complexity of available protections, allowing to choose the best means in the given situation and in the given time, implicitly facilitating their scrutiny.¹⁰

Theoretically speaking, nowadays privacy can be protected by regulatory (legal), organisational and technological means. By 'regulation', I deploy its political science meaning, that is 'sustained and focused control exercised by a public authority over activities valued by the community',¹¹ 'the ability of A to get B to do something that B would not otherwise do, or not do something B would normally do',¹² or 'the intentional use of authority to affect behaviour of a different party according to set standards, involving instruments of information-gathering and behaviour modification'.¹³ All these definitions focus on different aspects of regulation, but indisputably all have one element in common: that regulation is 'a way of controlling society'.¹⁴ (These definitions are silent as to the ultimate goal of regulation and implications resulting therefrom. I will come back to this point below, at section 3.2.1.3.)

When regulation *does* protect privacy, it does so in two ways, and the former comprises the latter. In a very general sense, the mere fact privacy is regulated constitutes a form of protection to an individual and to the society on a condition that such was the ultimate goal of regulation. It could set its boundaries or spell out conditions for a justifiable interference with one's interests. This is a broad understanding. In a more concrete sense, the regulatory framework for privacy can contain some particular elements – like individual rights, security measures and remedies – whose main role is either to make sure 'nobody gets hurt' or – should something bad happen – victims may seek justice. This is a narrow understanding. It spells out for example the tools available to those who wish to protect their own interests.

When regulation *does not* protect privacy, it does so in the same two ways. A privacy matter might deliberately not be regulated while it normally should have been. Alternatively, regulation might sanction a practice infringing individual's privacy without any safeguards. These might result for example in a far too broad access to personal information. Finally, a tool to protect privacy may not exist, may not offer any efficient level of protection (i.e. an illusion thereof) or may not be available in a given situation. Perhaps this is not an incontestable

¹⁰ C.C. HOOD, *The Tools of Government*, Macmillan, London 1983, pp. 2–11. Cf. also: C. HOOD and H. MARGETTS, *The Tools of Government in the Digital Age*, Palgrave Macmillan, Basingstoke 2007.

¹¹ P. SELZNICK, 'Focusing Organisational Research on Regulation' in R. NOLL (ed.), *Regulatory Policy and the Social Sciences*, University of California Press, Berkeley 1985, p. 363.

¹² A. FREIBERG, *The Tools of Regulation*, Federation Press, Sydney 2010, p. 84.

¹³ J. BLACK, 'Rebuilding the Credibility of Markets and Regulators' (2001) 3(1) *Law and Financial Markets Review* 1–2.

¹⁴ HOOD, above n. 10, p. 4.

example, but the need to remove or reduce public access to personal information that is claimed no longer relevant for the society resulted in the coinage of the 'right to be forgotten'.

Regulatory tools are perhaps the most widespread in the privacy universe and the law is their main manifestation. Formally speaking, the sources of law can range from (1) international treaties, legislation and other forms of rulemaking, to (2) case law (adjudication), (3) legal doctrine and (4) legal custom, to (5) general principles of law and equity.¹⁵ The regulation of privacy and tools for its protection originate predominantly from the first three sources.

The protection of privacy by rulemaking is usually tripartite. First, it is a fundamental right recognised both in international and supranational human rights instruments as well as in virtually all national constitutions in Western democratic states. Constitutionalisation of privacy protection traces back as early as to the Enlightenment movements, starting perhaps with the Fourth Amendment to the Constitution of the United States (1789) protecting against unreasonable searches and seizures by the federal government. The twentieth century brought the legal conceptualisation of privacy as a human right. In the aftermath of the atrocities of World War II, privacy became protected by international instruments, such as 1948 Universal Declaration of Human Rights (Art. 12) (non-binding) and 1966 International Covenant on Civil and Political Rights (Art. 17), and regional instruments, such as 1950 European Convention (Art. 8) on Human Rights and its 1969 American counterpart (Art. 11) (but *not* in its 1981 African counterpart, at least not directly). Most recently, the European Union (EU) bound itself with the Charter of Fundamental Rights (2009), recognising separately the right to privacy (Art. 7) and to personal data protection (Art. 8). There are also 'sector-specific' instruments, such as the 1989 Convention on the Rights of the Child (Art. 16). All in all, basic privacy rules are situated at the top of the hierarchy of legal norms and therefore touch upon the essential principles of a national legal system.¹⁶

Second, privacy and its protections are a *direct* object of regulation, either by civil, criminal and administrative branches of law. A patchwork of common law torts of privacy emerged after Warren and Brandeis' influential article 'The Right to Privacy'.¹⁷ Such a civil action, regardless of the label it bears, is nowadays widely recognised in the majority of jurisdictions. Some other jurisdictions even criminalise behaviour violating privacy.¹⁸ All in all, these means of protection

¹⁵ Cf. Art. 38 of the Statute of the International Court of Justice: 'The Court ... shall apply: international conventions, ... international custom, ... the general principles of law recognized by civilized nations; ... judicial decisions and the teachings of the most highly qualified publicists of the various nations'

¹⁶ S. GUTWIRTH, *Privacy and the Information Age*, Rowman & Littlefield, Lanham MD 2002, p. 32.

¹⁷ S. WARREN and L. BRANDEIS, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193–220.

¹⁸ Cf. P. DE HERT, 'The EU Data Protection Reform and the (Forgotten) Use of Criminal Sanctions' (2014) 4(4) *International Data Privacy Law* 262–268.

took the shape of a liability for some form of wrongdoing. These are therefore retroactive in principle.

When a single piece of law – be in an act of parliament or other statutory instrument – regulates privacy, it deals with a single aspect of privacy and most often it is the regulation of privacy when personal information is being handled. (I, of course, generalise here.) They bear, in English, names such as 'Privacy Act' or 'Data Protection Act'. Nowadays such laws can be found in more than a hundred jurisdictions.¹⁹ Such laws surfaced for the first time in Europe in 1970s and gradually became more common around the world. The earliest legal statutes – those of Western Germany's Hesse in 1970, Sweden in 1973 and of West Germany (federal) in 1977 – were legislated as a response to the gradual increase of processing of information with the aid of a computer within government and large private organisations (as only these entities needed and could have afforded to at the time).²⁰ Their focus changed over time, from countering the inhumane information processing (first generation), to vesting some rights in an individual (second) and in particular the right to self-determination (third), to strengthening the position of an individual and regulations of specific sectors (fourth generation).²¹

Regulation of data privacy at the international and regional levels dates back to 1980 with the Organization for Economic Co-operation and Development (OECD) issuing their non-binding data protection Guidelines, revised in 2013.²² In 1981 the Council of Europe opened for signature its 'Convention 108',²³ a first-ever binding treaty that is now adhered to by more than 50 jurisdictions worldwide and aspiring, after nearly completed modernisation, to lay a foundation for a global standard.²⁴ In 1990 the UN issued their, obviously non-binding, guidelines for the regulation of computerised personal data files.²⁵

¹⁹ G. GREENLEAF, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories', 2013, pp. 2–10.

²⁰ V. MAYER-SCHÖNBERGER, 'Generational Development of Data Protection in Europe' in P. AGRE and M. ROTEBERG (eds.), *Technology and Privacy: The New Landscape*, MIT Press, Cambridge MA 1997, p. 221.

²¹ Ibid., pp. 219–241. Each of Mayer-Schönberger's generations of data protection laws reflect the defence against the prevailing threat of that time. This could be compared with Clarke's 'eras of dataveillance': the era of justifiable centralisation (1940–80), of unjustified centralisation (1980–2000) and of dispersed power (from 2000 onwards) (R. CLARKE, 'The Eras of Dataveillance', 1994, p. 1, <<http://www.rogerclarke.com/DV/NotesDVEras.html>>).

²² OEDC, *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, Paris, 11 July 2013, <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

²³ Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 28 January 1981, ETS 108.

²⁴ G. GREENLEAF, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2012) 2(2) *International Data Privacy Law* 68–92; G. GREENLEAF, 'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?' (2013) 29(4) *Computer Law and Security Review* 430–436.

²⁵ United Nations, General Assembly, *Guidelines for the regulation of computerized personal data files*, A/RES/45/95, New York, 14 December 1990.

All in all, these laws usually spell out conditions for the handling of personal information as well as both empower individuals with regard to the handling of their data and offer protection against abuses thereof. In this sense, they combine proactive and retroactive elements. The protection they afford is – to a large extent – compulsory, i.e. stakeholder cannot waive it by agreement, a practice well known for example in contract law. They protect individuals by channelling the legitimate use of their personal data by others, i.e. both public authorities and private sector organisations. They empower individuals by vesting in them information and control over how their information is handled as well as they offer protection and remedies against abuses. For example, like many data privacy legal frameworks worldwide, the 1995 Data Protection Directive in the European Union gives a catalogue of rights that an individual can invoke and these include the right to access her data, to rectify any wrong or incomplete information, to object processing on certain lawful grounds and to seek remedy for damages and harm suffered. The Directive further protects her against being subject to an automated decision-making. With the progress of time, this catalogue is often being expanded. For example, the 2002 e-Privacy Directive, within its scope of application, introduced a data breach notification. In 2016 the General Data Protection Regulation not only universalised such notification but it also added e.g. the right to de-listing and to data portability. These laws are binding and compliance therewith is strengthened by a variety of sanctions; the most severe would be a punishment combined with invalidity (*lex plus quam perfecta*).

These laws I have overviewed above constitute a form of primary legislation and they are usually supplemented by a plethora of other forms of regulation by law.²⁶ For example, Moshell considers four legal means in this context: comprehensive, sectorial, self-regulation of privacy and 'privacy technologies'.²⁷ These could equally be binding or not (i.e. soft law). In the latter case, they constitute a set of norms for which no structural enforcement is foreseen and compliance depends solely on the will and/or rational calculations of regulated actors.

Third, privacy and its protections are an *indirect* object of regulation. Many of legal provisions outside the typical boundaries of (data) privacy law deal in one or another way with privacy and its protection. *De lege lata*, international anti-terrorism arrangements or free trade agreements in which the need for sharing personal information necessitated safeguards for individuals and their personal data. (Or a lack of such safeguards, in case of which it is a form of regulation that does *not* protect privacy.) If I look at an individual, in case of a violation, she can normally seek relief by complaining to the body that handles

²⁶ C. BENNETT and C.D. RAAB, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge MA 2006.

²⁷ R. MOSHELL, '... And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection' (2005) 37 *Texas Tech Law Review* 366–367.

her data, to a relevant supervisory authority or to a court of law, national or – in a few situations – supranational.²⁸ When she resorts to a public enforcement machinery, her ‘complaints and cases can be handled within various domains of law, ranging from administrative (if applicable) to civil and criminal law; the use of one does not usually preclude the use of any other.’²⁹ For example, a prohibition in the criminal procedure to disclose to the public the names of the accused and of experts and witnesses, among others, can be invoked to protect their privacy too.³⁰ The control of mergers and acquisitions of businesses running on personal data often has implications for privacy protection.³¹ Yet the most pertinent use is perhaps made of consumer law and especially of a class action. The recently filled in reference for a preliminary ruling to the Court of Justice of the EU (CJEU; Luxembourg Court) asks the question whether the use of a social networking site for purposes *both* private and professional qualifies its user as a consumer. If so, she could benefit from protective jurisdiction rules offered by EU private international law and sue a service provider headquartered in another country in the jurisdiction of her domicile.³²

De lege ferenda, tools for privacy protection are constantly being called for – as a response to the inadequacies of existing ones – and subsequently developed. The discourse thus far has most often looked at other branches of law for an inspiration on how to protect best various aspects of privacy. These include property law,³³ private international law (conflict of laws), consumer law,³⁴

²⁸ A. GALETTA and P. DE HERT, ‘The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-Oriented Remedial System?’ (2015) 8(1) *Review of European Administrative Law* 123–149.

²⁹ D. KLOZA and A. GALETTA, ‘Towards Efficient Cooperation between Supervisory Authorities in the Area of Data Privacy Law’, Brussels Privacy Hub Working Papers, Brussels 2015, <<http://www.brusselsprivacyhub.org/Resources/BPH-Working-Paper-VOL1-N3.pdf>>, p. 10.

³⁰ I am referring to a recent scandal in the Polish media (January 2017) in which the public television ‘broadcasted’, with a few instances of delay, a hearing at a court of law, without withholding the names of any person involved therein, thus breaching the criminal procedure (cf. Art. 355ff Code of Criminal Procedure; Act of 6 June 1997, as amended, OJ No. 89, Item 555) and the press law (cf. Art. 13(1) Press Law; Act of 26 January 1984, as amended, OJ No. 5, Item 24).

³¹ Cf. the most recent example: P. TEFFER, ‘EU wants to know if Facebook lied about Whatsapp’, *EU Observer*, 20 December 2016, <<https://euobserver.com/digital/136359>>. Cf. also EUROPEAN DATA PROTECTION SUPERVISOR, ‘Privacy and competitiveness in the age of big data. The interplay between data protection, competition law and consumer protection in the Digital Economy’, Brussels, March 2014, <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competition Law_big_data_EN.pdf>.

³² Case C-498/16, *Maximilian Schrems v. Facebook Ireland*.

³³ Cf. e.g., N. PURTOVA, *Property Rights in Personal Data: A European Perspective*, Kluwer Law International, The Hague 2011.

³⁴ Cf. e.g., A. GALETTA, D. KLOZA and P. DE HERT, ‘Cooperation among Data Privacy Supervisory Authorities: Lessons From Parallel European Cooperation Mechanisms’, Brussels–London–Warsaw–Castellón, 2016, pp. 38–62, <http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA2_D21_final_20160416.pdf>.

competition law,³⁵ contract law³⁶ and criminal justice,³⁷ among others, but it is environmental law that probably has attracted the most of attention.³⁸

Both direct and indirect regulation of privacy and of its protections owes much to the jurisprudence of the courts of law at all levels, like the Supreme Court of the United States, the European Court of Human Rights (ECtHR, Strasbourg Court),³⁹ CJEU⁴⁰ or advisory and standard-setting bodies, such as the Article 29 Working Party in the EU⁴¹ or the annual International Conference of Data Protection and Privacy Commissioners (ICDPPC). This picture would not be complete without international organisations, networks of regulators, civil society organisations and academia. In 2015, the United Nations (UN) Human Rights Commission created for the first time the position of a Special Rapporteur on the Right to Privacy,⁴² but even earlier calls asked for a specific, dedicated UN agency for the protection of privacy.⁴³

³⁵ Cf. e.g. D. KLOZA and A. MOŚCIBRODA, 'Making the Case for Enhanced Enforcement Cooperation between Data Protection Authorities: Insights from Competition Law' (2014) 4(2) *International Data Privacy Law* 120–138.

³⁶ Cf. L.A. BYGRAVE, *Internet Governance by Contract*, Oxford University Press, Oxford 2015.

³⁷ Cf. e.g. P. DE HERT and A. WILLEMS, 'Dealing with Overlapping Jurisdictions and Requests for Mutual Legal Assistance While Respecting Individual Rights. What Can Data Protection Law Learn from Cooperation in Criminal Justice Matters?' in P. DE HERT, D. KLOZA and P. MAKOWSKI (eds.), *Enforcing Privacy: Lessons from Current Implementations and Perspectives for the Future*, Wydawnictwo Sejmowe, Warsaw 2015, pp. 48–76, <http://www.phaedra-project.eu/wp-content/uploads/phaedra1_enforcing_privacy_final.pdf>.

³⁸ Cf. J. NEHE, 'Recognizing the Societal Value in Information Privacy' (2003) 78 *Washington Law Review* 1–92; D.D. HIRSCH, 'Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law' (2006) 41(1) *Georgia Law Review* 1–63; D. KLOZA, 'Public Voice in Privacy Governance: Lessons from Environmental Democracy' in E. SCHWEIGHOFER, A. SAARENPÄÄ and J. BÖSZÖRMENYI (eds.), *KnowRight 2012. Knowledge Rights – Legal, Societal and Related Technological Aspects. 25 Years of Data Protection in Finland*, Österreichische Computer Gesellschaft, Vienna 2013, pp. 80–97. Cf. also EMANUEL, Ch. 21, in this volume.

³⁹ Cf. R. GELLERT and S. GUTWIRTH, 'The Legal Construction of Privacy and Data Protection' (2013) 29(5) *Computer Law & Security Review* 522–530.

⁴⁰ Cf. J. KOKOTT and C. SOBOTTA, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3(4) *International Data Privacy Law* 222–228; G. ZANFIR, 'How CJEU's "Privacy Spring" Construed the Human Rights Shield in the Digital Age' in E. KUŻELEWSKA, D. KLOZA, I. KRAŚNICKA and F. STRZYCZKOWSKI (eds.), *European Judicial Systems as a Challenge for Democracy*, Intersentia, Antwerp 2015, pp. 111–126.

⁴¹ Cf. Y. POULLET and S. GUTWIRTH, 'The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: An Illustration of "Reflexive Governance"?' in O. DE SCHUTTER and V. MORENO LAX (eds.), *Human Rights in the Web of Governance: Towards a Learning-Based Fundamental Rights Policy for the European Union*, Bruylant, Brussels 2010, pp. 253–294.

⁴² United Nations, Human Rights Council, Resolution 28/16, <<http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>>.

⁴³ P. DE HERT and V. PAKONSTANTINO, 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?' (2013) 9(3) *I/S: A Journal of Law and Policy for the Information Society* 272–324. Cf. also DE HERT and PAKONSTANTINO, Ch. 25, in this volume.

2.1.2. *Not only law regulates*

However, not only law regulates. There is a wide repertoire of means, instruments and techniques that are used in regulating social behaviour.⁴⁴ Most classically, in his toolkit for regulation, Hood first distinguished 'detectors' and 'effectors'. The former are meant to obtain information and the knowledge gathered that way will constitute a basis for governmental action executed with the help of the latter. Second, in 'detecting' and 'effecting' government possesses four types of resources: nodality (i.e. information), treasure (i.e. financial resources), authority (i.e. legal power) and organisation (i.e. human resources, materials, equipment).⁴⁵

But it was Lawrence Lessig who, among law and technology scholars, offered a classic theory of regulation. His 'pathetic dot theory' looks at constraints of human behaviour. Lessig distinguishes four modalities that regulate human behaviour: law, social norms, market, and architecture (code).⁴⁶ The novelty of his theory, at the time it was proposed in 1990s, was that the computer code regulates similarly to architecture and thus 'regulation in cyberspace may be perfectly achieved through modifications to software codes'.⁴⁷ Both physical architecture and computer code constrain some behaviour by making other behaviour possible or impossible. Equally, as one enters a room through a door (sometimes, through a window, but that is not a standard behaviour), one may equally need some credentials to log in to a certain online service. (One may try to hack it, but that is not a standard behaviour either.)

More generally, political scientists like Morgan and Yeung classify modalities of regulation in five categories: command and control (i.e. rule-based coercion), competition and economic instruments (i.e. 'competitive forces arising from rivalry between competing units', like taxes, charges or subsidies), consensus (i.e. co-regulation or self-regulation), communication (i.e. persuasion and education) and techno-regulation (code) (i.e. elimination of undesired behaviour by 'designing out the possibility for its occurrence').⁴⁸ Freiberg goes further and distinguishes six main modalities, i.e. economic tools, transactional regulation, authorisation, structural regulation (i.e. manipulation of physical environment), informational regulation and legal regulation.⁴⁹ In comparison with modalities mentioned earlier, Freiberg considers transactional regulation and authorisation as standalone. By transactional means he understands 'regulation by contract, grant agreement or other financial arrangement' made in the public interest. This

⁴⁴ B. MORGAN and K. YEUNG, *An Introduction to Law and Regulation: Text and Materials*, Cambridge University Press, Cambridge 2007, p. 79.

⁴⁵ HOOD, above n. 10, pp. 2–6.

⁴⁶ L. LESSIG, *Code Version 2.0*, Basic Books, New York 2006, pp. 121–123, <<http://www.codev2.cc/download+remix/Lessig-Codev2.pdf>>.

⁴⁷ MORGAN and YEUNG, above n. 44, p. 102.

⁴⁸ *Ibid.*, pp. 79–149.

⁴⁹ FREIBERG, above n. 12, pp. 84–87.

form of regulation is based not on public authority exercised by the government, but on the equality of parties, known from contract law.⁵⁰ By authorisation he understands the power of the government to 'authorise, permit, allow or recognise or legitimate a particular activity, status or premises'.⁵¹

All these theories converge and what actually matters is 'picking the' right tool(s) 'for the job' and 'for the times'.⁵² These tools are not mutually exclusive, each of them can be used for diverse purposes, each produces the best effects in different contexts, and each has their own advantages and disadvantages as well as benefits and dangers.⁵³

2.2. BEYOND REGULATION⁵⁴

2.2.1. Organisational protections

Regulatory means do not exhaust the available toolkit of privacy protections. There exists a wide repertoire of organisational and technological means. Such measures are applied in many domains of life, from airports (e.g. security screening) to road traffic (e.g. speed limits), but – for my purposes – it is the theory of information security that is illustrative.⁵⁵ Specialists in the field would usually claim that information security is about protecting 'confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission'.⁵⁶ In other words, they would talk about a classical model of the 'CIA triad', in which each element represents a fundamental objective of information

⁵⁰ Ibid., p. 132.

⁵¹ Ibid., p. 141.

⁵² HOOD, above n. 10, pp. 7–11.

⁵³ D. KLOZA, N. VAN DIJK and P. DE HERT, 'Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies' in F. SKOPIK and P. SMITH (eds.), *Smart Grid Security. Innovative Solutions for a Modernized Grid*, Elsevier, Waltham MA 2015, p. 31.

⁵⁴ I am particularly indebted to Roger Clarke for his guidance on this matter.

⁵⁵ The notion of 'security' has multiple meanings. For example, scholars of international relations usually work with a definition of 'security' that involves 'the alleviation of threats to cherished values' (P.D. WILLIAMS, *Security Studies: An Introduction*, Routledge, Abingdon 2012, p. 1), affecting – according to one typology – five sectors: military, political, social, economic and environmental (B. BUZAN, *People, States and Fear: The National Security Problem in International Relations*, University of North Carolina Press, Chapel Hill 1983). For computer scientists, 'information' is one of those 'cherished values' and for them 'security' is about minimising 'the risk of exposing information to unauthorised parties' (H.S. VENTER and J.H.P. ELOFF, 'A Taxonomy for Information Security Technologies' (2003) 22(4) *Computers and Security* 299). Various aspects of security are in diverse relations with 'data privacy'. In particular, while 'security' of personal data is a requirement of 'data privacy', 'security' of a state is channelled by 'data privacy'. In the former type of relations, 'security' is at the service of 'data privacy', in the latter – 'security' is usually confronted with 'data privacy'.

⁵⁶ M.E. WHITMAN and H.J. MATTORD, *Principles of Information Security*, Cengage Learning, Boston 2012, p. 8.

security. Confidentiality refers to the restriction of access to information only to those who are authorised to use it, integrity – to the assurance that information has not been altered in an unauthorised way and availability – to the assurance that the service will be available whenever it is needed.⁵⁷

The 'CIA triad' is clearly a data-centric security model, yet it is often criticised for simplicity, as more is at stake when it comes to the security of information handling. This created a critical need to coin alternatives to the 'CIA triad' and the many proposals developed include, *inter alia*, the 'Parkerian Hexad',⁵⁸ the 1992 OECD security guidelines (revised 2002 and 2015),⁵⁹ national manuals – such as 'Engineering Principles for Information Technology Security' (2004) by the US National Institute of Standards and Technology (NIST),⁶⁰ 'Information Security Manual' by the Australian Signals Directorate (ASD) (2016),⁶¹ '10 Steps to Cyber Security' by the UK's National Cyber Security Centre (2016)⁶² – and, eventually, the ISO 27001 series of standards.⁶³ Each of them usually expand the 'CIA triad' by adding further principles and among these models the one offered by the NIST is perhaps the broadest, listing 33 such principles, adding e.g. an assumption of insecurity (principle no. 6) and the ease of use (principles nos. 12–15).

The principles of information security – such as the CIA triad – are effectuated by particular, concrete safeguards and controls.⁶⁴ They are meant to successfully counter attacks, reduce risk, resolve vulnerabilities and otherwise improve the security of information.⁶⁵ According to one classification, they could be proactive (i.e. aiming at avoidance, deterrence and prevention of a threat), reactive (detection of, recovery after and insurance against a threat)

⁵⁷ M. RHODES-OUSLEY, *Information Security The Complete Reference, Second Edition*, McGraw-Hill, London 2013, pp. 85–86.

⁵⁸ D.B. PARKER, *Fighting Computer Crime*, Scribner, New York 1998, pp. 230–239.

⁵⁹ OECD, *Guidelines for the Security of Information Systems and Networks*, Paris 2002, <<http://www.oecd.org/sti/ieconomy/15582260.pdf>>; OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, Paris 2015, <<http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>>.

⁶⁰ G. STONEBURNER, C. HAYDEN and A. FERGINGA, 'Engineering Principles for Information Technology Security (A Baseline for Achieving Security)' (2004) *NIST Special Publication 800-27 Rev A.*, <<http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>>, pp. 6–22.

⁶¹ AUSTRALIAN SIGNALS DIRECTORATE, *Australian Government Information Security Manual*, Canberra 2016, <<http://www.asd.gov.au/infosec/ism/index.htm>>.

⁶² NATIONAL CYBER SECURITY CENTRE, *10 Steps to Cyber Security*, London 2016, <<http://www.ncs.gov.uk/guidance/10-steps-to-cyber-security>>.

⁶³ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, *ISO/IEC 27001 – Information security management*, Geneva 2009–2013, <<http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>>.

⁶⁴ The distinction between these two terms in information security literature is rather problematic. While some general meaning was asserted to 'controls', the more accurate term would be 'safeguards' because 'controls' are 'second-level safeguards that ensure that intended safeguards are actually in place and working' (Roger Clarke in a private correspondence, September 2016).

⁶⁵ WHITMAN and MATTORD, above n. 56, p. 10.

as well as non-reactive, i.e. tolerance.⁶⁶ According to another, they could be of organisational or technological nature.

Organisational means concern the set-up of an entity handling information. An organisation, at a *general* level, would usually resort to e.g. procedural (administrative) safeguards, such as internal policies, standards and guidelines spelling out rules, roles and responsibilities for handling information. It would as well resort to physical, 'bricks and mortar' security of premises and of equipment handling information, such as fences, doors and locks. Security would receive adequate attention at the senior level of an organisation, e.g. by a dedicated officer with oversight powers. Staff would be continuously updated on developments in the area and information handling systems would be kept up-to-date and continuously tested against vulnerabilities. Eventually, backup copies would be made and business continuity strategies would be put in place. Seemingly trivial issues such as the provision of supporting utilities (e.g. energy supply or cooling system) and protection against the fire belong to this category too.

At a more *concrete* level, an organisation would e.g. employ restrictions as to the physical or temporal access to information. It would differentiate access thereto depending on a given, clearly defined role of a member of staff. It might restrict access to some particular workstations. An organisation would further employ multi-factor authentication with 'strong' passwords, comprising a combination of lower- and upper-case letters, numbers and signs, supplemented by other forms of identification, e.g. a token. It would decentralise all data storage (i.e. 'you don't put all your eggs in one basket'). Ultimately, it would register all the information handling operations. Such a log is vital for the purposes of accountability yet it also allows to look for patterns for anomalies, e.g. whether an employee accesses database outside normal hours of business and whether it was justified. All in all, a lot of security in practice is about 'logical access restrictions'.⁶⁷

The same organisation, at a *product* level, would aim at ensuring security 'by design'. This idea shares parallels with 'Privacy by Design' (cf. below, in this section) by departing from a paradigm that security is 'not an afterthought' and 'it has to be an integral part of any development project'.⁶⁸ In a classical understanding, 'implementation without security flaws' can be guided by eight foundational principles,⁶⁹ i.e.:

1. Economy of mechanism: keep the design as simple and small as possible.
2. Fail-safe defaults: base access decisions on permission rather than exclusion.

⁶⁶ R. CLARKE, 'Practicalities of Keeping Confidential Information on a Database With Multiple Points of Access: Technological and Organisational Measures', 1992, <<http://www.anu.edu.au/people/Roger.Clarke/DV/PaperICAC.html>>.

⁶⁷ Ibid.

⁶⁸ P. SIRIWARDENA, 'Security by Design' (2014) 58 *Advanced API Security* 11–31.

⁶⁹ J. SALTZER, and M. SCHOEDER, 'The Protection of Information in Computer Systems', 1974, sec. 1, <<http://web.mit.edu/Saltzer/www/publications/protection/>>.

3. Complete mediation: every access to every object must be checked for authority.
4. Open design: the design should not be secret.
5. Separation of privilege: where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.
6. Least privilege: every program and every user of the system should operate using the least set of privileges necessary to complete the job.
7. Least common mechanism: minimise the amount of mechanism common to more than one user and depended on by all users.
8. Psychological acceptability: it is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

The narrative of a data-centric security model would be normally applicable to the protection of privacy as long as personal information is being handled. (Note that organisational measures are not exclusive to data privacy, e.g. medical doctors normally receive each of their patients individually in an examination room behind closed doors. This is meant to protect aspects of privacy other than personal data.)⁷⁰ In many jurisdictions, security of data being handled is a requirement of data privacy law. Yet, contrary to the popular belief amongst the specialists in the field, information security does not equal data privacy, as for the latter there is more at stake.

Translating all these into the privacy universe, organisational protections include methods, techniques and measures such as:

- Privacy by Design (PbD);⁷¹
- privacy impact assessment (PIA),⁷² privacy risk management and other evaluative techniques;

⁷⁰ Cf. below n. 195.

⁷¹ The writings on each of these methods are voluminous and thus only basic 'textbooks' will be cited here. The concept of Privacy by Design was coined in 1990s by Ann Cavoukian, then Information and Privacy Commissioner of Ontario, Canada and is best described on a dedicated website, <<http://www.privacybydesign.ca>>. Cf. further esp. A. CAVOUKIAN, *Privacy by Design in Law, Policy and Practice. A White Paper for Regulators, Decision-Makers and Policy-Makers*, Information and Privacy Commissioner, Ontario, Toronto 2011, pp. 6–13.

⁷² There are many definitions of privacy impact assessment. One of the most comprehensive is the following: a PIA is a systematic, continuous as well as reasonably accountable, transparent and participatory activity of analysing (identifying, evaluating and proposing measures for mitigation of) consequences (positive and negative; intended and unintended) of a single initiative (*sensu largo*) on (a) given benchmark(s), if this initiative presents significant risks to the benchmark(s), with a view to support the informed decision-making as to the deployment of this initiative and its scale, constituting a means to protect the benchmark(s). Cf. further e.g. R. CLARKE, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25(2) *Computer Law & Security Review* 123–135; R. CLARKE, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (2011) 1(2) *International Data Privacy Law* 111–120; D. WRIGHT,

- privacy seals and certification;⁷³
- privacy icons (pictograms);⁷⁴
- privacy standardisation;⁷⁵
- privacy audits;
- appointment of a dedicated senior officer to oversight privacy matters, e.g. data protection officer (DPO), as it is known in Europe, or Chief Privacy Officer (CPO), as known in the Americas.

2.2.2. Technological protections

Technological protections are rather self-evident. Their generic categories can include, for example, access controls (e.g. two-factor authentication) and the use of cryptography as well as a wider range of measures against malware and otherwise hostile software (i.e. detection and eradication), against hostile takeover of an information system (i.e. firewalls) or against the insecurity of remote connections, e.g. virtual private networks (VPN).⁷⁶ These protections build on a premise that technology can invade individual interests but it can equally be used to counter such an invasion.

Translating all these into the privacy universe, technological protections manifest themselves predominantly by the so-called Privacy Enhancing Technologies (PETs). PETs constitute a 'system of [information and communications technologies] measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system'.⁷⁷ The concept of PETs was put together in 1995 in a join research paper of Canadian and Dutch data protection authorities and

'The State of the Art in Privacy Impact Assessment' (2012) 28(1) *Computer Law & Security Review* 54–61; D. WRIGHT and P. DE HERT (eds.), *Privacy Impact Assessment*, Springer, Dordrecht 2012; P. DE HERT, D. KLOZA and D. WRIGHT, 'Recommendations for a Privacy Impact Assessment Framework for the European Union', Deliverable D3 of the PIAF [A Privacy Impact Assessment Framework for data protection and privacy rights] project, Brussels/London 2012, <http://piafproject.eu/ref/PIAF_D3_final.pdf>; KLOZA, VAN DIJK and DE HERT, above n. 53, pp. 11–47).

⁷³ Cf. e.g. R. RODRIGUES, D. BARNARD-WILLS, D. WRIGHT, P. DE HERT and V. PAPA-KONSTANTINO, *EU Privacy Seals Project. Inventory and Analysis of Privacy Certification Schemes*, Publications Office of the European Union, Luxembourg 2013, pp. 100–116.

⁷⁴ Cf. e.g. M. HANSEN, 'Putting Privacy Pictograms into Practice: A European Perspective' (2009) 154 *GI Jahrestagung* 1703–1716.

⁷⁵ Cf. e.g. P. DE HERT, V. PAPA-KONSTANTINO and I. KAMARA, 'The Cloud Computing Standard ISO/IEC 27018 through the Lens of the EU Legislation on Data Protection' (2016) 32(1) *Computer Law & Security Review* 16–30.

⁷⁶ R. CLARKE, 'The Prospects of Easier Security for Small Organisations and Consumers' (2015) 31(4) *Computer Law and Security Review* 538–552.

⁷⁷ G.W. VAN BLARKOM, J. BORKING and J. OLK, *Handbook of Privacy and Privacy-Enhancing Technologies. The Case of Intelligent Software Agents*, College Bescherming Persoonsgegevens, The Hague 2003, p. 33.

originally was concerned with protecting privacy by pseudo-identities.⁷⁸ These technologies can be applied both by those who handle data and by those whose data are being handled (i.e. end-user PETs). The toolkit of PETs has expanded significantly ever since and nowadays it considers the application of categories technologies such as:

- de-identification of information: anonymisation, and especially randomisation (such as noise addition, permutation and differential privacy) and generalisation (such as aggregation, K-anonymity and L-diversity);⁷⁹
- pseudonymisation;
- cryptography, including strong, end-to-end encryption, be it symmetric, asymmetric or fully homomorphic;⁸⁰
- (multi-factor) identification, authentication and authorisation;
- decentralisation;
- techniques for data erasure;
- techniques for un-linkability and non-traceability;
- protection against malicious software (malware), e.g. anti-virus software;
- specific protocols, e.g. Platform for Privacy Preferences (P3P).⁸¹

Some other catalogues of PETs focus on practical tools that a layman on the street can apply, for example:⁸²

- device-management tools, e.g. live operating systems, file encryption and erasing software, password vaults;

⁷⁸ Ibid., p. 36; R. HES and J. BORKING, *Privacy-Enhancing Technologies: The Path to Anonymity*. Achtergrondstudies En Verkenningen. Registratiekamer, 1995, <<https://www.ipc.on.ca/images/Resources/anoni-v2.pdf>>.

⁷⁹ Cf. Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, WP 216, Brussels, 10 April 2014, pp. 11–19, 27–37, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

⁸⁰ Cf. C. GENTRY, 'Fully Homomorphic Encryption Using Ideal Lattices' (2009) 19 *Proceedings of the 41st Annual ACM Symposium on Symposium on Theory of Computing STOC 09*, 169–178.

⁸¹ Cf. <<http://www.w3.org/P3P>>.

⁸² R. CLARKE, 'Key Factors in the Limited Adoption of End-User PETs', 2014, <<http://www.rogerclarke.com/DV/UPETs-1405.html>>, fig. 1. The Electronic Privacy Information Center (EPIC) offers an *Online Guide to Practical Privacy Tools*, <<https://epic.org/privacy/tools.html>>, the Electronic Frontier Foundation (EFF) offers a *Surveillance Self-Defence Kit*, <<https://ssd.eff.org/en>>, the Centre for Internet and Society at Stanford University offers, in the form of a wiki, 'a list of free technologies aimed at empowering Internet users to gain better control over their data', <<http://cyberlaw.stanford.edu/wiki/index.php/PET>>, and Douglas Crawford has recently published his *Ultimate Privacy Guide*: <<https://www.bestvpn.com/the-ultimate-privacy-guide>>.

- traffic-related tools, e.g. Internet anonymisers, Virtual Private Networks (VPNs), proxy servers, firewalls, anti-malware software;
- web-related tools, e.g. web browser ad-ons, cookie/cache/Internet history cleaners, privacy friendly search engines and social networking sites;
- email-related tools, e.g. e-mail encryption, alternative e-mail accounts, anonymous remailers;
- other communications-related tools, e.g. secure instant messaging, Voice over Internet Protocol (VoIP) and video messaging; temporary mobile phones;
- other, e.g. alternative currencies or blind digital signatures.

This classification is obviously not watertight and when all protections work together, the distinction between them is rather nominal. Each of the three categories of protection – regulatory, organisational and technological – complement each other and often overlap. (One particular protection measure might belong to more than one type.) Further, these protections are interrelated and affect each other: regulation (e.g. laws or standards) may require the use of specific organisational and technological measures. For example, the recently passed GDPR in the EU requires a form of PIA to be conducted for certain information handling and further mandates data privacy to be protected ‘by design’. In some instances, both organisational and technological can have a regulatory effect, in a sense of Lessig’s ‘pathetic dot theory’ – they make certain actions or inactions (im)possible by requiring or ruling out some other. While regulatory protections are offered top-down, i.e. usually from the state, the organisational and technological are usually offered bottom up, i.e. from non-state actors. Finally, diverse protections would find diverse applications among various stakeholders. An organisation would pursue the goals of Privacy by Design and to that end would conduct a privacy impact assessment. A layman on the street would be rather interested in secure instant messaging software, offering strong, end-to-end encryption. Should she decide to discontinue using a particular service, she would exercise her right to object the processing of personal data.

3. INADEQUACIES OF CONTEMPORARILY AVAILABLE TOOLS FOR PRIVACY PROTECTION

3.1. INTRODUCTION: IRREVERSIBILITY OF HARM

The underlying problem of privacy protection is that of the irreversibility of harm. It manifests itself clearly with the informational aspect (type) of privacy. The mere fact a piece of *personal* information is being handled – be it collected, analysed, stored and destroyed, or whatever else operation thereon – constitutes an interference with and – possibly – a threat to the interests of an individual and,

in some instances, to those of a society.⁸³ (The best way to protect individuals and societies would be not to handle any information at all. Under such a paradigm, our societies would never work.) Such a piece of information might be disclosed without any good reason or authorisation, it might be used against the will of that person, thus in any case creating some degree of harm. Equally it all might go well: all handling would be secure enough and conducted in an interest of that particular person or in an interest of a given society, causing no harm of any nature nor scale to anybody. But, equally, it might all go wrong: a piece of information might be used against someone or may be revealed to a person, or perhaps worse, to a society, not intended to know it. Information once released, especially in the digital era, will circulate freely and would never be erased. Therefore, in this sense, a disclosure of personal information is irreversible. It follows that the consequences of such a disclosure rarely can be repaired, therefore making privacy harms irreparable. I hasten to explain that here I understand 'harm' rather broadly. Even if damage can largely be repaired with money, the significance of *mental* harm is much higher and no compensation can provide any relief thereto.

For example, I find ironic the famous battle Mr Mario Costeja fought in 2010–2014 to have some of his personal information removed from a search engine listing. In 1998, 'an announcement mentioning his name appeared [in one of the major Catalan newspapers] for a real-estate auction connected with attachment proceedings for the recovery of social security debts'.⁸⁴ The case 'has been fully resolved for a number of years and that reference [thereto] was now entirely irrelevant'.⁸⁵ It would probably be forgotten if the publisher had not decided to digitalise the archives of a newspaper, make them publicly available on the Internet and – what is crucial here – searchable by a machine.

⁸³ Cf. further the classical 'interference argument' by Adalbert Podlech coined in 1970s when the Western German doctrine of personal data protection was growing mature: '... jede Erhebung, Speicherung, Verarbeitung und Weitergabe personenbezogener durch Träger öffentlicher Gewalt in einem formellen Verfahren ein Eingriff in das durch Art. 2 Abs. 1 [Grundgesetz] gewährleistete informationelle Selbstbestimmungsrecht ist' (in essence: on the grounds of the German Constitution, any formal handling of personal data by public authorities constitutes an interference with the right to informational self-determination). A. PODLECH, 'Das Recht auf Privatheit' in J. PERELS (ed.), *Grundrechte als Fundament der Demokratie*, Suhrkamp, Frankfurt am Main 1979, p. 55. The concept of informational self-determination entered the Western German legal system with the famous 1983 population census decision of the Federal Constitutional Court (Bundesverfassungsgericht). BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u.a. – *Volkszählung*. Cf. further G. HORNING and C. SCHNABEL, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25 *Computer Law and Security Review* 84–88. I thank Frederik Zuiderveen Borgesius for bringing this matter to my attention.

⁸⁴ Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González (CJEU, 13 May 2014), §14.

⁸⁵ *Ibid.*, §15.

Notwithstanding the Luxembourg Court ruling in his favour,⁸⁶ nowadays putting the name of Mr Costeja into this particular search engine yields roughly 20,000 results.⁸⁷ Not only was his information searchable before he entered the courtroom, but the media attention the case received made the specific piece of information, which he wanted to hide, more widely known than before. Given the relevance of the Court's ruling, the Spanish data protection authority (DPA) found the facts behind the case to be in the public interest. This authority therefore eventually denied him a right to de-list, at a search engine, the many links to contents commenting on the case.⁸⁸ As a result, Mr Costeja's case sits comfortably in the category of the 'Barbara Streisand effect', i.e. a phenomenon in which an attempt to hide something produces exactly the reverse effect, facilitated by the use of technology.⁸⁹

The Court of Justice has created – or interpreted? – 'the right to be forgotten' (or rather 'the right to de-listing'), yet the efficiency of such a right today is highly questionable. This has to do with the way information and communications technologies (ICTs) function.⁹⁰ They work by copying information, by doing it fast and – normally – by allowing anybody to do so; this is their primary *modus operandi*. These copies are multiple, untraceable and thus uncontrollable. Asking a service provider, like Google, to remove certain links from its search engine results is efficient as it removes a major access point to the contested piece of information. But it does not remove this piece of information from a server on which it is stored. (In that case, it is a website of a newspaper which digitalised its archives.) Nor does it remove this information from proxy servers, from backup servers or from webpages archives. Google complies with the ruling and – upon receipt of a justified request – removes information from the results when these are sought from within the European territory. Accessing Google from e.g. Australia has produced unfiltered results. Mayer-Schönberger once famously advocated for an expiration date on a piece of information, as a solution to the problem of the infinite memory of ICTs.⁹¹ Immediately a market has been

⁸⁶ Ibid.

⁸⁷ As of the end of September 2016.

⁸⁸ Agencia Española de Protección de Datos (AEPD), Resolución No. R/02179/2015, Madrid, 14 September 2015, <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2015/common/pdfs/TD-00568-2015_Resolucion-de-fecha-14-09-2015_Art-ii-culo-16-LOPD.pdf>.

⁸⁹ E. MOROZOV, *The Net Delusion: The Dark Side of Internet freedom*, Public Affairs, New York 2012, pp. 120–123.

⁹⁰ I set aside here the debate on the impact of the right to be forgotten on the freedom of expression as this is a separate matter. Cf. further J.P. MIFSUD BONNICI and A.J. VERHEIJ, 'On Forgetting, Deleting, de-Listing and Starting Afresh!' (2016) 30(1–2) *International Review of Law, Computers & Technology* 1–4.

⁹¹ V. MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton 2009, pp. 171–173.

created for that: in 2011 a German company X-Pire offered software that added a self-destruction feature to one's pictures.⁹²

My point is that the law – or, broader, regulation – is helpless in such a situation. I am aware it is a strong statement. It cannot normally forbid digitalisation of written media like newspapers (it is against the freedom of expression and a few other freedoms and liberties), it cannot compel multinational companies outside a given jurisdiction to obey (extraterritorial jurisdiction is still relatively limited, despite recent attempts to extend the territorial scope of data privacy laws),⁹³ and it cannot prohibit media from reporting on a pending court case (again, the freedom of expression). Mr Costeja resolved to regulatory protections, but the law does not solve his problem now, nor is it capable of solving it in any foreseeable future. Other types of protections – organisational and technological – were of little use in his situation. The conclusion must be that the contemporarily available tools for privacy protection are inadequate.

3.2. INADEQUACIES

3.2.1. *Regulatory tools*

3.2.1.1. Inefficiency of contemporary regulation

How do the inadequacies of contemporarily available regulatory protections manifest themselves? I see these inadequacies as having at least a four-fold nature. First, it is the *inefficiency* of contemporary regulation, including the law. Second, it is the inability to keep pace with societal and technological developments. Third, it is the instrumental use of regulation. Fourth and finally, it is the diminishment of public trust.

The narrative of human rights is perhaps the most useful starting point to illustrate the inefficiency of contemporarily available regulatory protections. The European Convention on Human Rights confers on the individuals a number of enforceable human rights and the one that interests me here is the right to privacy.⁹⁴ The enjoyment of any rights conferred by the said Convention

⁹² Cf. <<http://petapixel.com/2011/01/17/x-pire-software-adds-a-self-destruct-feature-to-your-digital-photos>>.

⁹³ Cf. e.g. L. MOEREL, 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?' (2011) 1(1) *International Data Privacy Law* 28–46; D.J.B. SVANTESSON, *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing, Copenhagen 2013; and P. DE HERT and M. CZERNIAWSKI, 'Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context' (2016) 6(3) *International Data Privacy Law* 230–243.

⁹⁴ Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950, ETS 5.

is governed by a number of 'meta-principles'. First and foremost, its opening Article declares that the contracting parties 'shall secure to *everyone* within their jurisdiction the rights and freedoms defined [in the] Convention'.⁹⁵ Then the Convention goes on, enumerating 11 substantive rights and Art. 8 deals with the right to privacy. A wide range of 'meta-principles' comes back from Art. 13 onwards: itself, this provision proclaims the right to effective remedy, Art. 14 prohibits discrimination,⁹⁶ Art. 15 allows for limited derogations in the time of emergency, Art. 16 restricts political activity of non-citizens, Art. 17 prohibits the abuse of rights and Art. 18 puts limits on the restriction of rights. The subsequent Articles of the Convention establish the European Court of Human Rights and define its functioning. Finally, Art. 53 states that the Convention does not restrict the level of protection, i.e. it does not limit or derogate any right if national laws and/or other international instruments provide for a higher standard of protection.

Subsequent 'meta-principles' have been added by the judges in Strasbourg. On a numerous occasions and most recently in *Nježić and Štimac v. Croatia* (2015), the Court held that the 'object and purpose of the Convention as an instrument for the protection of individual human beings require that [its provisions] be interpreted and applied so as to make its safeguards *practical* and *effective*'.⁹⁷ With my collaborators, I have argued elsewhere that such a protection must also be *efficient*. While effectiveness indicates a 'possibility or capability of producing a result', efficiency goes a step further and indicates a possibility or capability of 'functioning or producing effectively and with the least waste of effort'.⁹⁸ In *X and Y v. the Netherlands* (1985), the Strasbourg Court held that a state can 'in certain circumstances' be 'responsible for the acts of third parties', thus adopting the German doctrine of *Drittwirkung* to European human rights.⁹⁹ In result, the state is obliged to afford practical and effective protection to all individuals within its jurisdictions, be it its relations with individuals (vertical effect) or in relations between the individuals themselves (horizontal effect).

Translating these to the privacy universe, the currently available regulatory protections often do not live up to these standards. Looking solely at the example of the EU data privacy regulation, the 1995 Data Protection Directive¹⁰⁰ fell victim to many troubles stemming from EU decision-making, suffering from a lack of sufficient quality as well as complexity, slowness and being 'hostage to

⁹⁵ Emphasis mine.

⁹⁶ Cf. also Art. 1 of Protocol No. 12 to the ECHR.

⁹⁷ *Nježić and Štimac v. Croatia*, App. no. 29823/13 (ECtHR, 9 April 2015), §61. Emphasis added.

⁹⁸ KLOZA and GALETTA, above n. 29, p. 4. Collins English Dictionary, <<http://www.collinsdictionary.com>>.

⁹⁹ *X and Y v. the Netherlands*, App. no. 8978/80 (ECtHR, 26 March 1985), §33.

¹⁰⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31–50.

the lowest common denominator'.¹⁰¹ The Directive was a political compromise build upon diverse experience of several EU Member States with regulating the processing of personal data.¹⁰² Furthermore, its dual aim of establishing internal market and protecting fundamental rights eventually caused doubts as to the validity of its legal basis.¹⁰³ Despite the Directive offering significant protections at the time of its enactment and transposition deadline (1998), compared *avant la lettre*, it has quickly become outdated.

A proposal for its replacement in entirety – i.e. the General Data Protection Regulation – was tabled in January 2012, predominantly to keep pace with the development of emerging technologies,¹⁰⁴ and signed into law in April 2016.¹⁰⁵ Despite great enthusiasm about the proposed text, expressed initially as a 'Copernican revolution'¹⁰⁶ and eventually as 'still a sound system for the protection of individuals',¹⁰⁷ many commentators observed that either the new Regulation would not solve existing problems or it would create new ones. Blume, for example, speaks of an 'illusion of a higher level of protection' that would result from the entry into force of GDPR.¹⁰⁸ Koops, highly critical, further argues that the direction of the data protection reform is fundamentally flawed for at least three reasons: (1) the individual's control over their data is a delusion, (2) so too is the conception that the reform simplifies the law, and (3) an attempt of comprehensiveness, i.e. to regulate all in a single statute, has failed.¹⁰⁹ Anecdotally, in a private conversation held in mid-2015 in Brussels, a representative of an office of a DPA in Europe joked that she would move to Morocco once the GDPR was passed, as Morocco would then offer a higher level of protection of privacy. The truth is most probably somewhere

¹⁰¹ J. ZIELONKA, *Is the EU Doomed?*, Polity, Cambridge 2014.

¹⁰² MAYER-SCHÖNBERGER, above n. 20, pp. 234–36.

¹⁰³ O. LYNKEY, 'From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis' in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht 2013, pp. 59–84.

¹⁰⁴ Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.01.2012, COM(2012) 11 final.

¹⁰⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1–88.

¹⁰⁶ C. KUNER, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (2012) 11(6) *Privacy and Security Law Report* 1–15.

¹⁰⁷ P. DE HERT and V. PAPAKONSTANTINOY, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32(2) *Computer Law & Security Review* 179–194.

¹⁰⁸ P. BLUME, 'The Myths Pertaining to the Proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 269–273.

¹⁰⁹ B.-J. KOOPS, 'The Trouble with European Data Protection Law' (2014) 4(4) *International Data Privacy Law* 250–261.

in-between. Davies recently reflected on the GDPR's final version that 'in spite of shortcomings, disappointments and lost opportunities, [it] should provide a more robust infrastructure of rights protection'.¹¹⁰

Regulatory inefficiencies could be also demonstrated by examining the quality of legal norms. Many legal instruments suffer from complexity and difficulty-to-navigate, making them 'anything but straightforward'¹¹¹ and the EU data protection law is no exception. It is hard not to recall Fuller's classical 'eight ways to fail to make law', i.e. his conditions of good law-making:

The first and most obvious lies in a failure to achieve rules at all, so that every issue must be decided on an *ad hoc* basis. The other routes are: (2) a failure to publicise, or at least to make available to the affected party, the rules he is expected to observe; (3) the abuse of retroactive legislation, which not only cannot itself guide action, but undercuts the integrity of rules prospective in effect, since it puts them under the threat of retrospective change; (4) a failure to make rules understandable; (5) the enactment of contradictory rules or (6) rules that require conduct beyond the powers of the affected party; (7) introducing such frequent changes in the rules that the subject cannot orient his action by them; and finally, (8) a failure of congruence between the rules as announced and their actual administration.¹¹²

Kuner has applied these to the European data protection law as in force in 1998, concluding the lack of rules to address certain problems, lack of public awareness of data privacy law, lack of clarity, contradiction of rules and failure of congruence between the rules and their administration.¹¹³

3.2.1.2. Ever-changing nature of the object of protection and of the context

The second reason to judge the contemporarily available regulatory protections as inadequate is the *ever-changing* nature of both the object of protection and the context in which the protection of this object is sought. Innovation and technology are regulated for two reasons. First, we want to stimulate the progress of both, and thus – indirectly – the progress of society in general. This objective justifies all public funding for research and development or all public efforts to create a stimulative environment for technology companies and start-ups, e.g. by reducing red-tape or offering affordable loans. Second, we want to eliminate or at least minimise those consequences of innovation and technology that we

¹¹⁰ S. DAVIES, 'The Data Protection Regulation: A Triumph of Pragmatism over Principle?' (2016) 3 *European Data Protection Law Review* 290–296, <http://edpl.lexxion.eu/data/article/10075/pdf/edpl_2016_03-006.pdf>.

¹¹¹ J. ZIELONKA, *Is the EU Doomed?*, Polity, Cambridge 2014, p. 40.

¹¹² L.L. FULLER, *The Morality of Law*, Yale University Press, New Haven 1964, p. 39.

¹¹³ C. KUNER, 'The "Internal Morality" of European Data Protection Law', 2008, pp. 10–15, <<http://ssrn.com/abstract=1443797>>.

consider negative, and thus – indirectly – eliminate or minimise harm of any nature to society and each individual member thereof, preferably before it occurs. This objective thus justifies all public transportation safety and security rules, e.g. speed bumps, although their efficiency might merit a separate discussion.

Following this perspective, regulation can be interpreted as an activity of putting a 'thin red line' between what we, as a society, want or desire and what we do not want nor desire. Such regulation would have been easy if innovation and technology, the society and their needs and desires, were of a *constant* nature. Conversely, they constantly *change*. They both progress on their own pace and these do not necessarily synchronise nor converge. Both the society and innovation and technology develop faster than regulation. Moore's Law is a perfect example thereof: Moore's predication that the number of transistors in a dense integrated circuit doubles approximately every two years have 'transformed computing from a rare and expensive venture into a pervasive and affordable necessity',¹¹⁴ causing – at the same time – a need to re-invent (a lot of) the law. The question whether the regulation of cyberspace – at the time when these technologies were emerging – requires a dedicated branch of law caused in the late 1990s a seminal debate on the 'law of the horse'.¹¹⁵ Furthermore, in the early 2000s, globalisation proved regulation solely at a national level to be inefficient, thus leading Beck to conclude that global risks require global responses.¹¹⁶ To add to this complication, what a given society needs or desires is not static and what is acceptable varies by cultures, contexts and time.

3.2.1.3. Instrumentalisation of regulation

The third reason for inadequacy is the *instrumentalisation* of regulation, including the law. I have analysed in section 2 that those who regulate have at their disposal a wide repertoire of tools for that purpose. Therefore the act of regulation requires a *choice* of an appropriate tool or of a combination of tools that would fit the purpose sought in a given context and in a given time. Such a choice is never simple and the main criterion of its evaluation is that whether a choice made is good or not.

Those who regulate have a complex decision to make if they want their choices to be judged good. Hood suggests four canons of good application of

¹¹⁴ G.E. MOORE, 'Cramming More Components onto Integrated Circuits' (1965) 38(8) *Electronics* 82–85. Cf. <<http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html>>.

¹¹⁵ F.H. EASTERBROOK, 'Cyberspace and the Law of the Horse' (1996) *University of Chicago Legal Forum* 207–217; L. LESSIG, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113(2) *Harvard Law Review* 501; L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, New York 1999.

¹¹⁶ U. BECK, 'The Cosmopolitan Condition: Why Methodological Nationalism Fails' (2007) 24(7–8) *Theory, Culture & Society* 286–290. I thank Paul De Hert for bringing this matter to my attention.

these tools.¹¹⁷ Some prior examinations – to a reasonable extent – of available alternatives would precede the selection of tools to regulate. Next, the tool chosen would match the regulatory goal pursued. The choice would not be ‘barbaric’, in a sense it would satisfy ethical criteria to which a given society subscribes, and – finally – would not waste resources in order to achieve the goals pursued.¹¹⁸

Each of these criteria, however objective they might look *prima facie*, would always involve an aspect of politics. For example, the combination of tools available for achieving a regulatory goal ‘runs into billions or even trillions if one assumes no incompatibilities or mutual exclusivities’. The catalogue changes over time: new tools are being added and others are being abandoned. A fully rational review of alternatives is thus rather impossible in any finite time.¹¹⁹ Furthermore, similarly to regulatory goals pursued, tools for regulation are not value-free. While some might be used for both ‘good’ and ‘bad’ purposes – and thus the context of their application matters – some other clearly belong to the latter category. Here Hood gives an example of an atomic bomb.¹²⁰ It follows that there is no intrinsically good tool for regulation. Therefore those who regulate would base their choices on their experience as well as considerations of ideological and economical aspects that are political in their nature. This in any case does not make their choices simpler: few societies subscribe to a single moral code. Instead, societies have adopted a variety of different ethical and ideological standards. Efficiency of their choices is not only about using least possible resources (time, money, manpower) but also about imposing least burden on those who are regulated. Eventually, their choices will be judged against political criteria of legitimacy (if the public accepts decisions without having to be coerced) and accountability (if and how those who regulate can justify their choices).¹²¹

Despite such complexity in choosing the right tool for regulation, there are instances in which politics will play a decisive role in such a choice. Here I understand ‘politics’ in its derogatory meaning, as an act ‘in the interests of status or power ... rather than as a matter of principle’.¹²² Those who regulate usually have a well-defined political agenda to achieve and this would determine their choices of tools. In other words, tools of regulation will be then used instrumentally and regulation would become a ‘servant of politics’.¹²³

¹¹⁷ HOOD, above n. 10, p. 133.

¹¹⁸ Ibid., pp. 132–152.

¹¹⁹ Ibid., pp. 134–135.

¹²⁰ Ibid., p. 140.

¹²¹ MORGAN and YEUNG, above n. 44, pp. 221–301.

¹²² Oxford Dictionary of English.

¹²³ K. DE VRIES and N. VAN DIJK, ‘A Bump in the Road. Ruling Out Law from Technology’ in M. HILDEBRANDT and J. GAAKEER (eds.), *Human Law and Computer Law: Comparative Perspectives*, Springer, Dordrecht 2013, pp. 89–121; S. GUTWIRTH, P. DE HERT and L. DE SUTTER, ‘The Trouble with Technology Regulation from a Legal Perspective. Why Lessig’s “Optimal Mix” Will Not Work’ in R. BROWNSWORD and K. YEUNG (eds.), *Regulating Technologies*, Hart Publishers, Oxford 2008, pp. 193–218.

Translating these to the privacy universe, tools of regulation might be used equally to protect or to intrude privacy. It is equally possible that a deliberate choice not to regulate or a failure to regulate, such as due to carelessness, may result in an intrusion into privacy for which no protection is available.

3.2.1.4. Diminishing trust in those who regulate, handle information and oversee

This brings me to the fourth and last identified inadequacy of regulatory protections and it is the *diminishing trust* in those who regulate, those who handle information and those who oversee these two.

Trust plays a crucial role in the functioning of social life. If one trusts, she grants some other person or people some discretionary power over something and thus accepts 'some amount of risk for potential harm in exchange for the benefits of cooperation'.¹²⁴ In the theory of democracy, when people have 'given up into the hands of the society, and therein to the governors', they have done so 'with this express or tacit trust, that it shall be employed for their good'.¹²⁵ On a daily basis, trust is 'an elementary fact of social life'.¹²⁶ 'If I am unwilling to trust that the strangers I meet on the street will not mug me, I will be unable to leave my house'.¹²⁷ Similarly, when people have to trade in goods or services, they would prefer that their business partners would refrain from undesirable behaviour.¹²⁸ Therefore the main role of trust is to 'reduce social complexity'¹²⁹ by 'ruling out possible, but undesirable and unfavourable, future actions of other people or organisations'.¹³⁰

With the rise of democracy, people have established trust in those who govern them in a belief that 'the government is capable of bringing about desired outcomes'¹³¹ or – at least – such a government would cause no harm. Yet there is a discrepancy between theory and practice. In late 2016 Eurobarometer reported that only some one-third of Europeans trust in the European Union, and only 27 per cent of them trust in their national governments.¹³² Surveys of American public opinion in 2015 suggest that trust in the federal government

¹²⁴ M.E. WARREN, *Democracy and Trust*, Cambridge University Press, Cambridge 1999, p. 1.

¹²⁵ J. LOCKE, *Second Treatise of Government*, 1690, sec. 1.

¹²⁶ N. LUHMANN, *Trust and Power*, Wiley, Chichester 1979, p. 4.

¹²⁷ WARREN, above n. 124, p. 4.

¹²⁸ D. GEFEN, 'E-Commerce: The Role of Familiarity and Trust' (2000) 28 (6): *Omega* 729.

¹²⁹ LUHMANN, above n. 126, p. 4.

¹³⁰ GEFEN, above n. 128, p. 728.

¹³¹ M.J. HETHERINGTON, *Why Political Trust Matters. Why Trust Matters*. Princeton University Press, Princeton 2004, p. 5.

¹³² EUROPEAN COMMISSION, *Standard Eurobarometer 85: Public opinion in the European Union*, July 2016, p. 14.

varies from 19 per cent to 51 per cent.¹³³ Only 37 per cent of Australians trusted their government in Canberra, and 75 per cent of them claim their federal government fails to contribute to greater good.¹³⁴ Such trust diminishes with each misstep of public authorities and the disclosures in 2013 about global mass surveillance practices played here a vital role. In their aftermath, only 6 per cent of American adults say they are 'very confident' that government agencies can keep their records private and secure, while another 25 per cent say they are 'somewhat confident'.¹³⁵

These surveys clearly indicate the insufficient trust in those who regulate, those who handle information and those who control these two. This lack of trust can have multiple reasons, and one of those is the lack of adequate oversight. The concepts of democracy, the rule of law (*Rechtsstaat*) and fundamental rights require that the judicial branch oversees the activities of two other branches, i.e. legislative and executive. (And that higher instances of this judicial branch oversee the lower instances.) In particular, courts of law are required to respect standards of an open and transparent environment, where cases, reasoning and decisions are made public, unless there is a good reason to keep it secret. This secrecy is rather exceptional and to be interpreted rather narrowly. This way the society trusts in the practice of courts, confident that these institutions would deliver justice.

I can think of a few examples from the privacy universe to illustrate my point. The Foreign Intelligence Surveillance Court (FISC or, colloquially, FISA Court) was established in 1978 to 'hear applications for and grant orders approving electronic surveillance anywhere within the United States'.¹³⁶ The FISA Court is composed of 11 judges sitting *ex parte* to hear from only one side in the case – an agency of a federal government, such as the National Security Agency (NSA). Its deliberations are kept secret and its decisions are rarely made public, short of some statistical data. (These statistics reveal that the FISA Court almost never denies any request for electronic surveillance.)¹³⁷ When a request is denied, a

¹³³ Pew Research Center, 'Beyond Distrust: How Americans View Their Government', November 2015 <<http://www.people-press.org/2015/11/23/1-trust-in-government-1958-2015/>>.

¹³⁴ EDELMAN, *Trust Barometer: Australia*, 2015, <<http://www.edelman.com.au/wp-content/uploads/2015/02/2015-Edelman-Trust-Australia-Results.pdf>>.

¹³⁵ G. GAO, 'What Americans Think about NSA Surveillance, National Security and Privacy', Pew Research Center, 2015, <<http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/>>.

¹³⁶ 50 USC 1803(a)(1).

¹³⁷ In 2015, the federal law enforcement agencies made 1499 applications to the FISA Court of which 1457 included requests for authority to conduct electronic surveillance. One application was withdrawn. The Court did not deny any applications in whole, or in part. The FISC made modifications to the proposed orders in 803 applications. Thus, the Court approved collection activity in a total of 1456 of the applications to conduct electronic surveillance. Cf. US Department of Justice, Assistant Attorney General, letter dated 28 April 2016, <<https://www.justice.gov/nsd/nsd-foia-library/2015fisa/download>>.

federal agency can request a Court of Review for reconsideration. That is known to have happened only a handful of times in the FISA Court's history and no case has ever been taken to the Supreme Court of the United States. It is not clear either if any of the service providers against whom the orders for electronic surveillance are made are able to appear before such this Court.¹³⁸ This secrecy combined with almost automatic approval of request caused the Court to bear the brunt of heavy criticism, even being nicknamed 'a kangaroo court with a rubber stamp'.¹³⁹

But not only courts of law are set up to oversee handling personal information. It is a part of each data privacy legal framework that a jurisdiction designates one or more agencies, independent of the government, to oversee compliance with data privacy laws. Such agencies – called privacy commissioners in some jurisdictions, and data protection authorities (DPAs) in others – play multiple roles. Their role of an ombudsman interests me the most. In this role, an authority acts on behalf of an alleged victim of a violation because she normally is in a less favourable position. This usually has to do with the lack of legal expertise and resources, in particular money. European statistics show that only one-third of the population is aware of such an agency in their country, and of those a half would prefer such an agency to deal with their problem.¹⁴⁰ I could not find any statistics discussing trust in DPAs, yet I will use four examples to illustrate my point how the inability to lead the office can diminish the trust vested in those oversight bodies.

The Office of the Privacy Commissioner of Australia, established in 1988, was joined in 2010 with its freedom of information (FoI) and information policy counterparts, previously held by Australian Ombudsman, to form the Office of the Australian Information Commissioner (OAIC). Three commissioners headed the newly created bureau and those for FoI and privacy reported to the Information Commissioner. In 2014 the federal government in Canberra attempted to abolish the OAIC altogether and to move the Privacy Commissioner to a position within the Australian Human Rights Commission. (The FoI and information policy portfolios were meant to return to the Ombudsman.) The government could not pass the reform legislation in the upper chamber of the federal Parliament and this created a political limbo hitherto unresolved. The government instead withdrew most of the Office's funding, forcing it to dismiss some of its staff and close its Canberra premises. The Information Commissioner, John McMillan, before his resignation in June 2015, was reported to work from home. In result, from 2015 the Privacy Commissioner also acts

¹³⁸ E. LICHTBLAU, 'In Secret, Court Vastly Broadens Powers of N.S.A.' (2013) *International New York Times*, p. 1.

¹³⁹ S. ACKERMAN, 'Fisa Chief Judge Defends Integrity of Court over Verizon Records Collection', *The Guardian*, 06.06.2013, <<https://www.theguardian.com/world/2013/jun/06/fisa-court-judge-verizon-records-surveillance>>.

¹⁴⁰ EUROPEAN COMMISSION, *Special Eurobarometer 431: Data protection*, 2015, pp. 51–57.

as interim Commissioner for FoI and information policy, being reappointed for the two other offices for three-month periods. Only September 2016 saw the permanent appointment of the incumbent Privacy Commissioner Timothy Pilgrim for a fixed term as Information Commissioner.¹⁴¹ (I too had a lot of difficulties in putting this level of complication in a single paragraph.)

The Australian example is not isolated. When in January 2014 Peter Hustinx finished his second term as the European Data Protection Supervisor (EDPS), a data protection authority for European Union's institutions, agencies, bodies and offices, his successor could not be chosen for almost a year. After the first public vacancy notice in July 2013,¹⁴² an inter-institutional 'selection board' found that all shortlisted candidates were lacking enough experience.¹⁴³ No new vacancy notice followed immediately after. The situation was unprecedented as the post had to be filled in in the middle of the reform process of the EU data privacy law, in which the office of the EDPS was a vivid commentator, working to ensure fulfilment of the EU fundamental right to personal data protection. Commentators frequently asked as to the explanation for the reasoning of the selection board as well as for overall transparency of the process, dubbing the whole process a 'political football'.¹⁴⁴ Hustinx expressed his concerns an open letter stating 'this uncertainty and the possibly long delays that may be involved ... are likely to harm the effectiveness and the authority of the EDPS over the coming months'.¹⁴⁵ Their demands were never satisfied. Simply a second vacancy notice was issued in May 2014 with a one-month deadline¹⁴⁶ and the post was filled in on 4 December 2014 by a joint decision of the European Parliament and the Council.¹⁴⁷

The EDPS story is linked to the story of the Inspector-General for the Protection of Personal Data (GIODO), the Polish DPA. On 4 December 2014 the incumbent Polish Inspector-General, Wojciech R. Wiewiórowski, was elected for the post of Assistant EDPS in Brussels. The vacancy in Warsaw was not filled until mid-April 2015. A candidate can be proposed e.g. by a group of members of parliament and thus the majority has initially proposed the candidacy of Mirosław Wróblewski, who later on withdrew it. The reasons for that remain unclear, yet the media speculated that the parliamentary group proposed this candidate without prior consultation with then prime minister, Ewa Kopacz.

¹⁴¹ I thank Roger Clarke for bringing this matter to my attention.

¹⁴² [2013] OJ C 219A/1–5.

¹⁴³ J. FLEMING, 'Pressure Grows over EU Data Watchdog Replacement', *EurActiv.com*, 09.01.2014, <<http://www.euractiv.com/section/ustice-home-affairs/news/pressure-grows-over-eu-data-watchdog-replacement/>>.

¹⁴⁴ C. KUNER, 'The Baffling Case of the Headless EDPS', *IAPP Privacy Perspectives*, 15.01.2014, <<https://iapp.org/news/a/the-edps-mess/>>.

¹⁴⁵ Cf. <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/News/14-01-07_Letter_to_EC_PH_EN.pdf>.

¹⁴⁶ [2014] OJ C 163A/6–9.

¹⁴⁷ [2014] OJ L 351/9.

Assuming the media were right, there is no constitutional requirement for such a consultation, thus such a delay can be only seen as a part of a political game. The subsequent candidate proposed by the parliamentary majority, Edyta Bielak-Jomaa, won the support of the lower chamber on 9 April 2015, yet in grotesque proceedings. The voting was held in the middle of the night, with MPs giving no attention whatsoever to the presentation of the candidates and observing party discipline when it came to the very moment of voting.¹⁴⁸ The upper chamber confirmed the nomination on 16 April.

Yet perhaps the most remarkable story about trust in DPAs is that of Hungary. From its establishment in 1992 until 1 January 2012, the functioning of the Hungarian authority followed an ombudsman model and it was set up as the Parliamentary Commissioner for Data Protection and Freedom of Information. A vivid debate as to the merits of such an arrangement was concluded with the entry into force of the new Constitution. Among many changes it brought, the post of the Parliamentary Commissioner was abolished and a new authority was set up, outside a national legislature, to fulfil the functions of a DPA. In result, the incumbent Commissioner András Jóri was forced to vacate his office. This caused a few Hungarian NGOs to complain to the European Commission, which monitors the compliance of the Member States with the EU law, that the premature termination of his mandate breached EU data privacy law. In order to act independently, a DPA must be assured that its term in office will not be cut short, other than for a few narrowly interpreted exceptions. The European Commission shared these views and launched before the CJEU an action against Hungary for its failure to fulfil this obligation.¹⁴⁹ There was no surprise when the Luxembourg Court ruled that

Hungary compelled [the Commissioner] to vacate office in contravention of the safeguards established ... to protect his term of office, thereby compromising his independence ... The fact that it was because of institutional changes that he was compelled to vacate office before serving his full term cannot render that situation compatible with the requirement ... of independence for supervisory authorities.¹⁵⁰

I cannot help but conclude this argument with a reference to the socio-psychological theory of procedural justice. It holds that people pay attention not only to the outcome of proceedings (distributive justice) but also the way of arriving at a given outcome.¹⁵¹ In other words, they care if the proceeding

¹⁴⁸ J. WĄTOR, 'Poseł Z Kartką Na Czole', *Gazeta Wyborcza*, 10.04.2015, <http://wyborcza.biz/biznes/1,100897,17733132,Posel_z_kartka_na_czole.html>.

¹⁴⁹ A. JÓRI, 'The End of Independent Data Protection Supervision in Hungary – A Case Study' in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht 2013, pp. 395–406.

¹⁵⁰ Case C-288/12, *Commission v. Hungary* (CJEU, 8 April 2014), §59.

¹⁵¹ T.R. TYLER, 'Procedural Justice and the Courts' (2008) 44 *Court Review* 26.

were fair¹⁵² and they are more likely to accept the outcome, even if unfavourable to them. The idea of procedural justice is based on four building blocks: voice (participation), neutrality, respect and trust. In particular, people infer whether those who decide upon them or represent them listen and consider their views, whether they 'are being honest and open about the basis for their actions; are trying to do what is right for everyone involved; and are acting in the interests of the parties, not out of personal prejudices'.¹⁵³ Tyler coined these conditions having courts of law in mind. I hold these are equally applicable to oversight bodies and this includes data privacy supervisory authorities. The few examples I have discussed above allow me to add in this context the conditions of transparency, stability, continuity and independence as major factors of public trust. The experience of the Australian, European, Polish and Hungarian DPAs teaches that both legislature and executive need to take these bodies seriously. The conclusion must be that trust in such oversight bodies is significantly diminished when public authorities ignore them, underestimate their role or treat them instrumentally, as enablers of political goals or disablers of political opponents.

3.2.2. Organisational tools

I have made only a mention of privacy impact assessments (PIAs) in section 2.2 as one of organisational tools to protect privacy. Their in-depth analysis lies outside the scope of this contribution but it shall suffice for my purposes to assume that PIAs are considered an adequate, broadest and – so far – most mature response to the challenges technology and globalisation posed to the protection of privacy. Much of their success depends on the quality of the process of assessment. Let me use the critique of PIAs to illustrate the point that organisational measures have too their limits in delivering adequate protection.¹⁵⁴

¹⁵² R. HOLLANDER-BLUMOFF, 'Just Negotiation' (2010) 88(2) *Washington University Law Review* 381.

¹⁵³ TYLER, above n. 151, pp. 30–31.

¹⁵⁴ For a critical analysis of other organisational measures, cf. e.g. S. GÜRSER, C. TRONCOSO and C. DIAZ, 'Engineering Privacy by Design' (2011) *Computers, Privacy & Data Protection (CPDP 2011)*, Brussels, pp. 1–25, <<https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf>>; M. HILDEBRANDT and L. TIELEMANS, 'Data Protection by Design and Technology Neutral Law' (2013) 29(5) *Computer Law and Security Review* 509–521; D. WIESE SCHARTUM, 'Making Privacy by Design Operative' (2016) 24(2) *International Journal of Law and Information Technology* 151–175 (concerning Privacy by Design); and R. RODRIGUES, D. WRIGHT and K. WADHWA, 'Developing a Privacy Seal Scheme (That Works)' (2013) 3(2) *International Data Privacy Law* 100–116; R. RODRIGUES, D. BARNARD-WILLS, P. DE HERT and V. PAPAKONSTANTINO, 'The Future of Privacy Certification in Europe: An Exploration of Options under Article 42 of the GDPR' (2016) 869 *International Review of Law, Computers & Technology* 1–23 (concerning privacy seals).

Before PIAs are even performed, they often meet with opposition arguing they would constitute another unnecessary regulatory burden, adding to already overgrown bureaucracy, causing unnecessary expenditure and delays in the decision-making process and in the implementation of a project. Opponents would not omit underlining the complexity of the assessment process in practice, difficulties it brings, combined with a lack of practical experience and minimal or non-existent guidance from those who require a PIA to be conducted. Proponents of PIAs lament that they are often performed perfunctorily and used instrumentally, both to the detriment of the protection of privacy.¹⁵⁵ PIAs are only a tool to support decision-making and thus they do not prevent privacy-intrusive projects from being implemented. A PIA final report might suggest not to implement a project or a part thereof, but nevertheless the decision-makers would approve it as they would perceive the risk worth taking.¹⁵⁶ Or worse, they would perform a PIA solely to fulfil the regulatory requirement but nevertheless would proceed with the implementation of the project.

Next, policies mandating PIAs are often criticised for their narrow scope, i.e. even when the performance of PIA is required by law, the requirements set forth are too narrow and too nuanced to deliver any adequate level of protection. It is further not expected that public authorities or businesses would perform a PIA when not required to do so by the law or otherwise incentivised. This narrowness manifests itself in a limited list of privacy-intrusive projects subjected to PIA. For example, the GDPR requires a form of PIA to be performed – at a minimum – when an individual is subjected to surveillance and decision-making based on profiling, when her sensitive data (such as medical records) are handled on a large scale and when public areas are systematically monitored. To further narrow this list, there exist plenty of exceptions allowing for avoidance of a PIA, such quantitative determinants as 'large scale', 'systematic' or 'extensive'. It is inevitable that those who handle information would attempt to define their projects in a way permitting to escape this regulatory requirement.¹⁵⁷ Yet the feeling is that there are plenty of other types of privacy intrusions resulting from data handlings that merit their subjection to a privacy impact assessment. Furthermore, with the ever-changing nature of society, and innovation and technology, a narrow and prescriptive catalogue of privacy-intrusive actions subjected to PIAs is rather counter-productive.

When PIAs have been performed, they usually lack transparency, i.e. the whole process is opaque and its final results are difficult if not impossible to find. Multiple stakeholders legitimately fear the disclosure of state secrets, trade secrets and otherwise privileged information, yet they fail to acknowledge the existence of certain solutions thereto, e.g. the removal of such information from a

¹⁵⁵ DE HERT, KLOZA and WRIGHT, above n. 72, p. 9.

¹⁵⁶ KLOZA, VAN DIJK and DE HERT, above n. 53, p. 32.

¹⁵⁷ I thank Colin J. Bennett for bringing this to my attention.

public version of their PIA final reports. For instance, the Canadian federal audit of PIAs carried out revealed that only a minority of the stakeholders audited were regularly posting and updating the results of PIA reports to their external websites. Just as the public reporting on PIAs was lacking in completeness, so too was it lacking in quality.¹⁵⁸

Even when the law requires a PIA process to consult external stakeholders, PIAs actually carried out give it limited scope or make it meaningless.¹⁵⁹ Again a Canadian example: many commentators observed that PIAs performed there seldom involve public consultation, opinion polling or other means of gauging the privacy values of the public. The end product tends to resemble a compliance checklist and does not require documentation of deliberations.¹⁶⁰ Systemically, PIAs are often performed too late, when the design of a project cannot be meaningfully influenced to protect privacy, and are equally often misunderstood by their confusion with audits. (While the *modus operandi* of PIAs is to influence the design of a project, thus being an *ex ante* tool, audits are meant to verify compliance once the project has been deployed, and perhaps, concluded, thus being *ex post* tools.) Finally, there is a popular conviction that once a PIA is completed, all privacy problems are solved for good. But, as time passes, both projects undergo changes and so do societal and technological contexts in which these projects are deployed. Thus PIAs often fail to be understood as a continuous process, to the detriment of privacy protection.

3.2.3. Technological tools

As with the critique of privacy impact assessments, I will use the criticism of the end-user Privacy Enhancing Technologies (PETs) in general, and of encryption in particular, to illustrate the shortcomings of technological tools for privacy protection.

The classical critique of PETs is four-fold. The first is that PETs are not for everyday users and this largely explains their limited adoption. They are designed predominantly for people who perceive the need to use technology to protect their privacy against incursions by public authorities, businesses and other individuals, and against unsafe and hostile technologies. Therefore the most likely adopters would include e.g. senior public officials and business executives whose work is particularly sensitive, victims of a crime and political activists, such as dissidents or whistle-blowers.¹⁶¹ The second critique is that of usability (ease of use). The

¹⁵⁸ J. STODDART, 'Auditing Privacy Impact Assessments: The Canadian Experience' in D. WRIGHT and P. DE HERT (eds.), *Privacy Impact Assessment*, Springer, Dordrecht 2012, p. 434.

¹⁵⁹ KLOZA, above n. 38, pp. 80-97.

¹⁶⁰ R. BAYLEY and C. BENNETT, 'Privacy Impact Assessments in Canada' in D. WRIGHT and P. DE HERT (eds.), *Privacy Impact Assessment*, Springer, Dordrecht 2012, p. 183.

¹⁶¹ CLARKE, above n. 82, pt. 4.3.

use of PETs is rather laborious: from learning how to use them to launching each individual tool each time it is needed. PETs do not come in a single software package, but rather each individual PET is a standalone tool. For example, there is normally different software to encrypt the contents of a hard drive and different software to encrypt e-mail communications. To add to this complexity, the use of such software is rather difficult for first-comers.¹⁶² The third critique is that usability is not the sole criterion. Assurance, or trust in a particular encryption technology, seems to be the missing link.¹⁶³ The fourth and final criticism is that PETs are mostly research artefacts rather than tools designed for people to use.¹⁶⁴

Encryption as a PET shares a lot of general critique of PETs but also has a few drawbacks on its own. The first critique is that there is no cryptographic technique that is absolutely unbreakable. The unbreakability depends on three factors cumulatively, i.e. the strength of the encryption algorithm, the length of the encryption key (128-bit-key is nowadays a bare minimum) and the security of the key management (to be kept separately in a safe and secure location).¹⁶⁵ The easiest way to break a cryptosystem is to try all possible keys (i.e. exhaustive key search), thus eventually guessing correctly, yet at a great expense of time and other resources. Further, implementations of encryption may contain accidental errors or deliberate 'back doors'.¹⁶⁶ Finally, cryptography constitutes a dual-use technology, being capable of both civilian and military applications. It is thus subjected to regulation, with certain jurisdictions either restricting or prohibiting its use, import and export or controlling the setting of international encryption standards.¹⁶⁷ The 1996 Wassenaar Arrangement,¹⁶⁸ currently

¹⁶² A. WHITTEN and J.D. TYGAR, 'Why Johnny Can't Encrypt. A Usability Evaluation of PGP 5.0' in L. CRANOR and G. SIMSON (eds.), *Security and Usability: Designing Secure Systems That People Can Use*, O'Reilly, Sebastopol CA 2005, p. 699.

¹⁶³ S. FAHL, M. HARBACH, T. MUDERS, M. SMITH and U. SANDER, 'Helping Johnny 2.0 to Encrypt His Facebook Conversations Categories and Subject Descriptors', *Symposium on Usable Privacy and Security (SOUPS)*, ACM, Washington DC 2012, p. 11.

¹⁶⁴ CLARKE, above n. 82, pt. 4.1.

¹⁶⁵ W. HON, C. MILLARD and I. WALDEN, 'The Problem of 'Personal Data' in Cloud Computing: What Information Is Regulated? The Cloud of Unknowing, Pt. 1', Legal Studies Research Paper 75/2011, London 2011, p. 23.

¹⁶⁶ S. GÜRSES and B. PRENEEL, 'Cryptography and Privacy in the Context of Big Data' in B. VAN DER SLOOT, D. BROEDERS and E. SCHRIJVERS (eds.), *Exploring the Boundaries of Big Data*, Amsterdam University Press, Amsterdam 2016, pp. 62–66.

¹⁶⁷ J. BALL, J. BORGER and G. GREENWALD, 'Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security', *The Guardian*, 06.09.2013, <<https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>>.

¹⁶⁸ Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Wassenaar 1996; cf. esp. the dual-use list, cat. 5, pt. 2, <<http://www.wassenaar.org/wp-content/uploads/2016/07/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf>>. Cf. also Council Regulation (EC) No. 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, [2009] OJ L 134/1–269, currently under revision, cf. COM(2016) 616 final.

comprising 42 jurisdictions, is perhaps most known example of multilateral export control regime.¹⁶⁹ Finally, criminal laws might require individuals to surrender cryptographic keys to law enforcement, yet the suspect might resort to the privilege against self-incrimination.¹⁷⁰

Encryption nevertheless survives most of the above-mentioned criticism and is thus considered an efficient technology to protect information in a digital environment. In the aftermath of the 2013 Snowden disclosures about the global mass surveillance practices, multiple stakeholders resorted, *inter alia*, to the widespread use of strong, end-to-end encryption without the possession of the key by any intermediary or manufacturer. In a 2013 questions and answers session with *The Guardian*, Snowden himself advised: 'Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.'¹⁷¹

4. THE BEHAVIOURAL ALTERNATIVE

4.1. HISTORY

*That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.*¹⁷²

Resorting to one's own behaviour to protect certain interests is perhaps as old as humanity and attempts of that type to secure communications offer a fascinating example to illustrate my point. In the era of verbal communications, the mere invention of writing made all communications secret, at least initially, as not many people were able to read. Human messengers, if they were to carry a written message, were chosen from among illiterates, a practice still known in the nineteenth century.¹⁷³ As the skill of writing became more widespread, additional precautions were needed to ensure secrecy.¹⁷⁴ Thus cryptography, i.e.

¹⁶⁹ B.-J. KOOPS, *The Crypto Controversy: A Key Conflict in the Information Society*, Kluwer Law International, The Hague 1999, pp. 97–113.

¹⁷⁰ Ibid., pp. 167–200; B.-J. KOOPS, 'Commanding Decryption and the Privilege Against Self-Incrimination' in C.M. BREUR, M.M. KOMMER, J.F. NIJBOER and J.M. REIJNTJES (eds.), *New Trends in Criminal Investigation and Evidence*, Intersentia, Antwerp 2000, pp. 437–438.

¹⁷¹ G. GREENWALD, 'Edward Snowden: NSA Whistleblower Answers Reader Questions', *The Guardian*, 17.06.2013, <<https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower>>.

¹⁷² WARREN and BRANDEIS, above n. 17.

¹⁷³ D.J. SOLOVE, *Understanding Privacy*, Harvard University Press, Cambridge MA 2008, pp. 61–65.

¹⁷⁴ A.C. LEIGHTON, 'Secret Communication among the Greeks and Romans' (1969) 10(2) *Technology and Culture* 140.

the art and science of making communications unintelligible to all except the intended recipients, was invented and since antiquity has been widely used in politics and warfare. Julius Caesar used one of the earliest known cryptographic systems. Around 50 BC Caesar wrote to Cicero using a cipher that shifts the Latin alphabet three places to the right and wraps the last three letters back onto the first three letters.¹⁷⁵ But, equally in politics and warfare, the adversary wants to read a cryptic message. Therefore cryptanalysis, i.e. reading secret messages and uncovering the cryptographic system utilised, played a vital role in the conclusion of many conflicts. The recovery of an Enigma machine from a sinking Nazi submarine, and breaking its code by Polish mathematicians, is believed to have been a turning point in World War II.¹⁷⁶ Both cryptography and cryptanalysis progressed with the advent of computers, crowned with Diffie's and Hellman's revolutionary development of asymmetric cryptography in 1976.¹⁷⁷

Surprisingly, when sophisticated cryptography combined with a plethora of other cutting-edge measures employed to protect digital communications fails, a return to simplicity might be more fruitful. I found entertaining a piece of news brought by *The Guardian* in 2014 when – in the aftermath of the Snowden revelations – reportedly both Russian and German secret services ditched their computers and returned to the use of mechanical, analogue typewriters.¹⁷⁸ At least a piece of information would remain in a predetermined, finite number of easily traceable copies, assuming photocopies were not made.

Nevertheless, secrecy of communications is not only a domain of politics and warfare. Messages have been concealed and coded also for purely private purposes. To take a most mundane example, for generations children have kept their secrets in diaries secured with padlocks, or in a hiding place known only to them. Similarly, they use their own key-language (idioglossias) to communicate with peers, so that their parents or unwelcome colleagues cannot learn the contents of their communications. To take the most prominent example, only a handful of readers would not be familiar with the encryption software called 'Pretty Good Privacy', or 'PGP'. It has been widely used since the 1990s, especially in e-mail communications, and is to a large extent based on Diffie's and Hellman's invention. The idea is that anyone with a *public* key of a particular addressee can lock a message addressed to her. The addressee is the only person

¹⁷⁵ D. LUCIANO and G. PRICHETT, 'Cryptology: From Caesar Ciphers to Public-Key Cryptosystems' (1987) 18(1) *The College Mathematics Journal* 1–2.

¹⁷⁶ Ibid., p. 3; M. REJEWSKI, 'How Polish Mathematicians Broke the Enigma Cipher' (1981) 3(3) *Annals of the History of Computing* 213–234.

¹⁷⁷ W. DIFFIE and M.E. HELLMAN, 'New Directions in Cryptography' (1976) 22(6) *IEEE Transactions on Information Theory* 644–654; D. KAHN, 'Cryptology Goes Public' (1979) 58(1) *Foreign Affairs* 153–154.

¹⁷⁸ P. OLTERMANN, 'Germany "May Revert to Typewriters" to Counter Hi-Tech Espionage,' *The Guardian*, 2014.

knowing her *private* key, so she and only she herself can unlock the message and read its contents.¹⁷⁹

4.2. TYPOLOGY

How do people adjust their behaviour to protect privacy? I hasten to explain to the reader that the typology I propose here is my first attempt to classify and make sense of behavioural tools for privacy protection. I also re-emphasise this typology grew up from my own experience, observations and discussions with relatives, friends and colleagues rather than from any specific scientific method. It is thus meant to be an invitation to further discussion, which – it is hoped – would help to render this toolkit as complete as possible.

Behavioural tools for privacy protection could be used *individually*, by a person concerned, normally in her own personal interest, or *collectively*, by a societal group, usually in their own collective interests. These protections could include a wide range of *actions* and *inactions*. They might *directly* target the objective of privacy protection or might target some other objective, thus *indirectly* adding to the protection of privacy. Behavioural tools are usually scalable: people might be engaging in such actions or inactions on a *permanent* or *temporary* basis, or at *regular intervals* (e.g. 'digital detox'). They might employ different behaviour in their *professional* (at work) and *private* life (at home). They might engage for their own benefit (i.e. *inward* tools) or for the benefit of other people (e.g. their relatives and friends, their social group or even the society at large; *outward* tools).

The spectrum of behavioural tools opens with *non-engagement*, i.e. the choice not to use certain services. The first sub-category is *non-participation* and it starts with small daily choices, ranging to essential, more drastic decisions. Initially, people would cease to use services or service providers notorious for invading their privacy. In the latter instance, this might amount to conscious avoidance of particular brands. It might further amount to avoidance of services or service providers originating from particular countries that are not considered trustworthy. (Some people would test or experiment with these services and providers before.) Some people would perform certain transactions offline instead of online. If there was an option to pay cash for theatre tickets for a performance in the neighbourhood, they would go to the box office instead ordering them on a website. People would refuse to give their postcode for statistical purposes (a common practice in some supermarket chains). Some people, as a matter of principle, would not use social networking sites (Facebook or Google Plus), or would use some of them for professional reasons only, e.g.

¹⁷⁹ Cf. <<http://www.pgpi.org/doc/pgpintro>>.

LinkedIn or Twitter. I have known people who have ceased to use them. Some people do not possess or use a mobile phone or – a few more – do not use any 'smart' functionalities thereof. I have known people who disconnect from all digital services for a given period of time, celebrating e.g. 'digital detox' or 'National Day of Unplugging'.¹⁸⁰ I have also known people who still use paper agendas and diaries for planning their time. (The latter, I was told, is partially because 'we slowly but consequently lose our ability to handwrite'.)¹⁸¹

The second sub-category of non-engagement is *non-disclosure* and it concerns partaking in a wide spectrum of services, but having first carefully chosen *which* information, *if ever*, to disclose, *how* to disclose or which sub-services to subscribe in, and to *what extent*. It is an attempt to meaningfully partake in services with no or only minimal, selective disclosure of information. Non-disclosure, similarly to non-participation, starts with trivial daily choices. I have known people who would never set-up an account for just a single online transaction or would never opt-in for any newsletters while buying goods or services over the Internet. (It is a common practice of ticket-selling intermediaries or airlines to offer to 'become a member' and to subscribe to newsletters with 'best offers ever'.) People would uninstall software when they no longer need it, even when they used it only once or twice. I have known people who install a mobile application of Uber each time they need to use its services; such a need must arise for them rather sporadically. They might opt for a pre-paid mobile phone bought with cash over a subscribed one – still available in some countries – and thus making it easy to change, should the need arise (cf. 'burner phones'). When paying with a pseudonymous currency, e.g. Bitcoin, they would hide their IP number and use a new address each time they send and receive a new payment. They would exchange cash for cryptocurrencies in a dedicated bank machine. I have known people who provide their office address for delivery of goods bought online, catalogues and 'less important' correspondence as a means to avoid disclosing their home address. I have also known people, especially youngsters, who set up their social networking sites to display different contents to different groups, i.e. their classmates see different photos than their parents.

The spectrum continues with the protection of the security and secrecy of activities as well as the obfuscation of the mere fact thereof (*concealment*). Here people would resolve to *technological* and – to a lesser extent – *organisational* means. However, what qualifies these two types as behavioural tools is the way these are assessed, chosen and used. Further, it is the way these means create and

¹⁸⁰ Cf. <<http://nationaldayofunplugging.com>>.

¹⁸¹ Statement on file with the author. Some inspiration for such temporary disconnection from the digital world might have come from a documentary movie *Finding Paul Miller* (2013); cf. P. MILLER, 'I'm Still Here: Back Online after a Year without the Internet', *The Verge*, 01.05.2013 <<http://www.theverge.com/2013/5/1/4279674/im-still-here-back-online-after-a-year-without-the-internet>>.

change habits of their users. People would first enquire and assess whether a given means would offer them the protection they seek. As there exist replacements for the vast majority of technologies (e.g. there are a few alternatives to a major online maps provider), they would choose predominantly those whose main aim is to protect privacy. Often they would use them in addition to the other technologies used, e.g. they might install a specific add-on into their web browser. (The sole aim of these additional technologies might be to protect security of information and then their security features are at a service of privacy.) People would prefer technologies offered by providers originating from countries with laws more supportive for individual privacy or providers who store information of their clientele in such jurisdictions. (I have nevertheless known people who, having obtained a new mobile device, would each time wipe out its memory and install a trusted operating system, even at the pain of losing warranty.) It has become a common practice, after the 2013 Snowden disclosures, for Europeans to choose European organisations whose servers are located on the Old Continent, thus making them 'NSA-proof'.¹⁸² Certain organisations made their business model on this criterion of geographic location. In other words, geography matters and people would 'shop' for a favourable forum. People who have specific background would prefer open source technologies as they would build their trust therein on the verification the software code whether it actually delivers the promised protections. A trust in a technology or its providers is usually enhanced with clear privacy policies and 'social contracts'. (For example, in such a 'contract', the Tor Project claimed it would never 'implement front doors or back doors into [their] projects'.)¹⁸³

When people start using e.g. end-to-end, military-grade encryption of their e-mails, they would often change the way they read and write these. They would access their e-mail account solely via website, which they would open only in a web browser offering a strong preservation of anonymity, e.g. Tor. For some other services, they would force their browser to connect only using a secure connection (i.e. the HTTPS protocol), they would set it up to clear browsing history and cookie files at the end of each session or they would enable a 'do-not-track-me' functionality and disable any form of geo-location. There are further instances when complex security, secrecy and obscurity are necessary, for example whistle-blowers. They might use particular technologies only for a single purpose, e.g. an e-mail account to communicate with one person, and this each time with the use of a so-called live operating system.

People might further re-organise their daily habits to protect their privacy. They might conceal and diffuse their identity. The use of pseudonyms, such as nicknames, anonymisation of web searches, by the use of dedicated search

¹⁸² Wojciech R. Wiewiórowski coined this term.

¹⁸³ Cf. <<https://blog.torproject.org/blog/tor-social-contract>>.

engines, and anti-malware software are the simplest example here. They would opt for an anonymous travel card in a city, if possible, even if this option is more expensive. They would refuse to accept a 'smart meter' to calculate their energy consumption. People might use different service accounts – e.g. multiple e-mail addresses and logins for instant messengers – for different purposes, e.g. professional reasons or online shopping. They would use dedicated software to ensure erasure of data from a hard drive, should these data no longer be needed, or to remove traces of their activities ('digital footprint') from the Internet.¹⁸⁴

On some rare occasions, people would protect the security and secrecy of their activities by resolving to classical methods of cryptography (writing code) and steganography (concealing information within other non-secret information). They might develop some keywords and nicknames with specific meaning asserted that is known only to a closed circle of people. (They might pay attention not to mention any names; *nomina sunt odiosa*.) They might speak a rare, foreign language (e.g. in public spaces) or even invent and speak a new one; the latter would be extremely rare. They might simply call instead or type on an instant messenger since voice – at the current level of technology development – is still more difficult for a machine to meaningfully analyse than any computer-typed text. Or – the simplest solution – they would not discuss a given matter in any public space.

People would ultimately resort to organisational, 'bricks and mortar' means, such as coverage (hiding) and obliteration. For example, people would place removable stickers on the lens of their laptop's built-in video camera and microphone. ('Removable' as they from time to time would actually use the camera.) In their houses, windows would be coverable with curtains or blinds. When entering a password on a device, they would cover their keyboard, similarly to typing in a PIN number on a credit card terminal. They would recycle only shredded documents, if they contained any valuable information, e.g. health records or bank statements. (Some people would burn them in a fireplace.) At home, they would keep their passport – and other documents embedded with radio-frequency identification (RFID) devices – in a cover capable of blocking its detection and interaction therewith. Even simply while walking at an airport, people would hide, cover or just turn over their boarding passes and passport so that nobody can guess or read their names and nationalities.¹⁸⁵ If a battery is still removable from their mobile devices, they would take it out during meetings they perceive to be sensitive, otherwise they would hold them e.g. in a microwave.

The spectrum of behavioural tools closes with a wide range of *proactive* tools. While the previously discussed tools are predominantly aimed at reducing

¹⁸⁴ Cf. <<http://www.abine.com/deleteme>> or <<http://www.deseat.me>>.

¹⁸⁵ A lot can be read from merely a front cover of a passport and from its colour.

threats to privacy, these aim to increase the level of privacy protection. People would engage in protest when their collective interest is threatened, e.g. a mass surveillance practice is to be put in place in a given jurisdiction. One of the earliest examples of significant protest aiming at safeguarding privacy was held in the Netherlands in 1971 and targeted a national census. Never again would such a comprehensive survey of the entire population be held in the country.¹⁸⁶ More recently, in 2008 the Dutch protested against a compulsory roll-out of smart meters in the entire country. As a result of public outrage, the relevant bill was amended in the parliament to accommodate privacy safeguards.¹⁸⁷ These developments are believed to have inspired the introduction of privacy safeguards in the energy sector at EU level.¹⁸⁸ As a case in point, August 2016 saw the beginning of public outrage against the lack of anonymity of a national census in Australia. This protest gained popularity especially after the hashtag #CensusFail went viral on Twitter and the registration website went down.¹⁸⁹

People might organise themselves in advocacy groups and in particular set up dedicated non-governmental organisations (NGOs). I can immediately think of some global players such as the Electronic Frontier Foundation (EFF),¹⁹⁰ some 'regional' players like the European Digital Rights [EDRi]¹⁹¹ and 'national ones', like *Digital Rights Ireland*,¹⁹² *Fundacja Panoptikon*¹⁹³ in Poland or *La Quadrature du Net* in France.¹⁹⁴

Finally, people might engage in *awareness-raising*. Parents would teach their children about basic aspects of security while using the Internet. Whistle-blowers might contribute to the enhancement of protection should their disclosures bring a change therein. Ethical ('white-hat') hacking, i.e. breaking into protected systems and networks to test and assess their security, although at the limits of moral acceptability, closes the spectrum of collective tools.

¹⁸⁶ C. BENNETT, *The Privacy Advocates. Resisting the Spread of Surveillance*, MIT Press, Cambridge MA 2008, pp. 134–137.

¹⁸⁷ Cf. e.g. C. CUIJPERS and B.-J. KOOPS, 'The "Smart Meters" Bill: A Privacy Test Based on Article 8 of the ECHR. Study Commissioned by the Dutch Consumers' Association', Tilburg 2008, <http://www.consumentenbond.nl/morello-bestanden/pdf-algemeen-2008/onderzoek_UvT_slimme_energij.pdf>; C. CUIJPERS and B.-J. KOOPS, 'Smart Metering and Privacy in Europe: Lessons from the Dutch Case' in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht 2013, pp. 269–293; KLOZA, VAN DIJK and DE HERT, above n. 53.

¹⁸⁸ S. GOEL, Y. HONG, V. PAKONSTANTINO and D. KLOZA, *Smart Grid Security*, Springer London 2015, pp. 46–57.

¹⁸⁹ Cf. <<https://censusfail.com>>.

¹⁹⁰ Cf. <<http://www.eff.org/secure-messaging-scorecard>>.

¹⁹¹ Cf. <<http://edri.org>>.

¹⁹² Cf. <<https://www.digitalrights.ie>>.

¹⁹³ Cf. <<http://panoptikon.org>>.

¹⁹⁴ Cf. <<http://www.laquadrature.net>>.

Table 1. An early typology of behavioural tools for privacy protection

- Individual - Collective	- Inaction - Action	Direct	<div>- Non-engagement<ul style="list-style-type: none">• Non-participation• Non-disclosure• Selective disclosure</div>	<div>- Temporary - Permanent - Regular intervals</div>	<div>- Professional - Private</div>	<div>- Inward - Outward</div>
		Indirect	<div>- Secrecy, security and concealment<ul style="list-style-type: none">• Technological means<ul style="list-style-type: none">• Forum shopping• Trust seeking• End-user PETs<ul style="list-style-type: none">• Encryption• Pseudonymisation• Anonymisation• Cryptography• Steganography</div> <div>• Organisational means<ul style="list-style-type: none">• Coverage (hiding)• Obliteration</div>			

4.3. IMPLICATIONS

4.3.1. Characteristics

An attempt to offer an early typology of behavioural tools for privacy protection has brought me to offer some general observations about their inherent features. A careful reader would immediately note that these tools are predominantly addressed to a layperson on the street, seeking for a new means to safeguard her interests. This does not exclude other stakeholders, such as private organisations, from adopting some of behavioural protections. These behavioural tools are useful predominantly to protect privacy when personal data are being handled.¹⁹⁵

¹⁹⁵ There are plenty of conceptualisations of types (or of the scope) of ‘privacy’. From a chronological viewpoint, the modern understanding of privacy started with ‘the right to be let alone’ as defined by WARREN and BRANDEIS, above n. 17, pp. 193–220. The scholarship on privacy continues e.g. with Westin’s four states of privacy: solitude, intimacy, anonymity and reserve (A.F. WESTIN, *Privacy and Freedom*, Atheneum, New York 1967), Posner’s economic critique of privacy (R. POSNER, ‘The Right of Privacy’ (1978) 12(3) *Georgia Law Review* 393–422) and Regan’s recognition of its societal value (P. REGAN, *Legislating Privacy: Technology, Social Values and Public Policy*, University of North Carolina Press, Chapel Hill 1995,

Again, their applicability to data privacy does not exclude their usefulness for the protection of types of privacy, e.g. the one of body or association. Behavioural tools have been coined in a response to privacy threats posed by globalisation and technological development and thus they are predominantly applicable to the digital world. They are most useful if applied *ex ante*, i.e. before information is disclosed or, broader, any privacy threat materialises itself. They are thus predominantly of a preventive nature. Finally, behavioural protections are not limited by the territoriality of regulation. In other words, contrary to the regulatory tools, but alike to organisational and technological ones, behavioural tools know no geographical boundaries for their application.

4.3.2. *Conditions*

I can immediately think of at least four conditions for a successful application of behavioural tools for privacy protection. The first condition is to be *aware* of a privacy threat itself and of a possibility to make certain choices and undertake certain actions or inactions to avoid or minimise such threat.

An individual who resolves to behavioural tools must be 'genuinely alarmed'¹⁹⁶ and – to a large extent – need to be a 'proficient users' of new

pp. 212–243), among others. More recent attempts to conceptualise include Clarke (R. CLARKE, 'Introduction to Dataveillance and Information Privacy and Definitions of Terms', 1997, <<http://www.rogerclarke.com/DV/Intro.html>>) who initially distinguished four types – privacy of the person, of personal data, of personal behaviour and of personal communication – and supplemented them in 2013 with privacy of personal experience. Later, Finn, Wright and Friedewald enlarged this catalogue by the privacy of thoughts and feelings, of location and space, of association (R.L. FINN, D. WRIGHT and M. FRIEDEWALD, 'Seven Types of Privacy' in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht 2013, pp. 3–32). In parallel, Rössler distinguished three types: decisional, informational and local privacy (B. ROSSLER, *The Value of Privacy*, Wiley, Cambridge 2005, pp. 86–142) and Solove observed four major types of handlings of personal data that might cause harm to individual: information collection, processing, dissemination as well as invasion (SOLOVE, above n. 173, pp. 10–11). Most international human rights instruments, drafted in 1950s and 1960s, distinguish four broad aspects of the right to privacy: private life, family life, home and communications. The broad scope of privacy was confirmed by the European Court of Human Rights who ruled that it is 'not possible or necessary to attempt an exhaustive definition' of privacy (*Niemietz v. Germany*, 1992). Most recently, Koops et al. have 'structure[d] types of privacy in a two-dimensional mode, consisting of eight basic types of privacy (bodily, intellectual, spatial, decisional, communicational, associational, proprietary, and behavioural privacy), with an overlay of a ninth type (informational privacy) that overlaps, but does not coincide, with the eight basic types' (B.-J. KOOPS, B. CLAYTON NEWELL, T. TIMAN, I. ŠKORVRANEK, T. CHOKREWSKI and M. GALIČ, 'A Typology of Privacy' (2016) 38 *University of Pennsylvania Journal of International Law* 1–76). I quote here these various conceptualisations merely to demonstrate both the wide scope of the notion of privacy as well as the complexity in its delimitation.

¹⁹⁶ J. FRANZEN, 'Imperial Bedroom', *New Yorker*, 12.10.1998, pp. 48–53.

technologies.¹⁹⁷ In practice, a good deal of behavioural protections would be used by 'knowledgeable and obsessive enthusiasts' or – in other words – 'geeks'.¹⁹⁸

The level of awareness in the society about privacy threats and measures available to counter them is, however, insufficient. On the one extreme, there are people who were born and risen in the digital era – i.e. 'digital natives'¹⁹⁹ – and for them the question how to navigate amongst emerging technologies is rather obsolete. On the other extreme, there are 'digitally divided' or 'digitally excluded' people. Because of their lack of digital literacy, vulnerabilities or language barriers, they are unable to fully enjoy digital technologies. Despite the problem of 'digital divide' being of predominantly temporal nature and despite breeze familiarity of digital technologies amongst 'digital natives', the problem is that still not everybody knows *enough* to identify and evaluate privacy threats and to act thereon. And even amongst those who know, their awareness is rather inaccurate and insufficient.²⁰⁰

The vast majority of Europeans see 'disclosing personal information as an increasing part of modern life', yet they are not sufficiently aware of the ways in which to protect their privacy.²⁰¹ Individuals are often 'uninformed and confused' and hence often 'misinterpreting their own behaviour'.²⁰² It is still a common practice that people click 'I agree' without giving even the slightest thought that they are consenting to a certain practice of data handling and that such a practice might run counter to their interests. Europeans lack further information on the available remedies in case something goes wrong.²⁰³ They are often unaware of the existence of a national data protection authority (DPA) that could offer them assistance in such a situation.²⁰⁴ All in all, the privacy universe forgets that – although people usually claim they care about 'privacy', and even if they really do so – in practice they often have their attention taken up by 'more immediate problems: jobs, shelter, health, education, food, water'.²⁰⁵ Despite people increasingly bringing digital education from homes and schools,

¹⁹⁷ MOSHELL, above n. 27, p. 367.

¹⁹⁸ Oxford Dictionary of English.

¹⁹⁹ M. PRENSKY, 'Digital Natives, Digital Immigrants' (2001) 9(5) *On the Horizon* 1.

²⁰⁰ J.B. RULE, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Elsevier, New York 1980, p. 184.

²⁰¹ EUROPEAN COMMISSION, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, Brussels 2011, p. 5.

²⁰² G. GONZÁLEZ FUSTER, 'How Uninformed Is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection' (2014) 19 *IDP. Revista de Internet, Derecho y Política* 99.

²⁰³ FRA, 'Access to Data Protection Remedies in EU Member States', Publications Office of the European Union, Luxembourg 2011, pp. 32–34.

²⁰⁴ EUROPEAN COMMISSION, above n. 201, p. 174.

²⁰⁵ J. CANNATACI, intervention at the Computers, Privacy and Data Protection (CPDP) Conference, Brussels, 25.01.2017.

it is rather basic and thus still more is needed.²⁰⁶ I have observed multiple efforts undertaken to raise awareness. For instance, European authorities organise on an annual basis a data protection day on 28 January and their Asian-Pacific counterparts engage annually in 'Privacy Awareness Week' in early May. I have further observed the question of privacy protection being dealt with in popular culture. Recent motion pictures, such as *Erasing David* (2010), Laura Poitras' documentary *Citizenfour* (2014) – and the 2015 Academy of Motion Picture Arts and Sciences' Oscar for the best documentary it won – as well as Oliver Stone's recent biopic *Snowden* (2016), have contributed significantly to the increase in public understanding of privacy problems. (I set aside any evaluation of their artistic value.)

The second condition for a successful application of behavioural tools is that of *proximity*. An individual would resort to behavioural tools when she perceives the threat as directly relevant for safeguarding her own interests or interests of a social group she belongs to. Such a perception is highly subjective, contextual and rarely consistent. This is so because the appropriate level of privacy protection is only something that can be decided at an individual level and according to the highly variable instincts about what is, and is not, intrusive or sensitive.²⁰⁷ An anecdote to illustrate my point: when I moved to study in Copenhagen, the otherwise perfect apartment where I was supposed to live had no curtains to cover the windows. When I asked the landlady to provide them in the flat, she – immediately and without any hesitation – wondered if I had something to hide. Initially her reaction surprised me, but later on I thought that her own perception of privacy was legitimate. She might not have anything to hide. But I did not have anything to expose to the neighbours on the opposite side of the street. My viewpoint here was equally legitimate. Eventually, curtains appeared in the windows.

The third condition concerns the *gravity* of a threat. People would engage in behavioural tools when the threat – in their perception – is sufficiently significant. As with the criterion of proximity, human perception of gravity of a privacy threat highly depends both on the context and on their judgement. Translating this to the privacy universe, for example, a whistle-blower risking lifetime sentence for her disclosures – at the end of the day, she is never sure whether she would be recognised as a whistle-blower in a given jurisdiction and whether she would be asserted with the protection due – would be predominantly concerned about the safety and security of herself and her mission.²⁰⁸ She would resort to

²⁰⁶ G. GONZÁLEZ FUSTER, D. KLOZA and P. DE HERT, 'The Many Faces of Privacy Education in European Schools' in G. GONZÁLEZ FUSTER and D. KLOZA (eds.), *The European Handbook for Teaching Privacy and Data Protection at Schools*, Intersentia, Cambridge 2016, p. 15.

²⁰⁷ BENNETT, above n. 186, pp. 210–214.

²⁰⁸ P. DE HERT and D. KLOZA, 'WikiLeaks, Privacy, Territoriality and Pluralism. What Does Matter and What Does Not?', Tilburg Institute for Law, Technology and Society Blog, 2011, <http://www.vub.ac.be/LSTS/pub/Dehert/Dehert_361.pdf>.

advanced encryption techniques to share otherwise classified information at her disposal. Outlets such as WikiLeaks or SecureDrop of the Freedom of the Press Foundation have created and described sophisticated channels for transmitting information.²⁰⁹ Furthermore, that few people feel the same about risk every day of their lives makes it more complicated. As people grow older, wiser, richer or poorer – and as the society and technology progress – people's perception of what risk is and their aversion to taking risk will shift, sometimes in one direction, sometimes in the other.²¹⁰

The final condition is that of *usability*. The easiness of use might play a decisive role in the choice of behavioural tools for privacy protection. The problem is well known with from the criticism of the end-user PETs.²¹¹ If any new tools require sophisticated knowledge, experience and a good deal of effort and patience to apply in practice, their applicability would find application only amongst determined 'geeks'. In practice, a perfect choice of such technologies is, obviously, not possible, and thus people are left with a dilemma between more protection at the detriment of usability or less protection yet better usability.

4.3.3. Problems

Behavioural tools for privacy protection are not unproblematic. I fear that their use might bring negative social implications such as chilling effect, lower quality of service and even exclusion. Put simply, people might choose not to engage in certain services capable of intruding their privacy that are otherwise rather legitimate. The chilling effect on the freedom of speech – e.g. not expressing own views as these might be used against the speaker – is perhaps the most obvious example. I have known people in certain countries who prefer not to have political opinion as this might put their lives in danger. Translating this to the privacy universe, I have known people who would not access someone else's profile on a social networking site when this site registers and discloses who has viewed it to the latter person. But this is not an isolated example: I might like and I might find useful some level of artificial intelligence of an instant messenger from a major service provider. Yet their practices of handling personal data have instantly dampened my enthusiasm for this type of innovation. I did not subscribe. By remaining faithful to the means of communication chosen earlier, which have proven their reliability, the quality of my digital experience might be diminished. Furthermore, people resorting to behavioural tools for privacy protection might exclude themselves from some parts of social life. For example,

²⁰⁹ Cf. <<https://wikileaks.org/#submit>> and <<https://securedrop.org>>.

²¹⁰ P.L. BERNSTEIN, *Against the Gods: The Remarkable Story of Risk*, Wiley, New York 1998, p. 263.

²¹¹ Cf. above section 3.2.3.

I do not have any account on any 'private' social networking site. (Except for professionally oriented Twitter and LinkedIn accounts.) I do not feel that I need it or that – by excluding myself – I lose something. My choice was dictated by many reasons and the protection of my privacy is only one of them. However, in extreme cases, this choice of mine excludes me from social activities procured with the use of such a platform. If people use such sites for example to invite guests for a housewarming party, I might not receive an invitation, unless these people send me an e-mail or make a phone call. Other people might judge me anti-social. Overall, I feel such a price is worth paying.

I further fear that the usage of behavioural tools might be abused and that, as a consequence, certain stakeholders might 'strike back'. The state might consider these tools counterproductive to its efforts in e.g. maintain national security and thus it might attempt to restrict their use. (Encryption would be the most pertinent example here; I return to it below.) Equally businesses might find these protections running contrary to their interests. (Let me illustrate this point by recalling some websites, usually media outlets, which 'refuse' to work if an add-block software continues to run).

The problem of 'striking back' can be seen from the perspective of international human rights law. It sets forth certain limitations for the enjoyment of rights and for their restriction. First and foremost, there exist limits as to the exercise of own privacy. 'Privacy' is not a limitless concept and the law reflects that. The right to privacy could be interfered with on a condition such interference is legal, proportionate, necessary in a democratic society and serves a legitimate aim. Further, staying within the legal discourse, rights are not meant to be abused and the law reflects that too. On the other side, those who attempt to interfere with 'privacy' not only have to respect the above-mentioned limitation criteria but also must interpret these limitations narrowly. In other words, *in dubio pro libertate*. Thus each attempt to interfere with privacy and each new type of its protection cannot escape the compliance with these conditions.

I found the example of the usage of encryption and attempts to counter it illustrative as to the quest for equilibrium between two legitimate yet seemingly competing interests at stake – e.g. national security versus individual privacy. Technologies of cryptography are, by definition, capable of good and bad. Information may be encrypted to safeguard legitimate secrets or to help to blow the whistle. It also may be encrypted to ensure that the plotting of an illicit action is not undermined. Here is the crypto controversy: the accommodation of the conflicting interests of privacy and information security, on the one hand, with the interests of law enforcement and national security, on the other.²¹² While some commentators call for 'a right to encrypt personal information

²¹² KOOPS, above n. 169, p. 2.

effectively',²¹³ some jurisdictions consider limiting its use in the name of national security, e.g. France and Germany.²¹⁴ I share the conviction that to ban entirely the use of encryption or to significantly undermine its effectiveness – e.g. by introduction of 'back doors' or 'key escrows' – would be disproportionate. It might even render encryption meaningless. At the end of the day, nobody questions the need for national security, but the question is rather how?

I eventually fear that – as with cryptography – certain behavioural tools would meet the same fate: their use will be confronted with their abuse. There is no straightforward answer. Each development – be it a disclosure of a secret, a political dispute, a voice in a debate or a note to a case – helps to delineate borders between their legitimate use and abuse. This question of use versus abuse may be answered in two ways. Looking from the ethics point of view, different schools of ethics might provide diverse answers, arguing either for individual (i.e. privacy) or collective interests (i.e. national security) to prevail. Looking from the viewpoint of democracy, the rule of law (*Rechtsstaat*) and fundamental rights viewpoint, a more formal, i.e. procedural, answer might arrive. Nevertheless, such an answer will never escape a moral judgement.

5. CONCLUSION

This contribution has been an invitation to consider an alternative type of privacy protections – behavioural. I have observed that 'the way in which one acts or conducts oneself' sometimes has a dedicated goal of safeguarding one's own privacy.²¹⁵ It all started with a contestation with a friend of mine that 'you too cover your laptop camera with a sticker'. This observation opened a vivid discussion with family, friends and colleagues. I have concluded that certain individual choices, actions and inactions aimed at privacy protection – i.e. behavioural tools for privacy protection – do not necessarily fit into the three types of protections existing thus far, i.e. regulatory, organisational and technological. Therefore it was logical to coin a new type of protections, analyse its emergence, typology and implications.

I have then concluded that these new behavioural tools have emerged in response to the inadequacies of contemporarily available protections. I have observed that – even with my own laptop camera – I have covered it with a removable sticker because neither regulation efficiently prohibits abusive

²¹³ M. KIRBY, 'Privacy Protection, a New Beginning: OECD Principles 20 Years on' (1999) 6(3) *Privacy Law and Policy Reporter* 25–34.

²¹⁴ B. CAZENEUVE, *Initiative franco-allemande sur la sécurité intérieure en Europe*, Paris, 26.08.2016, <<http://www.interieur.gouv.fr/Le-ministre/Interventions-du-ministre/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe>>.

²¹⁵ Oxford Dictionary of English.

global mass surveillance practices nor there exists software, in which I can have confidence, to ensure that the laptop camera does not operate without my prior knowledge and consent. I have subsequently learned about a friend of mine, whom I nicknamed here Joseph, who had to cease to use one of his private e-mail addresses as a way of protecting himself against abusive surveillance practices, because neither existing organisational nor technological protections could have helped him.

These behavioural tools for privacy protection are by no means a silver bullet to the privacy problem. They do not aim to replace the three types of protections tools existing thus far. They rather aim at supplementing and completing them. The proposition that solely a single type of protective measures cannot achieve privacy protection remains valid. Behavioural tools are addressed to those individuals who are conscious of both their privacy and threats thereto, who perceive these threats as directly relevant for them (and the societal group they belong to) and who consider these threats as significantly dangerous for them (and to these groups). Yet these tools are often less easy to apply in practice. A careful reader would further conclude these protections know no jurisdictional boundaries, are predominantly applicable to informational aspect of privacy when challenged by digital technologies and produce best effects if applied *ex ante*. I have focused on individuals and their privacy, but I cannot exclude other stakeholders making choices, undertaking actions and inactions to protect privacy, their own or others, and – further – their other interests. But this is a subject matter for separate analysis.

This contribution has been an invitation to stakeholders – from the layman on the street and the computer ‘geek’ to those who regulate, handle information to those who oversee compliance, having diverse roles and responsibilities – to consider behavioural tools as a standalone and legitimate means of privacy protection. The way in which I have presented this novelty here is, obviously, not final. With the ever-changing nature of the society and technology, this new type of tools would require re-visiting and re-conceptualising, should the need arise.