Chapter 16
On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law

Ugo Pagallo

16.1 Introduction

In the first edition of *The Sciences of Artificial* (1969), Herbert A. Simon lamented the lack of research on "the science of design" which characterized the curricula of both professional schools and universities throughout three decades after the Second World War. In the phrasing of the Nobel laureate, the reason hinged on academic respectability, because "in terms of the prevailing norms, academic respectability calls for subject matter that is intellectually tough, analytic, formalizable, and teachable. In the past much, if not most, of what we knew about design and about artificial sciences was intellectually soft, intuitive, informal, and cook-booky" (Simon 1996, 112).

Thirty years later, in *Code and Other Laws of Cyberspace* (1999), Lawrence Lessig similarly stressed the lack of research on the impact of design on both social relationships and the functioning of legal systems, that is, how human behaviour may be shaped by the design of spaces, places and artefacts (*op. cit.*, pp. 91–92).

Thenceforth, the scenario has dramatically changed. Not only, according to Simon, an academically respectable "science of design" has emerged since the mid 1970s, when the *Design Research Centre* was founded at Carnegie Mellon University (the institute became the "Engineering Design Research Centre" in 1985). Significantly, over the last 10 years, legal scholars and social scientists have increasingly focused on the ethical and political implications of employing design mechanisms to determine people's behaviour through the shaping of products, processes, and Information & Communication Technology (ICT)-interfaces and platforms.

On one hand, let me mention work on the regulatory aspects of technology in such fields as universal usability (Shneiderman 2000); informed consent (Friedman et al. 2002); crime control and architecture (Katyal 2002, 2003); social justice (Borning et al. 2004); allegedly perfect self-enforcement technologies on the internet (Zittrain 2007); and design-based instruments for implementing social policies (Yeung 2007).

Ugo Pagallo (✉)
Law School, University of Torino, via s. Ottavio 54, 10124 Torino, Italy
e-mail: ugo.pagallo@unito.it

S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*,
DOI 10.1007/978-94-007-2903-2_16, © Springer Science+Business Media B.V. 2012

On the other hand, following seminal work on the ethics of design (Friedman 1986; Mitcham 1995; Whitbeck 1996), and privacy (Agre 1997), it is noteworthy that scholars have examined data protection issues raised by the design of ICT, by the means of value-sensitive design (Friedman and Kahn 2003; Friedman et al. 2006), legal ontologies (Abou-Tair and Berlik 2006; Mitre et al. 2006; Lioudakis et al. 2007), projects on platforms for privacy preferences (P3P), (Jutla and Zhang 2005; Cranor et al. 2008; Reay et al. 2009) and PeCAN platforms (Jutla et al. 2006; Jutla 2010), down to the topology of complex social networks (Pagallo 2007). In addition, the idea of incorporating data protection safeguards in ICT was the subject matter of both "Privacy by Design. The Definitive Workshop" organized in Madrid in November 2009 (Cavoukian 2010), and the "Intelligent Privacy Management Symposium" held at Stanford University, CA., on 22–24 March 2010 (the program is online at http://research.it.us.edu.au/magic/privacy2010/schedule.html).

Although the idea of embedding privacy safeguards in information systems and other types of technology is not new, e.g., recital 46 and Article 17 of the European Union (EU) directive 46 from 1995 (D-46/95/EC), privacy commissioners have been particularly active in recent times. For example, in the document on "The Future of Privacy" from the 1 December 2009, the European authorities on data protection, that is, the EU Working Party Article 29 D-95/46/EC have frankly admitted that a new legal framework is needed and, more particularly, it "has to include a provision translating the currently punctual requirements into *a broader and consistent principle of privacy by design*. This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT" (WP29 2009). Among the examples of how the new principle can contribute to better data protection, the WP29 recommends what Norman Potter presented in his 1968 book *What is a Designer* (Potter 2002) as "environmental design" (i.e. designing spaces) and "product design" (i.e. forging objects).

As an illustration of the first kind of design, think about people's anonymity and the challenge of protecting people's privacy in public (Nissenbaum 1998). While the use of, say, CCTVs proliferates and seems unstoppable, the European authorities on data protection propose to design video surveillance in public transportation systems, in such a way that faces of individuals cannot be recognizable (WP29 2009).

Similarly, when making personal data anonymous is considered a priority, matters of design also concern how we organize data processes and product design. A typical instance is given by the WP29's example on the processing of patient names in hospitals via information systems, where patient names should be kept separated from data on medical treatments or health status. Likewise, in accordance with the principle of controllability and confidentiality of the data to be processed, biometric identifiers "should be stored in devices under control of the data subjects (i.e. smart cards) rather than in external data bases" (WP29 2009).

(In the third section of the paper, I address another kind of design that Norman Potter calls communication design. A good example is given by the user friendliness of ICT interfaces and public complaints against Facebook's data protection policies. Whether or not we buy this form of privacy by design, the social network announced on 26 May 2010, to have "drastically simplified and improved its privacy controls" which previously amounted to 170 different options under 50 data protection-related settings. . .)

Meanwhile, the Ontario's Privacy Commissioner, Ann Cavoukian, has developed the formula "privacy by design" she invented in the late 1990s, so as to cope with the "ever-growing and systemic effects" of both ICT and large-scale networked data systems (Cavoukian 2009). After more than 10 years of efforts and increasing success, the Commissioner organized the aforementioned "definitive workshop" on the principle of privacy by design in November 2009. On that occasion, Cavoukian summed up the idea of handling today's data protection issues, according to seven principles:

1. We have to view data protection in proactive rather than reactive terms, making privacy by design preventive and not simply remedial;
2. Personal data should be automatically protected in every IT system as its default position;
3. Data protection should accordingly be embedded into design;
4. The full functionality of the principle which follows from (2) and (3) allows a positive-sum or win-win game, making trade-offs unnecessary (e.g. privacy vs. security);
5. A cradle-to-grave, start-to-finish, or end-to-end lifecycle protection ensures that privacy safeguards are at work even before a single bit of information has been collected;
6. No matter the technology or business practices involved, the design project should make data protection mechanisms visible and transparent to both IT users and providers;
7. Finally, the principle "requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options" (Cavoukian 2010). In other words, privacy by design requires an individual-focused respect for user privacy.

In the light of these seven tenets, I admit that the principle of privacy by design looks particularly promising in such different fields as data protection in CCTV systems, biometrics, social networks, smart environments, data loss prevention and more. The principle may in fact represent a turning point in how we address most of the challenges in data protection due to the development of cloud computing, the internet of things, or the semantic Web (Kim et al. 2002; Jutla and Xu 2004; Breuker et al. 2009), by strengthening people's habeas data and allowing us to prevent the risk of hampering economic growth due to alleged privacy reasons. Moreover, the principle shows an effective way to solve some of the extra-territorial legal effects and jurisdictional issues created by digital technology, since privacy assurance can become a default mode of operation for both private companies and public institutions in transnational law (Pagallo 2008).

However, this success entails its own risks, such as current misapprehensions in today's debate and divergent interpretations of the principle among commissioners and scholars. Whereas some propose a version of the principle of privacy "as" design, that is, making most legal provisions on data protection preventive and automatic, it is far from clear what type of design mechanism the WP29 is referring to, when claiming that privacy by design "should be binding" for data controllers, technology designers and producers (WP29 2009). Should the aim be to integrate compliance with regulatory frameworks through design policies or, conversely, should the aim be to prevent harm-generating behaviour from occurring?

In order to offer a hopefully comprehensive view of these issues, this chapter is presented in three sections.

First, I examine the idea of making all the legal provisions on data protection automatic, according to points (ii), (iii), and (v) of Cavoukian's scheme (2010). As shown by 10 years of efforts on the development of platforms for privacy preferences, "the P3P specification is not yet mature enough in terms of element definitions to handle many legal subtleties cleanly" (Jutla 2010). Far from being mere subtleties, however, the first section of the chapter aims to show that such legal hurdles to the "end-to-end lifecycle" of data protection regard some of the most important notions of the legal framework, that is, highly context-dependent normative concepts like data controller, security measure or, even, personal data.

Secondly, these difficulties emphasize the ethical issues of design and the strong moral responsibilities behind the use of alleged perfect self-enforcement technologies. Whereas individual preferences play a crucial role in determining levels of access and control over information in digital environments, people's behaviour would unilaterally be determined on the basis of automatic techniques rather than by choices of the relevant political institutions (Lessig 2004). In the name of individual autonomy, this is why I propose to frame the ethical issues of design and its modalities, by adopting a stricter version of the principle (Pagallo 2009).

Thirdly, such a stricter version of privacy by design is examined in connection with the democratic rule of law and the principle that individuals have to have a say in the decisions affecting them. As suggested by the European Data Protection Supervisor (EDPS), Peter Hustinx, in the Opinion from 25 July 2007 (2007/C 255/01), the challenge of protecting personal data "will be to find practical solutions" through typical transnational measures such as "the use of binding corporate rules by multinational companies" and "international agreements on jurisdiction" (*op. cit.*, § 44). Analogously, efforts should aim at "promoting private enforcement of data protection principles through self-regulation and competition" (*op. cit.*, § 65), while "accepted standards such as the OECD-guidelines for data protection (1980) and UN-Guidelines could be used as basis" (*op. cit.*, § 44).

To conclude, privacy by design should encourage people to change their conduct (e.g. user-friendly interfaces), or limit the effects of harmful behaviour (e.g. security measures) by strengthening people's rights and broadening the range of their choices. There is, indeed, "respect for user privacy" (Cavoukian 2010), when averting both the risks of paternalistic drifts and further conflicts of values in the realm of privacy by design. Rather than a "cradle-to-grave lifecycle" of automatic protection, let us reinforce the pre-existing individual autonomy (Pagallo 2011a).

16.2 Technology and its Limits

I mentioned some of the different ways the scholars have addressed points (ii), (iii) and (v) of Cavoukian's scheme, so that personal data should automatically be protected in every IT system as its default position and even before a bit of information has been collected. Leaving aside value sensitive design-approaches, P3P and PeCAN platforms, let me focus on current efforts in Artificial Intelligence (AI) & Law and, more specifically, in legal ontologies, so as to stress the first limit of the principle of privacy by design, that is, current state-of-the-art in technology.

Legal ontologies is the field of AI that aims to model concepts traditionally employed by lawyers through the formalization of norms, rights and duties, in fields like criminal law, administrative law, civil law, etc. (Breuker et al. 2009; Casanovas et al. 2010). The objective is that even a machine should comprehend and process this very information, by preliminarily distinguishing between the part of the ontology containing all the relevant concepts of the problem domain through the use of taxonomies (e.g. ontological *requirements*), and the ontology which includes both the set of rules and restraints that belong to that problem domain (e.g. ontological *constraints)*. An expert system should thus process the information in compliance with regulatory legal frameworks through the conceptualization of classes, relations, properties and instances pertaining to that given problem domain of data protection. Following what has been said about the ongoing project on the "Neurona Ontology" developed by Pompeu Casanovas and his research team in Barcelona, Spain, the goal is to implement new technological advances in managing personal data and provide organizations and citizens "with better guarantees of proper access, storage, management and sharing of files" (Casellas et al. 2010). By programming the software of the system to comply with regulatory frameworks of data protection, it is feasible to help company officers and citizens "who may have little or no legal knowledge whatsoever."

In technical terms, we should pay attention to the bottom-up approach that starts from legal concepts defined by scholars. A traditional top-down approach works well for the *topmost level*, where the representation instruments are at the disposal of the ontology-builders and the basic conceptual primitives such as relation, role, qualia, processes, etc., are precisely defined. However, a lot of issues arise when the *core ontology* level is taken into account, because the amount of information involved in the project of making data protection safeguards automatic is hardly compressible. Simply put, data protection regulations not only include "top normative concepts" such as notions of validity, obligation, prohibition, and the like. These rules present also highly context-dependent normative concepts like personal data, security measures, or data controllers. In order to grasp some of the difficulties of embedding data protection safeguards in a software program, simply reflect on three facts:

1. In the aforementioned document on "The Future of Privacy", the EU WP29 warns that "Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects";

2. In the Opinion from the 1 February 2010, the EU WP29 insisted that "the concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Therefore, determining control may sometimes require an in-depth and lengthy investigation" (doc. 00264/10/EN WP 169)
3. Finally, on 23 March 2010, the European Court of Justice declared that liability of online referencing service providers depends on "the actual terms on which the service is supplied." In other words, according to the judges in Luxembourg, it is necessary to determine "whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores" (*Google v. Louis Vuitton case*, § 114 of the decision).

The difficulty to program the WP29's "factual influence" of the data controller or the ECJ's "actual terms" of the service provided on the internet, does not mean that projects on legal ontologies and privacy by design should be abandoned. On the contrary, these difficulties suggest a bottom-up rather than a top-down approach, in order to lawfully process growing amounts of personal data. By splitting the work into several tasks and assigning each to a working team, we should start from smaller parts and sub-solutions of the design project, to end up with "global answers" (Casellas et al. 2010). The evaluation phase consists in testing the internal consistency of the project and, according to Herbert Simon's "generator test-cycle," entails the decomposition of the complete design into functional components. The test generates alternatives and examines them against the set of *requirements* and *constraints*, so that "important indirect consequences will be noticed and weighed. Alternative decompositions correspond to different ways of dividing the responsibilities for the final design between generators and tests." (Simon 1996, 128)

Further criteria and empirical methods have been proposed: apart from functional efficiency, we should consider the robustness, reliability, and usability of design projects. Evaluation and verification of the design can additionally employ automated and regression-oriented tests, use of prototypes, internal checks among the design team, users tests in controlled environments, surveys, interviews and more (Flanagan et al. 2008). On this basis, we can quantify the growing amount of personal data processed in compliance with regulatory frameworks. This is the focus of the research on legal ontologies and the support of privacy preservation in location-based services (Mitre et al. 2006), the management of information systems (Abou-Tabir and Berlik 2006; Casellas et al. 2010), or middleware architectures for data protection (Lioudakis et al. 2007), each of which aims at integrating smaller parts and sub-solutions into the design. Remarkably, there are even cases where the conceptualization of classes, relations, properties and instances pertaining to a given problem domain, does not seem particularly complex, for example, the design of information systems for hospitals to ensure that patient names are kept separated from data on medical treatments or health status (WP29 2009).

However, by lawfully processing growing amounts of personal data, it does not follow that goals (ii), (iii) and (v) of Cavoukian's scheme, that is, making data protection automatic by design, are at hand. Besides the difficulty of formalizing highly context-dependent concepts such as data processor or data controller, designers must take into account that privacy is not a zero-sum game between multiple instances of access and control over information. Personal choices play indeed the main role when individuals modulate different levels of access and control, depending on the context and its circumstances (Nissenbaum 2004). Moreover, people may enjoy privacy in the midst of a crowd and without having total control over their personal data, whereas total control over that data does not necessarily entail any guarantee of privacy (Tavani 2007). Such constraints emphasize the first limit of the principle: in accordance with today's state-of-the-art, no expert system allows us to fully achieve goals (ii), (iii) and (v) of Cavoukian's principles of privacy by design. To the best of my knowledge, it is impossible to programme software so as to prevent, say, forms of harm-generating behaviour as simple as defamations, but leaving aside technical details, how about the desirability of such a project?

16.3 Ethical Constraints

Some of the most relevant problems concerning today's data protection hinge on the information revolution and the fact that no clear legal boundaries exist in digital environments. State-action is often ineffective due to the ubiquitous nature of information: while citizens of nation states are often affected by conduct that the state is unable to regulate (e.g. spamming), this situation may also lead to the illegitimate condition where a state claims to regulate extraterritorial conduct by imposing norms on individuals, who have no say in the decisions affecting them (Post 2002). According to the 2007 EDPS Opinion, "this system, a logical and necessary consequence of the territorial limitations of the European Union, will not provide full protection to the European data subject in a networked society where physical borders lose importance (. . .): the information on the Internet has an ubiquitous nature, but the jurisdiction of the European legislator is not ubiquitous" (Hustinx 2007).

The ineffectiveness of state-action depends on how ICT allows information to transcend traditional legal borders, questioning the notion of the law as made of commands enforced through physical sanctions. Spamming is again a good example for it is par excellence *transnational* and does not diminish despite harsh criminal laws (as the *CAN-SPAM Act* approved by the U.S. Congress in 2003). Since the mid 1990s, as a consequence, companies and big business have tried to find out a remedy for the apparent inefficacy of state-action in protecting their own rights. While lobbying national and international law-makers in the copyright field, some of the most relevant companies focused on how to enforce their (alleged) exclusivity rights through the development of self-enforcement technologies, for example, Digital Rights Management (DRM). By enabling right-holders to monitor and regulate the use of their own copyright protected works, companies would have prevented unsolvable problems involving the enforceability of national laws and conflicts of law at the international level.

However, whether or not DRM works and can be held to be fair, the aim of privacy by design, that is, to exert "automatic control" over personal information is even more debatable than the use of DRM technology for the protection and enforcement of digital copyright. Whereas Steve Jobs (2007) conceded in his *Thoughts on Music* that DRM-compliant systems raise severe problems of interoperability and, hence, antitrust-related challenges, the aim of privacy by design to automatically prevent harm-generating conducts from occurring looks problematic for three reasons.

First, we have evidence that "some technical artefacts bear directly and systematically on the realization, or suppression, of particular configurations of social, ethical, and political values" (Flanagan et al. 2008). Specific design choices may result in conflicts between values and, vice versa, conflicts between values may impact on the features of design. Consider the different features that privacy by design acquires, once data protection is grasped in terms of property rights or human dignity, of total control or contextual integrity, of restricted access or limited control over digital information. At the end of the day, should an artefact be designed in accordance with the opt-in model for users of electronic communication systems or, vice versa, according to the opt-out approach? Moreover, reflect upon the information system of hospitals which I mentioned in the previous section: should we privilege the efficacy and reliability of that information system in keeping patient names separated from data on medical treatments or health status? How about users, including doctors, who may find such mechanism too onerous?

Secondly, attention should be drawn to the difficulties of achieving such total control. Doubts are cast by "a rich body of scholarship concerning the theory and practice of 'traditional' rule-based regulation [that] bears witness to the impossibility of designing regulatory standards in the form of legal rules that will hit their target with perfect accuracy" (Yeung 2007). The worthy aim to prevent people's privacy infringements involves *strong moral responsibility* of both the designers and public authorities, in that use of self-enforcement technologies collapses "the public understanding of law with its application eliminating a useful interface between the law's terms and its application" (Zittrain 2007). As a response to the inefficacy of state-action in digital environments, the development of this type of technology risks to curtail freedom and individual autonomy severely, because people's behaviour would unilaterally be determined on the basis of technology, rather than by choices of the relevant political institutions. In the phrasing of Larry Lessig, "the controls over access to content will not be controls that are ratified by courts; the controls over access to content will be controls that are coded by programmers" (Lessig 2004).

Finally, there is the issue of security in balancing different levels of access and control via software: the expert system should not be capable to only balance personal preferences *and* matters of "property rights" (Spinello 2003), "trade-offs" (Nissenbaum 2004), or "integrity" (Grodzinsky and Tavani 2008), which often depend on contextual choices. In fact, design projects should be capable to evaluate this (sensitive) information safely, although experts warn that "the only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts" (Garfinkel and Spafford 1997). Whereas the use of self-enforcement technologies may be compatible with the precautionary principle in the area of intellectual property rights (Weckert and Moor 2004; Clarke 2005), this does not seem to be the case of privacy by design. DRM's shortcomings principally impact on companies that employ such devices to protect their own copyright protected files: in the case of privacy, however, the use of alleged self-enforcement technologies would directly impact on everyone of us as "informational objects" (Floridi 2006).

Therefore, I suggest abandoning the idea of making data protection automatic by design, so as to prevent every harm-generating conduct from occurring.

Rather, we should focus on other mechanisms we may aim at through design, that is, both the aim to encourage the change of people's behaviour via user friendly interfaces and to decrease the impact of harm-generating conducts through "digital air-bags" as encryption and other security measures (von Ahn et al. 2008).

Let us examine projects on privacy by design, by considering today's "habeas data" in connection with the principle of the rule of law.

16.4 Habeas Data

As shown by the proceedings of the 2009 IVR 24th World Congress in Beijing, China, on *Global Harmony and the Rule of Law* (see http://www.ivr2009.com/), not only "harmony" is a very controversial concept of the millennial political tradition of China, but Western scholars are sparkly divided by the meaning of the "rule of law" as well (whether or not we conceive it as the German *Rechtsstaat*, the French *État de droit*, the Spanish *Estado de derecho*, the Italian *Stato di diritto*, and so forth). While the appeal of the formula historically derives from Plato's distinction between the "empire of the laws," that is, rule by law, and "empire of men," namely, rule under the will of men, it is unclear whether the view of the rule of law adopts a thin-procedural or a thick-substantive approach to distinguishing between rule of law, rule by law, etc. (Summers 1993). It is noteworthy that "despite a growing empirical literature, there remain serious doubts about the relationship, and often causal direction, between the rule of law and the ever-increasing list of goodies with which it is associated, including economic growth, poverty reduction, democratization, legal empowerment and human rights" (Peerenboom 2009).

In this context, it suffices to dwell on the traditional connection between the rule of law and the principle of *habeas corpus*, that is, individual protection against arbitrary (both public and private) action. Over the last two decades, several provisions on data protection, for example, Article 8 of the EU Charter of Fundamental Rights, have complemented the traditional version of the principle of *habeas corpus*, linked to the physical body, with a new kind of protection, that is *habeas data*, as an extension of that protection to the electronic body of each individual (Rodotà 2006). What is at stake with the principle of privacy by design accordingly concerns whether some kinds of "electronic protection" violate people's right to have a say in the decisions affecting them, that is, what the German Constitutional Court frames in terms of the individual "informational self-determination." As well known, the *Bundesverfassungsgericht* (BVerfG) has furthered the concept since its *Volkszählungs-Urteil* ("census decision") from 15 December 1983.

Furthermore, we have to ascertain whether protection of the electronic body via design policies may entail what Kant criticized as paternalism (Kant 1891). By adopting a sort of automatic *habeas data*, the threat is to impinge on the "property of the will" to rule over itself, so that, according to *Grounding for the Metaphysics of Morals*, the risk is to overprotect individuals against every harm and, even, against themselves. In the light of the panoply of projects and approaches in the field of data protection mentioned in this paper, it is crucial to preliminarily distinguish three aims of design (Yeung 2007), so as to take sides on the legal constraints of the principle:

1. Design may prevent harm-generating behaviour from occurring;
2. Design may aim to decrease the impact of harm-generating conducts;
3. Design may encourage the change of social behaviour.

Although design is not necessarily digital (Lessig 1999), the information revolution has induced a more sophisticated legal enforcement than, say, the installation of speed bumps in roads to reduce the velocity of cars. In the case of data protection, scholars should determine what kind of design mechanism is compatible with the tenets of the rule of law, in order to ensure the minimization and quality of the data, its controllability, transparency, and confidentiality, down to the user friendliness of information interfaces.

The first aim of design mechanism, that is, the prevention of harmful conducts thanks to the use of self-enforcement technologies, seems highly problematic in this context. Besides the technical and ethical reasons that make such a protection neither feasible nor desirable in the realm of *habeas data*, perfect automation of data protection mechanisms impinges on the individual right to the "informational self-determination"—that is, the *informationelle Selbstbestimmung* of the BVerfG—which includes the right to determine whether personal data can be collected and, eventually, transmitted to others; the right to determine how that data may be used and processed; the right to access that data and, where necessary, to keep it up to date; besides the right to delete that data and to refuse at any time to have the data processed. Since the enforcement and guarantee of most of these rights are beyond today's state-of-the-art in technology (see Sect. 16.2), it follows that an automatic *habeas data* would impose norms on subjects who have no say in the decisions affecting them (Lessig 2004; Zittrain 2007), thereby making people lose their capacity for making moral choices (Brownsword 2005). Instead of letting people determine autonomously levels of access and control over personal data, depending on personal choices and circumstances, the use of self-enforcement technologies seems incompatible with a basic tenet of the democratic rule of law—autonomy.

But, how about the remaining mechanisms of privacy by design, that is, when the aim is not to prevent certain actions from being chosen overall, but to merely inspire a different conduct by encouraging people to change their behaviour or decreasing the impact of harm-generating conducts? Are these aims compatible with the rule of law?

On one hand, design mechanisms closely regard point (vii) of Cavoukian's principles of privacy by design, that is, the individual-focused approach respectful of user privacy. The idea is well represented by current efforts on security measures, location-based services, friendly interfaces, P2P overlay platforms, default settings and more (Pagallo 2011b). In all the examples of *this* type of design mechanisms, it is arguably correct to stress that "privacy assurance must ideally become an organization's default mode of operation" (Cavoukian 2009). The aim to decrease the impact of harm-generating conducts, as air-bags do in cars, does not seem to impinge on individual autonomy and personal data, because ICT mechanisms as well as air-bags are designed to respect people's choices when they, say, drive cars or modulate different levels of privacy, according to the context. As an instance of "digital air-bags," consider "the power of defaults" (Kesan and Shah 2006), so that we can ensure that values of design are appropriate for novice users and, still, the system improves efficiency. Likewise, reflect on modifications to user interfaces by increasing, or reducing, the prominence of a default setting, so as to allow users to configure and use their software as they deem appropriate. Moreover, consider security measures, such as reCAPTCHA, that aim to prevent automated programs from abusing online services (von Ahn et al. 2008). The aim of such design projects that reduce the effects of harmful conducts fully respects the Kantian principle of autonomy because the only responsibility, both legal and moral, which is at stake with this type of design mechanism concerns the technical meticulousness of the project and its reliability, as it occurs with security measures for the information systems of an atomic plant or a hospital.

On the other hand, by encouraging the change of social behaviour, design projects suggest to assess the impact of design choices on people's conduct. This is the case of the free-riding phenomenon on P2P file-sharing networks, where most peers tend to use these systems to find information and download their favourite files without contributing to the performance of the system. Whilst this behaviour is triggered by many properties of P2P applications like anonymity and hard traceability of the nodes, designers have proposed ways to tackle the issue through incentives based on trust (e.g. reputation mechanisms), trade (e.g. services in return), or alternatively slowing down the connectivity of the user who does not help the process of file-sharing (Glorioso et al. 2010). The editorials in *The Economist* aside, some scholars have nevertheless stressed a threat of paternalism behind the very idea of encouraging the change of people's behaviour (Kruner 2003; Volkman 2003). After all, this type of design mechanism may represent a way of modelling social conduct so as to protect people against all forms of harm. This threat makes urgent a normative viewpoint such as information ethics (Floridi 2005), online privacy policies (Tavani 2007), ethics of design (Friedman 1986; Mitcham 1995; Whitbeck 1996; Flanagan et al. 2008), machine ethics (Moor 2006; McLaren 2006), and more, for we should previously test the goodness of data protection laws, in order to prove the goodness of our own design projects. Is there a way to ensure that privacy by design does not violate the anti-paternalistic stance of the rule of law by encouraging people to change their conduct? How about conflicts between values that necessarily reverberate on design choices? Is, say, Jeffrey Rosen right, when stressing the fear that "cultural differences will make thoughtful regulation difficult" in data protection? What does it mean for data protection that "the French will bare their breasts but not their salaries and mortgages, and the reverse is true in the U.S."? (As Rosen declares in Mills 2008.)

Although it is notoriously difficult to solve conflicts of values with their divergent interpretations, we might prevent most issues in today's *cul de sac* by embracing one of the several examples and design mechanisms put forward by the EU Working Party's document on "The Future of Privacy." Whether or not you agree that the European legal framework "is clearly and deeply flawed as an account of what informational protection is all about" (Volkman 2003), we need not sympathize with Brussels to follow the proposal that the principle of privacy by design should be implemented in accordance with a bottom-up rather than a top-down approach, that is, depending on individual autonomous choices via self-regulation and competition among private organizations (WP29 2009).

As a result, besides a stricter version of privacy by design as a way to decrease the "informational entropy" of the system through "digital air-bags," we find a further design mechanism compatible with the rule of law. When encouraging people to change their behaviour by the means of design, the overall goal should be to reinforce people's pre-existing autonomy, rather than building it from scratch. In the wording of the EU privacy commissioners, the principle should enable business and individuals to "take relevant security measures by themselves" (WP29 2009).

16.5 Conclusions

It is unlikely that privacy by design will offer the one-size-fits-all solution to the problems in the realm of data protection, although privacy by design is a good candidate for understanding how we have coped with privacy issues over the last few years. The principle may in fact be a turning point in how we address most of the challenges in data protection, by strengthening people's habeas data, without hampering economic growth for alleged privacy reasons. In different fields as data protection in CCTV systems, biometrics, social networks, smart environments, data loss prevention and more, projects are increasingly processing growing amounts of personal data in compliance with current normative frameworks, strengthened by the capacities of computers to draw upon the tools of AI and operations research.

Notwithstanding the merits, however, there are three reasons why we should be aware of the limits of privacy by design. These limits are especially relevant when the aim is to automatically protect personal data as the default position of every ICT system, even before a single bit of information has been collected, that is, points (ii), (iii) and (v) of Cavoukian's scheme on the principle (Cavoukian 2010). Let me sum up these limits.

First, I mentioned work on legal ontologies, value-sensitive design, P3P or PeCAN platforms, so as to show the limits of today's state-of-the-art in technology. Besides the difficulty of modelling highly context-dependent normative concepts as data controllers and the "neutrality" of the services provided on the internet, designers should take into account that privacy is not a zero-sum game but concerns personal choices on levels of access and control over information that often depend on the context. Making all the provisions of data protection automatic is simply out of reach.

The second limit involves the ethical constraints of the approach and the process of both law-making and legal enforcement. Not only conflicts between values do impact on the features of design but, vice versa, design choices may result in further conflicts between values. Since privacy may be conceived in terms of human dignity or property rights, of contextual integrity or total control, it follows that privacy by design acquires many different features. Moreover, self-enforcement technologies risk to curtail freedom and individual autonomy severely, because people's behaviour would be determined on the basis of design rather than by individual choices.

Finally, two tenets of the rule of law, that is, autonomy and anti-paternalism, stressed the legal constraints of privacy by design as a means to prevent harm-generating behaviour from occurring. By adopting a sort of automatic *habeas data*, the risk is to impinge on what Kant defined the "property of the will" to rule over itself and, two centuries later, the BVerfG presented as the individual right to "informational self-determination." Leaving aside the technical unfeasibility of goals (ii), (iii) and (v) of Cavoukian's model, it is undisputable that the more personal choices are wiped out by automation, the bigger the threat of modelling social conduct via design, that is, Kantian paternalism.

As a consequence, this chapter has proposed a stricter version of the principle of privacy by design which seems to be technically feasible, ethically sound and lawful. On one hand, in accordance with goals (i) and (vi) of Cavoukian's scheme (2010), privacy by design can legitimately aim to automatically reduce the impact of harm-generating behaviour, so that "privacy assurance must ideally become an organization's default mode of operation" (Cavoukian 2009). Besides values of design that are appropriate for novice users and, hence, procedural constraints for changing the setting of the interfaces on voluntary and fully informed basis, I mentioned security measures that aim to prevent automated programs from abusing online services: "digital air-bags" as friendly interfaces, P2P overlay platforms or default settings will not impinge on individual autonomy, no more than traditional air-bags affect how people drive. On the other hand, in connection with point (vii) of Cavoukian's model, privacy by design can legitimately aim to encourage the change of social behaviour if, and only if, the goal is to strengthen people's rights by widening the range of their choices. This is the version of the principle put forward by the example of both the WP29 and the European Data Protection Supervisor, when endorsing the enforcement of data protection through self regulation and competition (Hustinx 2007; WP29 2009), thus preventing claims of paternalism by fostering individual habeas data.

The result is a final convergence over the "full functionality" of the principle, that is, point (iv) of Cavoukian's scheme. A positive-sum or win-win game becomes possible by embedding data protection safeguards in technology with the aim to encourage people to change their conduct as well as to decrease the effects of harmful behaviour. As shown by current work on legal ontologies, middleware architectures for data protection, the management of information systems, and more, trade-offs such as privacy vs. business, privacy vs. security, privacy vs. copyright, are not always necessary. However, it is not only a matter of business and security—privacy by design concerns a basic tenet of the rule of law such as the principle of autonomy.

References

Abou-Tair, D. el Diehn I., and Stefan Berlik. 2006. An ontology-based approach for managing and maintaining privacy in information systems. *Lectures notes in computer science*, 4275: 983–994 (Berlin-Heidelberg: Springer).

Agre, Philip E. 1997. Introduction. In *Technology and privacy: The new landscape*, eds. Philip E. Agre and Mark Rotenberg, 1–28. Cambridge: The MIT Press.

von Ahn, Luis, Maurer, Benjamin, McMillen, Colin, Abraham, David, and Manuel Blum. 2008. reCAPTCHA: Human-based character recognition via web security measures. *Science* 321 (5895): 1465–1468.

Borning, Alan, Friedman, Batya, and Peter H. Kahn. 2004. Designing for human values in an urban simulation system: Value sensitive design and participatory design. *Proceedings of eighth biennial participatory design conference*, 64–67. Toronto: ACM Press. http://www.urbansim.org/pub/Research/ResearchPapers/vsd-and-participatory-design-2004.pdf. Accessed 23 Dec 2010

Breuker, Joost, Casanovas, Pompeu, Klein, Michel C.A., and Enrico Francesconi (eds.). 2009. *Law, ontologies and the semantic web*. Amsterdam: IOS Press.

Brownsword, Roger. 2005. Code, control, and choice: Why east is east and west is west. *Legal Studies* 25 (1): 1–21.

Casanovas, Pompeu, Pagallo, Ugo, Sartor, Giovanni, and Gianmaria Ajani (eds.). 2010. AI approaches to the complexity of legal systems. *Complex systems, the semantic web, ontologies, argumentation, and dialogue*. Berlin: Springer.

Casellas, Nuria, Torralba, Sergi, Nieto, Juan-Emilio, Meroño, Albert, Roig, Antoni, Reyes, Mario, and Pompeu Casanovas. 2010. The Neurona ontology: A data protection compliance ontology. Paper presented at the intelligent privacy management symposium, Stanford University, CA., USA. 22–24 March 2010.

Cavoukian, Ann. 2009. *Privacy by design*. Ottawa: IPC.

Cavoukian, Ann. 2010. Privacy by design: The definitive workshop. *Identity in the Information Society* 3 (2): 247–251.

Clarke, Steve. 2005. Future technologies, dystopic futures and the precautionary principle. *Ethics and Information Technology* 7 (4): 121–126.

Cranor, Lorrie F., Egelman, Serge, Sheng, Steve, McDonald, Aleecia M., and Abdur Chowdhury. 2008. P3P deployment on websites. *Electronic Commerce Research and Applications* 7 (3): 274–293.

Flanagan, Mary, Howe, Daniel C., and Helen Nissenbaum. 2008. Embodying values in technology: Theory and practice. In *Information technology and moral philosophy*, eds. Jeroen van den Hoven and John Weckert, 322–353. New York: Cambridge University Press.

Floridi, Luciano. 2005. Information ethics, its nature and scope. *Computers and Society* 36 (3): 21–36.

Floridi, Luciano. 2006. Four challenges for a theory of informational privacy. *Ethics and Information Technology* 8 (3): 109–119.

Friedman, Batya. 1986. Value-sensitive design. *Interactions* 3 (6): 17–23.

Friedman, Batya, Howe, Daniel C., and Edward Felten. 2002. Informed consent in the mozilla browser: Implementing value-sensitive design. *Proceedings of 35th annual hawaii international conference on system sciences* 247. IEEE Computer Society.

Friedman, Batya, and Peter H. Kahn Jr. 2003. Human values, ethics, and design. In: *The human-computer interaction handbook*, eds. Julie A. Jacko and Andrew Sear, 1177–1201. Mahwah: Lawrence Erlbaum Associates.

Friedman, Batya, Kahn, Peter H. Jr., and Alan Borning. 2006. Value sensitive design and information systems. In *Human-computer interaction in management information systems: Foundations*, eds. Ping Zhang and Dennis Galletta, 348–372. New York: Armonk.

Garfinkel, Simson, and Eugene Spafford. 1997. *Web security and commerce*. Sebastopol: O'Reilly.

Glorioso, Andrea, Pagallo, Ugo, and Giancarlo Ruffo. 2010. The social impact of P2P systems. In *Handbook of peer-to-peer networking*, eds. Xuemin Shen, Heather Yu, John Buford and Mursalin Akon, 47–70. Heidelberg: Springer.

Grodzinsky, Frances S. and Herman T. Tavani. 2008. Online file sharing: Resolving the tensions between privacy and property interest. In *Proceedings of ETHICOMP2008 "Living, Working and Learning Beyond Technology"*, eds. Terry W. Bynum, Maria Calzarossa, Ivo De Lotto and Simon Rogerson, 373–383. Mantova: Tipografia Commerciale.

Hustinx, Peter. 2007. Opinion of the European data protection supervisor on the communication from the commission to the European parliament and the council on the follow-up of the work program for better implementation of the data protection directive. *Official Journal of the European Union* 27 Oct. 2007, C 255: 1–12.

Jobs, Steve. 2007. Thoughts on music. http://www.apple.com/hotnews/thoughtsonmusic/. Accessed 20 April 2009.

Jutla, Dawn N., and Liming Xu. 2004. *Privacy agents and ontology for the semantic web. Americas conference on information systems*. New York City: CUSP.

Jutla, Dawn N., and Yanjun Zhang. 2005. Maturing E-privacy with P3P and context agents. In *Proceedings of IEEE international conference on E-Technology, E-Commerce and E-Service*, 536–541. Hong Kong.

Jutla, Dawn N., Bodorik, Peter, and Yanjun Zhan. 2006. PeCAN: An architecture for user privacy and profiles in electronic commerce contexts on the semantic web. *Information Systems* 31 (4–5): 295–320.

Jutla, Dawn N. 2010. Layering privacy on operating systems, social networks, and other platforms by design. *Identity in the Information Society* 3 (2): 319–341.

Kant, Immanuel. 1891. *Kant's principles of politics, including his essay on perpetual peace. A contribution to political science* (1795), (trans: Hastie W.). Edinburgh: Clark.

Katyal, Neal. 2002. Architecture as crime control. *Yale Law Journal* 111 (5): 1039–1139.

Katyal, Neal. 2003. Digital architecture as crime control. *Yale Law Journal* 112 (6): 101–129.

Kim, Anya, Hoffman, Lance J., and C. Dianne Martin. 2002. Building privacy into the semantic web: Ontology needed now. *Semantic web workshop 2002*. Honolulu, Hawaii. http://semanticweb2002.aifb.uni-karlsruhe.de/proceedings/Position/kim2.pdf. Accessed on 23 Dec 2011.

Kesan, Jay P. and Rajiv C. Shah. 2006. Setting software defaults: Perspectives from law, computer science and behavioural economics. *Notre Dame Law Review* 82:583–634.

Kuner, Christopher. 2003. *European data privacy law and online business*. Oxford: Oxford University Press.

Lessig, Lawrence. 1999. *Code and other laws of cyberspace*. New York: Basic Books.

Lessig, Lawrence. 2004. *Free culture: The nature and future of creativity*. New York: Penguin Press.

Lioudakis, Georgios, Koutsoloukasa, Eleftherios, Tselikasa, Nikolaos, Kapellakia, Sofia, Prezerakosa, Georg, Kaklamani, Dimitra and Iakovos Venieris. 2007. A middleware architecture for privacy protection. *The International Journal of Computer and Telecommunications Networking* 51 (16): 4679–4696.

McLaren, Bruce. 2006. Computational models of ethical reasoning: Challenges, initial steps, and future directions. *IEEE intelligent systems* 2006 (July/August): 29–37.

Mills, Elinor. 2008. To be anonymous or not to be, that is the privacy question: interview to jeffrey rosen. *News blog*. http://news.cnet.com/8301-10784_3-9889255-7.html. Accessed 15 Oct 2010.

Mitcham, Carl. 1995. Ethics into design. In *Discovering design*, eds. Richard Buchanan and Victor Margolin, 173–179. Chicago: University of Chicago Press.

Mitre, Hugo, Gonzàlez-Tablas, Ana Isabel, Ramos, Benjamin, and Arturo Ribagorda. 2006. A legal ontology to support privacy preservation in location-based services. *Lectures notes in computer science*, 4278: 1755–1764 (Berlin-Heidelberg: Springer).

Moor, James. 2006. The nature, importance, and difficulty of machine ethics. *IEEE intelligent systems* 21(4): 18–21.

Nissenbaum, Helen. 1998. Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy* 17 (5–6): 559–596.

Nissenbaum, Helen. 2004. Privacy as contextual integrity. *Washington Law Review* 79 (1): 119–158.

Pagallo, Ugo. 2007. Small world-paradigm and empirical research in legal ontologies: A topological approach. In *The multilanguage complexity of European law: Methodologies in comparison*, eds. Gianmaria Ajani, Ginevra Peruginelli, Giovanni Sartor and Daniela Tiscornia, 195–210. Florence: European Press Academic.

Pagallo, Ugo. 2008. *La tutela della privacy negli Stati Uniti d'America e in Europa: Modelli giuridici a confronto*. Milano: Giuffrè.

Pagallo, Ugo. 2009. Privacy e design. *Informatica e diritto* 1:123–134.

Pagallo, Ugo. 2011a. Designing data protection safeguards ethically. *Information* 2 (2): 247–265.

Pagallo, Ugo. 2011b. The trouble with digital copies: A short km phenomenology. In *Ethical issues and social dilemmas in knowledge management organizational innovation*, eds. Gonçalo J. Morais da Costa, 97–122. Hershey: IGI Global.

Peerenboom, Randy. 2009. The future of rule of law: The challenges and prospects for the field. *Hague Journal on the Rule of Law* 1 (1): 5–14.

Post, David G. 2002. Against "Against Cyberspace". *Berkeley Technology Law Journal* 17 (4): 1365–1383.

Potter, Norman. 2002. *What is a designer*. London: Hyphen Press.

Reay, Ian, Dick, Scott, and James Miller. 2009. A large-scale empirical study on P3P privacy policies: Stated actions vs. legal obligations. *ACM transactions on the web* 3(2): 1–34.

Rodotà, Stefano. 2006. The retention of electronic communication traffic data. *Revista d'Internet, dret i política* 3:53–60.

Shneiderman, Ben. 2000. Universal usability. *Communications of the ACM* 43 (3): 84–91.

Simon, Herbert A. 1996. *The sciences of the artificial*. Cambridge: The MIT Press.

Spinello, Richard A. 2003. The future of intellectual property. *Ethics and Information Technology* 5 (1): 1–16.

Summers, Robert S. 1993. A formal theory of rule of law. *Ratio Iuris* 6 (2): 127–142.

Tavani, Herman T. 2007. Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy* 38 (1): 1–22.

Volkman, Richard. 2003. Privacy as life, liberty, property. *Ethics and Information Technology* 5 (4): 199–210.

Weckert, John and James Moor. 2004. Using the precautionary principle in nanotechnology policy making. *Asia Pacific Nanotechnology Forum News Journal* 3 (4): 12–14.

Whitbeck, Caroline. 1996. Ethics as design: Doing justice to moral problems. *Hastings Center Report* 26 (3): 9–16.

Working Party (WP) Article 29 D-95/46/EC. 2009. *The future of privacy*. 02356/09/EN–WP 168.

Yeung, Karen. 2007. Towards an understanding of regulation by design. In *Regulating technologies: Legal futures, regulatory frames and technological fixes*, eds. Roger Brownsword and Karen Yeung, 79–108. London: Hart Publishing.

Zittrain, Jonathan. 2007. Perfect enforcement on tomorrow's internet. In *Regulating technologies: Legal futures, regulatory frames and technological fixes*, eds. Roger Brownsword and Karen Yeung, 125–156. London: Hart Publishing.