

Article

## Designing Data Protection Safeguards Ethically

Ugo Pagallo

University of Torino, Law School, via s. Ottavio 20, Torino 10124, Italy;

E-Mail: ugo.pagallo@unito.it

Received: 12 February 2011; in revised form: 2 March 2011 / Accepted: 14 March 2011 /

Published: 29 March 2011

---

**Abstract:** Since the mid 1990s, lawmakers and scholars have worked on the idea of embedding data protection safeguards in information and communication technology (ICT) with the aim to access and control personal data in compliance with current regulatory frameworks. This effort has been strengthened by the capacities of computers to draw upon the tools of artificial intelligence (AI) and operations research. However, work on AI and the law entails crucial ethical issues concerning both values and modalities of design. On one hand, design choices might result in conflicts of values and, *vice versa*, values may affect design features. On the other hand, the modalities of design cannot only limit the impact of harm-generating behavior but also prevent such behavior from occurring via self-enforcement technologies. In order to address some of the most relevant issues of data protection today, the paper suggests we adopt a stricter, yet more effective version of “privacy by design.” The goal should be to reinforce people’s pre-existing autonomy, rather than having to build it from scratch.

**Keywords:** AI and the law; autonomy; data protection; design; information ethics; legal ontologies; privacy by design; responsibility

---

### 1. Introduction

Over the past 15 years lawmakers and privacy commissioners have discussed the idea of embedding data protection safeguards in information and communication technology (ICT) In 1995, the obligation of data controllers to implement appropriate technical and organizational measures was laid down in the first European directive on data protection, namely, in Art 17 of D-95/46/EC. According to Recital 46 of the directive, the aim is to embed “appropriate measures” in ICTs “both at the time of the design

of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing” of personal data.

In the late 1990s, the concept of “Privacy by Design” was further developed by the Ontario’s Privacy Commissioner, Ann Cavoukian, to handle the “ever growing and systemic effects” of both ICT and large-scale networked data systems [1]. In April 2000, a working paper on “Privacy Design Principles for an Integrated Justice System” was jointly presented by the Ontario’s Privacy Commissioner and the U.S. Department of Justice.

Besides lawmakers and national advisors on data protection, scholars have dwelled on the topic as well. There has been seminal work on the ethics of design [2-4], and privacy [5]. Recently, research has focused on data protection issues involved in the design of ICT by means of value-sensitive designs [6,7], legal ontologies [8-10], P3P [11-13] and PeCAM platforms [14,15], down to the topology of complex social networks [16,17]. In addition, the idea of incorporating data protection safeguards in ICT was further discussed in “Privacy by Design. The Definitive Workshop” organized in Madrid in November 2009 [18], as well as in the “Intelligent Privacy Management Symposium” held at Stanford University, CA, USA, on March 22-24, 2010 (the program is available online at <http://research.it.uts.edu.au/magic/privacy2010/schedule.html>).

The topic being very popular, I believe that there are three reasons why current efforts on “privacy by design” are particularly relevant. First, there is a legal reason, in that most of the provisions on privacy and design have been disappointing. The European authorities on data protection, *i.e.*, the EU Working Party Art. 29 D-95/46/EC, have frankly admitted the impasse in the 2009 document on “The Future of Privacy” [19]. Not only is a new legal framework needed but, according to the EU commissioners, 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” [19].

Secondly, research on “privacy by design” is stimulated by current developments in the fields of artificial intelligence and operations research, which are disclosing new perspectives in how we can deal with flows of information in digital environments. It is enough to mention work in the “semantic Web” and its potential impact on data protection [20-22].

Finally, we have the open questions of the internet and its evolution. Apart from “generative technologies” like the PCs that allow innovation, experimentation and the wide-open web of creative anarchy on the internet, this technology permits the spread of copyright infringements, spam, and viruses as well [23]. These twofold features are evident in the case of file-sharing applications such as P2P systems [24,25]. Whereas some scholars describe this interaction as the key to a new paradigm, others claim that it undermines crucial elements of our societies, such as incentives for knowledge producers or protection of the personal sphere from unwanted scrutiny. As a result, generative technologies raise some of the problems Dieter M. Arnold and Herman Tavani put forward in the special issue of *Information* on “Trust and Privacy in Our Networked World”: How can I ensure that my disclosed personal data are not misused? How and when can I share personal data with trusted people only?

Moreover, these open questions are entwined with the current “balkanization” of the internet, namely, the set of digital walls which are being created, both for private and public reasons, at national and international levels.

On one hand, matters of trust and privacy in digital environments are suggesting both private companies and some hundred million people to opt for more reliable, yet sterile appliances like mobile phones, e-books and video games consoles. The trend is paradigmatically illustrated by Facebook’s closed e-mail system, or Apple’s archipelago of services and mobile devices.

On the other hand, in the name of sovereignty, nation-states are tightening control over the internet and play a fundamental role in the so-called “neutrality of the web.” Not only authoritarian countries determine what people can see and do in digital environments through the monitoring and filtering of e-traffic, creation of firewalls, denials of service, and so forth. What is more, design policies of western countries may involve risks of paternalistic approaches.

Scholars and privacy authorities [1,18,19,23] have thus proposed to forestall such scenarios, by strengthening data protection safeguards and empowering users through the implementation of appropriate measures in technological artifacts. The general idea is to develop expert systems that process and control personal data in compliance with regulatory frameworks, thereby letting company officers and citizens take security measures by themselves.

Yet, embedding data protection safeguards in ICT, video surveillance systems, bio-metric identifiers and the like, might end up in a vicious circle. There is, in fact, evidence that “some technical artifacts bear directly and systematically on the realization, or suppression, of particular configurations of social, ethical, and political values” [26]. This means that specific design choices may result in conflicts between values and, *vice versa*, conflicts between values may impact on the features of design. Would the idea of embedding regulatory measures in ICT replicate the same divergences we find in today’s debate on data protection? Conversely, can the principle of “privacy by design” offer solutions to the current balkanization of the internet?

In order to address these issues, the paper is organized in three sections. First, I examine the legal features of data protection in the light of current AI research in privacy by design. Special attention is paid to efforts in “legal ontologies” and the aim to model highly context-dependent normative concepts like personal data, security measures, and data controllers.

Second, I stress the ethical issues of design. By embedding data protection safeguards in ICT, we necessarily deal with values and interpretations thereof that may affect design features. Likewise, the modalities of design look problematic, for they cannot only limit the impact of harm-generating conducts but also prevent social behavior from occurring through the use of self enforcement technologies.

Third, and finally, I propose a stricter, yet more effective version of “privacy by design.” We may claim that “privacy assurance must ideally become an organization’s default mode of operation” [1], if, and only if, in accordance with current work in informational privacy [27], contextual integrity [28], and online policies [29], privacy by design is devoted to strengthen the autonomy of the individuals, letting people determine levels of access and control over personal data in digital environments.

## 2. The Design of Legal Frameworks

More than a decade ago, in *Code and Other Laws of Cyberspace*, Lawrence Lessig lamented the lack of research involving the impact of design on both social relationships and the functioning of legal systems [30].

In a few years, nevertheless, this gap has begun to be filled by work on privacy [31], universal usability [32], informed consent [33], crime control [34,35], social justice [36], self-enforcement technologies [37], and more. Not surprisingly, today there is a variety of design approaches to data protection [6-17]: design may shape places or products, spaces or processes, to decrease the impact of harm-generating conducts or, alternatively, to encourage the change of social behavior.

In the following section, I illustrate some concrete examples of privacy by design, in order to cast light on the regulatory effects of technology.

Then, I provide some technicalities of “legal ontologies”: This stricter perspective allows me to insist on the ethical stakes of embedding data protection safeguards in technological artifacts.

### 2.1. Spaces, Products and Messages

The concept of design can be understood as the act of working out the shape of objects: we actually mould the form of products and processes, together with the structure of spaces and places, so as to comply with regulatory frameworks. Such a shaping is not necessarily digital [30]. Consider, for example, the installation of speed bumps in roads as a means to reduce the velocity of cars (lest drivers opt to destroy their own vehicles). Still, the ICT revolution has obliged us to forge more sophisticated ways of legal enforcement: In the case of data protection, design should in fact aim to ensure the minimization and quality of the data, its controllability, transparency, confidentiality, down to the user friendliness of information interfaces [19]. According to the phrasing of Norman Potter in his 1968 book on *What Is a Designer* [38], we achieve these goals by designing spaces (environmental design), objects (product design), or messages (communication design).

As an illustration of the first kind of design, consider the case of people’s anonymity and the issue to protect people’s privacy in public [39]. 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 [19].

Moreover, when making personal data anonymous is considered a priority, matters of design also involve how we organize data processes and products. A typical instance is given by the processing of patient names in hospitals via information systems: here, 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” [19].

Besides environmental design (e.g., privacy friendly CCTV systems), and product design (e.g., smart cards), an example of communication design is given by public complaints against Facebook’s data protection policies and the services of Google Buzz. On May 26, 2010, Facebook announced to have “drastically simplified and improved its privacy controls” which previously amounted to 170 different options under 50 data protection-related settings. The default configuration of the system has therefore been set to record only the name, profile, gender and networks of the user,

while “friends” are no longer automatically included in the flow of information and platform applications, such as games, widgets, and the like, can finally be turned off by their *aficionados*.

However, in order to grasp the ethical stakes of embedding data protection safeguards in technology, Potter’s seminal distinction between environment, products and messages should be improved. In the next section, we will accordingly examine a further distinction between subjects (*i.e.*, places, products, organisms) and goals of design, the aim being to pinpoint the ways design mechanisms may encourage behavioral change and reduce or prevent harm-generating conducts [40].

In any event, the examples on video surveillance transport networks, information systems in hospitals, and smart cards for biometric identifiers make clear how to materialize the idea of embedding privacy safeguards in technological artifacts. Let us now consider some technical features of the principle via the approach of “legal ontologies.”

## 2.2. Legal Ontologies

Legal ontologies model concepts traditionally employed by lawyers through the formalization of norms, rights, and duties, in fields like criminal law, administrative law, civil law, *etc.* [22]. 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.

An interesting example of the approach is offered by 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 so as to provide organizations and citizens “with better guarantees of proper access, storage, management and sharing of files” [41]. By programming the software of the system to comply with regulatory frameworks of data protection, a further aim is to help company officers and citizens “who may have little or no legal knowledge whatsoever.”

Still, it could be argued that data protection regulations include more than “top normative concepts” such as notions of validity, obligation or prohibition. These rules present highly context-dependent normative concepts like personal data, security measures, or data controllers. Significantly, in the document on “The Future of Privacy” [19], the European authorities on data protection warn that “Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects.” Later, in the Opinion from the February 1, 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). In a similar way, on March 23, 2010, the European Court of Justice has 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 vs. Louis Vuitton case*, § 114 of the decision).

The difficulty of reducing the informational complexity of legal systems, where concepts and relations are subject to contextualization and evolution, has suggested several projects of legal ontologies to adopt a bottom-up rather than a top-down approach, *i.e.*, “starting from smaller parts and sub-solutions to end up with global” answers [41]. By splitting the work into several tasks and assigning each to a working team, the evaluation phase consists in testing the internal consistency of the project and, according to Herbert Simon’s “generator test-cycle,” involves 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” [42].

Further criteria and empirical methods have been proposed: Apart from functional efficiency, we should pay attention to the robustness, reliability, and usability of design projects. Evaluation and verification of the projects 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 [26]. Far from achieving any value-free judgment, the idea is to develop expert systems and friendly interfaces that strengthen the individual right to data protection.

After all, work in legal ontologies allows us to quantify the growing amount of personal data processed in compliance with legal frameworks: This is what occurs with research in the management of information systems [8,41], support of privacy preservation in location-based services [9], or middleware architectures for data protection [10], each of which aims at integrating smaller parts and sub-solutions of the design project. Interestingly, there are cases where the conceptualization of classes, relations, properties, and instances pertaining to a given problem domain, does not seem particularly complex, *e.g.*, the design of information systems for hospitals to ensure that patient names are kept separated from data on medical treatments or health status. Therefore, as scholars properly distinguish “central” from “peripheral” uses of technological artifacts and their design [43], lawyers should go on differentiating between “clear” and “hard cases” [44], insofar as it is feasible to program expert systems that lawfully process growing amounts of personal data, notwithstanding the highly context-dependent nature of the concepts involved.

However, the design of data protection safeguards does not concern only the formalization of the concepts traditionally employed by lawyers. As it occurs with other design approaches to data protection as value sensitive-perspectives [6,7], PeCAN platforms [14,15], and network theory [16,17], research on legal ontologies and AI and Law should take into account the role of ethical decisions in the evaluation phase of design projects, *e.g.*, levels of access and control over personal data [26,29], modulating the “ontological friction” of the informational environment [27].

Ultimately, privacy implies a sort of legal mediation between opposing interests [25], a matter of “trade-offs and balance” [28], of “balanced property rights” [45], and “contextual integrity” [46,47]. This is why scholars often debate on privacy *and* national security, privacy *and* copyright, privacy *and* freedom of speech, and so forth, so that research in privacy by design ought to examine what the

jargon of legal theory defines as a *relative* human right, *not* an *absolute* human right as, say, in the case of ban on torture [48].

In order to broaden the picture and complete the presentation on current efforts in the field of data protection, the next section focuses on the constraints of designing privacy safeguards ethically.

### 3. Three Issues of Design Ethics

Following research on the ethics of design [2-4], and privacy [5], a number of recent publications have dealt with the ethical issues involved in the design of expert systems, friendly interfaces, middleware architectures and the like. Let me sum up these problems, according to three perspectives [26,40,49].

First, I examine ethical issues of privacy by design entwined with “values” and their interpretation [26].

Then, ethical problems of privacy by design will concern its goals or “modalities” [40].

Finally, matters of design ethics are presented in terms of “responsibility” [49].

The aim of the section is to illustrate what is the ethical stake of embedding data protection safeguards in technological artifacts. As in Plato’s early dialogues, questions are piled up and no answers will be given: a normative approach is offered only in the final section of the paper.

#### 3.1. Values

Flanagan, Howe and Nissenbaum have recently insisted on the mutual interaction between values and technology: value concepts influence possible developments of technology, as technology reshapes these values and their environmental framework [26].

In the first case, conflicting values and interpretations thereof may impact on the very design of an artifact, according to what people find good or valuable. Consider, for example, 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 controllability over digital information. At the end of the day, should an artifact be designed in accordance with the standard European opt-in model for users of electronic communication systems or, *vice versa*, according to the American opt-out approach?

Furthermore, criteria such as minimization and quality of the data, together with its controllability, transparency, and confidentiality, might clash. Going back to the information systems in 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?

In sum, by striking a balance between different goals design can aim at, multiple choices of design may result in further conflicts of values. As work on self-enforcement technologies shows [37,40], people’s behavior can unilaterally be determined on the basis of automatic techniques that bypass their choices. Hence, by adopting a specific choice of design in a given artifact, people would be adapting to a specific value, e.g., the opt-in *vs.* opt-out diatribe. As a result, is the principle of “privacy by design” replicating the divergences we may find in today’s debate among lawyers and policy makers? Was not

the principle intended to overcome possible conflicts between values by embedding data protection safeguards in ICT and other types of technology?

### 3.2. Goals

Karen Yeung has proposed to approach the set of ethical issues raised by design, distinguishing between the subjects in which design is embedded and the underlying design mechanisms or “modalities of design” [40]. On one side, we can design not only places and spaces, products and processes, but biological organisms as well. This latter case concerns plants grown through OGM technology, genetically modified animals like Norwegian salmons, down to the current debate on human, post-humans, and cyborgs [50]. On the other side, the modalities of design may aim to encourage the change of social behavior, to decrease the impact of harm-generating conducts, or to prevent that those harm-generating conducts may even occur. As an illustration of the first kind of design mechanisms, consider the installation of speed bumps in roads as a means to reduce the velocity of cars. As an example of the second modality of design, think about the introduction of air-bags to reduce the impact of harm-generating conducts. Finally, as an instance of total prevention, it is enough to mention current projects on “smart cars” able to stop or to limit their own speed according to the driver’s health conditions and the inputs of the surrounding environment.

So, if we go back to the principle of privacy by design, we can ask what policy are we pursuing? Is the goal of the project to change social behavior, or to decrease the impact of harm-generating conducts? And, how about conceiving design as a means for total prevention? Could it constitute an infallible self-enforcement mechanism preventing privacy infringements overall?

### 3.3. Responsibilities

Grodzinsky, Miller and Wolf have insisted on a further set of ethical issues involved in the design of places, products and processes, down to the design of artificial agents [49]. In particular, what is ethically problematic is the responsibility of computer scientists and designers, as also the distinction between “strong” and “weak” forms of moral responsibility, when programming an artificial agent like Robbie CX30 in Richard Epstein’s story on *The Case of the Killer Robot* [51].

This is indeed an interesting case so as to tell “weak” from “strong” forms of moral responsibility, because the robot would respond to stimuli by changing the values of its inner states and, what is more, it would be able both to modify these states without external stimuli and to improve the rules through which those very states change. In a nutshell, we are considering the responsibility of a designer who is creating a *proper* artificial agent, *i.e.*, a subject that is interactive, autonomous and adaptable [52,53].

In general terms, people are responsible for what they voluntarily agree upon, *e.g.*, through strict contractual obligations. In addition, obligations can be imposed by the government to compensate damage done by wrongdoing: while there is responsibility for intentional torts when the individual has voluntarily performed a wrongful action, people are responsible for lack of due care when they fail to guard against foreseeable harm. This is the kind of responsibility particularly relevant in this context, in that even the best-intentioned and best-informed designer cannot foresee all the possible outcomes of the artifacts and unintended consequences. (By the way, this is the reason why you have seen those

extremely detailed and sometimes strange labels on products, by which manufacturers warn about risks or dangers involving the improper use of the artifact.) So, without making the legal and moral aspects of the problem overlap, should we hold designers responsible for the unintended or unforeseeable consequences of their projects? Should we prohibit some kinds of design? Conversely, would it be legitimate to strike a balance between cases of “strong moral responsibility” and methods of compensation or of compulsory assurance? Does this alternative represent a new chapter in the clash between openness and the principle of precaution?

#### **4. A Normative Approach to Design**

The aim of this section is to determine to what extent matters of values, goals and responsibility make the principle of privacy by design fruitful in today’s data protection. The analysis is organized in the light of four points.

First, issues of design ethics are considered in connection with the notion of responsibility and the hypothesis to prohibit some sort of design due to the strong moral responsibility involved in the project. A normative approach will draw from current work on macro ethics [27].

Next, I analyze modalities and objects of design projects to find out whether some of them should be prohibited or, alternatively, considered unworkable. The macro ethics viewpoint is integrated with research in contextual integrity [28] and informational privacy [29].

Then, I take into account conflicts of values that divide designers as well as policy makers. As Jeffrey Rosen has declared in March 2008, the fear is that “cultural differences will make thoughtful regulation difficult” in data protection: after all, in the words of the law professor, “the French will bare their breasts but not their salaries and mortgages, and the reverse is true in the U.S.” [54].

The conclusion suggests a stricter version of “privacy by design” in order to find out a viable solution to most of the relevant issues involving responsibility, goals and values of design.

##### *4.1. Precaution*

A traditional way to deal with the problem of responsible design is to apply the principle of precaution. Although different formulations have been given, the overall idea is clear: when science is not confident about whether or not a certain technology poses a threat, we should refrain from action. The burden of proof falls in other words on those who support the opinion of taking action, whereas past experiences would have taught how to take precautions in the event of evidence on “false-negative” risks while acting against “false-positive” ones.

In informational terms [27], the principle of precaution could be reformulated as follows: every attempt to adapt may reduce the complexity of the environment while enriching its informational nature, but highly sensitive issues as public health or food safety suggest that the burden of proof should fall on those who advocate taking action. The reason hinges on the strict link between the informational reduction of those attempts to adapt and their direct consequences or impact on the environment as a whole.

However, burden of proof varies according to the field and there are many cases in which the precautionary principle is arguably inadequate for coping with the unknown consequences of technology. Simply consider the web and the internet, both designed to be unpredictable or “out of

control” [55], and nonetheless leading “to an explosion of offerings that might never have evolved had central control of the network been required by design” [56]. Consequently, we should act, and not refrain from acting, when it is likely that the evolutionary attempt to reduce the complexity of the environment increases the wealth of the “infosphere” [57]. This is to say with regard to the principles of information ethics, that we should pay attention to the “entropy” of the infosphere so as to determine when the principle of precaution may prevail in the name of “flourishing of informational entities” [57,58].

On this basis, bans of design are legitimate if, and only if, evidence shows that their outcomes lead to the impoverishment of the environment. This is, for instance, the U.S. Supreme Court’s golden rule in most technological cases, such as the Betamax case in the mid 1980s, or on P2P file sharing applications-systems in the early 2000s. Likewise, the information perspective allows us to determine the legitimacy of design mechanisms or modalities of privacy by design, by looking at the impact on the individual flourishing [27]. But, how about Grodzinsky, Miller and Wolf’s standpoint [49], that designers retain “strong moral responsibility” for the unpredictable behavior of their artificial agents? Does the principle of privacy by design necessarily entail matters of “strong moral responsibility”? Does the thesis mean we should avert the design of both autonomous artifacts like smart robots and smart environments for the protection of people’s privacy?

In order to determine the moral responsibility of design projects in a precautionary way, I suggest both objects and modalities of design be considered [40]. In AI design of artificial agents and, more specifically, of autonomous robots, for example, is indispensable to discern humanoids, adaptive robot servants, robot soldiers, robot toys and even robot nannies, each of which has its own benefits and drawbacks. Accordingly, we should distinguish between the “weak moral responsibility” of designing robots that decrease the impact of harm-generating behavior, e.g., eco-robotics for cleaning the environment, and the “strong moral responsibility” of designing robot soldiers deployed in the battlefield [53]. Whereas the distinction hinges on how design may impact the “flourishing of informational entities” [57,58], it also defines limits to the principle of precaution. Let me explain how this demarcation works in the realm of data protection.

#### 4.2. Fairness

Karen Yeung’s taxonomy [40] proposes nine possible combinations between subjects of design (*i.e.*, places, products, organisms) and its modalities (*i.e.*, behavioral change and reduction or prevention of harm-generating conducts). What are the relevant scenarios in the field of privacy and design? Leaving aside cases of genetically modified salmon and of OGM plants, what about the most interesting hypotheses for data protection?

Regarding the *objects of design*, my view is that we should go on focusing on spaces and products, rather than organisms and other human fellows. To the best of my knowledge, ethical and legal issues of human design involve contemporary debate on bioethics, cyborgs and robotics, rather than data protection safeguards through design policies (as the eye bulbs Tom Cruise acquires in the popular motion picture *Minority Report*). Thus, dealing with places, artifacts or processes, it is necessary to analytically distinguish the *modalities of design*, namely, between the aim to encourage the

change of people's behavior and the goal to decrease and even to prevent the impact of harm-generating conducts.

In the first scenario, design can induce the change of people's behavior via friendly interfaces [8,41], location-based services [9], and the like. An interesting case is offered by the free-riding phenomenon of P2P networks, where most peers tend to use these systems to find information and download their favorite files without contributing to the performance of the system [59]. Whilst this selfish behavior 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 both on trust (e.g., reputation mechanisms), and trade (e.g., services in return). This latter scheme implies a sort of digital barter, as in the 'tit-for-tat' model of Bit Torrent or the credit system of Emule, along with bond schemes that involve forms of digital money like Kazaa's "Alnet's points". The idea is that "the receiver can recompense the provider immediately, during or after the service provision, or she can promise a service in return" [60].

These examples of design mechanisms are relevant because encouraging people to change behavior prevents risks of paternalism, by widening the range of choices and options. Compared to the "strong moral responsibilities" examined in the previous paragraph [49], it is therefore arguable that design responsibility should be grasped as "weak" in this case.

Moreover, design mechanisms may aim to decrease the impact of harm-generating behavior rather than changing people's conduct. This aim of design is well represented by efforts in security measures [61]. As with friendly interfaces, location-based services and so forth, responsibility for this kind of design mechanism should be deemed "weak", insofar as the goal of design is by definition to prevent the impoverishment of the infosphere [57].

In order to prevent misunderstandings, I do not claim that this "weak" form of moral responsibility does not involve a "strong" responsibility of the designer when considered from a further viewpoint: for instance, design projects in security measures often raise this kind of "strong moral responsibility" once you are interested in establishing their reliability, e.g., security measures in the informative system of an atomic plant. In the context of this paper, however, the issue consists in determining neither the technical meticulousness of the project nor the impact of technical inaccuracies on individual well-being. Rather, the focus is on the moral responsibility that hinges on the aim of the project, *i.e.*, encouraging the change of people's behavior or, alternatively, decreasing the effects of harm-generating conducts.

But, how about conceiving a design as a means of total prevention? Could it be an infallible self-enforcement technology preventing harm-generating conducts overall?

In the terms of Grodzinsky, Miller and Wolf's analysis [49], there are three reasons why moral and political responsibility turns out to be so "strong" that this type of design mechanism should not be applied to the field of privacy by design.

First, privacy is hardly a zero-sum game between multiple instances of access, control, and protection over information in digital environments. In fact, personal choices play the main role when individuals modulate different levels of access and control, depending on the context and its circumstances [28]. All in all, 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 guaranteed privacy [29].

Secondly, the use of self-enforcement technologies raises further ethical issues, since people's behavior would unilaterally be determined on the basis of automatic techniques rather than by individual and collective choices. A kind of infallible self-enforcement technology not only "collapses the public understanding of law with its application, eliminating a useful interface between the law's terms and its application" [37]. What is more, there are instances of self-enforcement technology, e.g., Digital Rights Management (DRM), that enable copyright holders to monitor and regulate the use of their protected artifacts, thus impinging on people's privacy in another way.

Finally, attention should be drawn to the technical difficulties of design, when modeling concepts traditionally employed by lawyers, through the formalization of norms, rights, or duties, so as to fit the processing of a machine. As shown by work on AI, legal ontologies and privacy by design, serious difficulties arise when reducing the informational complexity of a system, where concepts and relations are subject to contextualization and evolution. Arguably, "a rich body of scholarship concerning the theory and practice of 'traditional' rule-based regulation bears witness to the impossibility of designing regulatory standards in the form of legal rules that will hit their target with perfect accuracy" [40]. In the phrasing of Eugene Spafford, it would be important to understand 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" [62].

#### 4.3. Goodness

In their work on "embodying values in technology" [26], Flanagan, Howe and Nissenbaum have properly stressed that objects and mechanisms of design are necessarily entwined with values. Leaving aside hypotheses of data protection via human engineering or infallible self-enforcement technologies, values are critical when embedding data protection safeguards in places, products and processes. Although it is notoriously difficult to solve conflicts of values with their divergent interpretations, this work [26] shows how we can tackle such a variety of contrasting values in the field of privacy by design.

On one hand, legal systems help us to overcome a relevant number of issues: "In the case of privacy, for example, the designers might not be free to embody their preferred conception of privacy, but need to take into consideration the sometimes detailed guidance of legal doctrine or explicit regulation" [26]. Consider the limits of designing systems in the field of health-related information, which must comply with the regulation governing that flow of information pursuant to the U.S. HIPAA, *i.e.*, the Health Insurance Portability and Accountability Act from 1996. Likewise, think of the issues involving the use and development of P2P systems, where the impact of legal and political decisions on the design of technology is particularly relevant [24,25]. Regardless of legal "hard cases," the variety of contrasting values among stakeholders or scholars is often mitigated by the intervention of the law [26].

On the other hand, different interpretations of artifacts that embody values are counter-balanced by empirical methods of evaluation and verification of the project, which include its "operationalization," that is, the analysis and definition of the value concepts involved [26]. As in the case of privacy by design through the expertise of legal ontologies [8-10,41], we can employ several methods like Simon's "generator test-cycle" [42], use of prototypes, automated and regression-oriented tests, or

users tests in controlled environments. These methods allow us to understand how design projects embed values in artifacts, because “verifying the inclusion of values is likely to draw on strategies and methods not unlike those applied to other design criteria like functional efficiency and usability” [26].

However, it may be argued that the intervention of the law, as well as the use of methods of empirical evaluation and verification of design projects, do not really solve our problem, since some legal rules may simply be “bad.” In connection with current efforts in macro ethics [27,57], contextual integrity [28] and informational privacy [29], it follows that we should test the viability of data protection laws in order to prove the worthiness of our design projects. In fact, would all the provisions of, say, the Health Insurance Portability and Accountability Act be uncontroversial?

Luckily enough, focusing on the ethical constraints of privacy by design, we do not have to exhaustively assess legal provisions on data protection *per se*. As said matters of design responsibility suggest that, most of the time, encouraging people to change their behavior and decreasing the impact of harm-generating conducts rely on forms of “weak moral responsibility.”

However, there are exceptions: privacy by design entails cases of strong (legal, political and moral) responsibility when they involve individual autonomy, *i.e.*, literally, a person’s Kantian property to rule (*nomos*) over herself (*auto*).

#### 4.4. Autonomy

There is a remarkable convergence between current work on informational privacy and recent declarations of the European commissioners on data protection. As the EU WP29 affirms in the document on “The Future of Privacy” [19], design should aim to broaden individual options by letting people opt for security measures by themselves. This goal fits like hand in glove with research on contextual integrity and flourishing ethics [28,57,58], for the aim is to balance restricted access and limited control over personal data in digital environments [29,45,46]. More particularly, we may rightly claim that “privacy assurance must ideally become an organization’s default mode of operation” [1,18], if, and only if, privacy by design is devoted to strengthen people’s autonomy by widening their range of choices. This stricter version of the principle prevents two risks related to the “strong moral responsibilities” of privacy by design.

On one hand, issues of data protection should be grasped “by” design, not “as” design, that is, as if the goal were to reverse the idea that technology has decreed “The End of Privacy” [63], “The Death of Privacy in the 21st Century” [64], or “Privacy Lost” [65]. What is at stake, in fact, is not to prevent privacy infringement through an allegedly infallible self-enforcement technology: Such a goal is neither desirable nor achievable, for both ethical and technical reasons. Rather, we should conceive “privacy by design” as a means to decrease the effects of harm-generating conducts (e.g., security measures), or, alternatively, to encourage the change of people’s behavior (e.g., friendly interfaces).

On the other hand, this stricter version of the principle averts paternalism, namely, the idea of protecting citizens against themselves [66]. Not only the editorials in *The Economist*, but also scholarly criticisms of the European data protection policies often stress this threat [67]. According to Richard Volkman, for example, the European legal framework “is clearly and deeply flawed as an account of what informational protection is all about” in that “restrictions are so sweeping that many perfectly legitimate business models are *de facto* outlawed by such a law” [68].

It is unwarranted to sympathize with Brussels, however, to follow the EU Working Party's proposal that the principle of privacy by design should be implemented in accordance with a bottom-up rather than a top-down approach: it shall depend on the autonomous choices of individuals via self-regulation and competition among private organizations [19]. Whilst the goal of ensuring compliance with regulatory frameworks through data protection safeguards in ICT may end up in modeling of individual behavior, a normative approach suggests how to prevent this threat. The overall goal of privacy by design should be reinforcing people's pre-existing autonomy, rather than building it from scratch: On this basis, dealing with values, responsibility, and modalities of design, we achieve three results.

First, compliance with regulatory frameworks suggests that, most of the time, design projects will regard cases of "weak" (not "strong") moral responsibility in data protection [49]. Leaving aside the technical accuracy of the projects, design should aim to increase individual options or decrease the effects of harm-generating conducts.

Secondly, observation of the detailed guidance and explicit regulation of privacy authorities [26] prevents multiplying conflicts of values with their divergent interpretations through privacy by design-policies. Generally, the aim will be to ensure by design the minimization and quality of the data, its controllability, transparency, and confidentiality, down to the user friendliness of information interfaces [19].

Finally, by restricting the modalities and goals of design in the field of data protection, e.g., by excluding to design allegedly infallible self-enforcement technologies, we defend individual autonomy against paternalism. At the end of the day, the supposedly perfect automation of data protection mechanisms would by default impose norms on individuals, who have no say in the decisions affecting them (hence, jeopardizing the democratic rule of law).

## 5. Conclusions

The paper has focused on today's research on the principle of "privacy by design", and the efforts to solve some of the problems raised by the use of generative technologies and the current balkanization of the internet. More particularly, we have seen that the general idea is to handle most of today's issues in data protection, by embedding privacy safeguards in ICT and other types of technology. According to Ann Cavoukian, this approach can be summed up in seven principles [18]:

- (i) We have to view data protection in *proactive* rather than reactive terms, making privacy by design *preventive* and not simply remedial;
- (ii) Personal data should be *automatically* protected in every IT system as its *default* position;
- (iii) Data protection should accordingly be *embedded into design*;
- (iv) The *full functionality* of the principle which follows from ii) and iii), allows a "positive-sum" or "win-win" game, making trade-offs unnecessary (e.g., privacy *vs.* security);
- (v) 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;
- (vi) 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;

(vii) 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” [18]. In other words, privacy by design requires an individual-focused *respect for user privacy*.

In light of this framework [69,70], we have seen how relevant the principle of privacy by design is in such different fields like the “future of the internet” [23], data protection via CCTV systems, biometrics, social networks, smart environments, data loss prevention, and more.

However, the paper also stressed two critical issues of the principle, mainly involving points (ii) and (v) of Cavoukian’s scheme, so as to shed light on its conclusive point (vii), which is in regard to the autonomy of individuals.

First, there is the problem of making all the legal provisions on data protection automatic. As shown by ten 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” [15]. Far from being mere subtleties, however, the first section of this paper showed that such legal hurdles to the “end-to-end lifecycle” of data protection, involve some of the most important notions of the legal framework, *i.e.*, 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 allegedly 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 behavior would unilaterally be determined on the basis of automatic techniques rather than by choices of the relevant political institutions. This is why, in the name of individual autonomy, I proposed to frame the ethical issues of design and its modalities (second section of the paper) by adopting a stricter version of the principle (third section of this article).

In sum, privacy by design should encourage people to change their behavior (e.g., user-friendly interfaces), or limit the consequences of harmful behavior (e.g., security measures), by strengthening individual rights and broadening the range of choices available to people. As a result, we do show “respect for user privacy,” yet we avert 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 ensure and reinforce the pre-existing autonomy of individuals.

## References

1. Cavoukian, A. *Privacy by Design*; IPC Publications: Ontario, Canada, 2009; p. 8.
2. Friedman, B. Value-sensitive design. *Interactions* **1986**, *3*, 17-23.
3. Mitcham, C. Ethics into design. In *Discovering Design*; Buchanan, R., Margolis, V., Eds.; University of Chicago Press: Chicago, IL, USA, 1995; pp. 173-179.
4. Whitbeck, C. Ethics as design: Doing justice to moral problems. *Hastings Cent. Rep.* **1996**, *26*, 9-16.
5. Agre, P.E. Introduction. In *Technology and Privacy: The New Landscape*; Agre, P.E., Rotenberg, M., Eds.; The MIT Press: California, CA, USA, 1997; pp. 1-28.

6. Friedman, B.; Kahn, P.H., Jr. Human values, ethics, and design. In *The Human-Computer Interaction Handbook*; Jacko, J., Sears, A., Eds.; Lawrence Erlbaum Associates: Mahwah, NJ, USA, 2003; pp. 1177-1201.
7. Friedman, B.; Kahn, P.H., Jr.; Borning, A. Value sensitive design and information systems. In *Human-Computer Interaction in Management Information Systems: Foundations*; Zhang, P., Galletta, D., Eds.; Armonk: New York, NY, USA, 2006; pp. 348-372.
8. Abou-Tair, D.; Berlik, S. *An Ontology-based Approach for Managing and Maintaining Privacy in Information Systems*; Springer: Berlin, Germany, 2006; pp. 983-994.
9. Mitre, H.; González-Tablas, A.; Ramos, B.; Ribagorda, A. *A Legal Ontology to Support Privacy Preservation in Location-Based Services*; Springer: Berlin, Germany, 2006; pp. 1755-1764.
10. Lioukadis, G.; Lioudakisa, G.; Koutsoloukasa, E.; Tselikasa, N.; Kapellakia, S.; Prezerakosa, G.; Kaklamania, D.; Venierisa, I. A middleware architecture for privacy protection. *Comput. Netw.* **2007**, *5*, 4679-4696.
11. Jutla, D.N.; Zhang, Y. Maturing e-privacy with P3P and context agents. In *Proceedings of IEEE International Conference on E-Technology, E-Commerce and E-Service*; Hong Kong, China, 2005; pp. 536-541.
12. Cranor, L.F.; Egelman, S.; Sheng, S.; McDonald, A.M.; Chowdhury, A. P3P deployment on websites. *Electron. Commer. R. A.* **2008**, *7*, 274-293.
13. Reay, I.; Dick, S.; Miller, J. A large-scale empirical study on P3P privacy policies: Stated actions vs. legal obligations. *ACM Trans. Web* **2009**, *3*, 1-34.
14. Jutla, D.N.; Bodorik, P.; Zhang, Y. PeCAN: An architecture for user privacy and profiles in electronic commerce contexts on the semantic web. *Inform. Syst.* **2006**, *31*, 295-320.
15. Jutla, D.N. Layering privacy on operating systems, social networks, and other platforms by design. *Identity Inform. Soc.* **2010**, *3*, 319-341.
16. Pagallo, U. "Small world" paradigm and empirical research in legal ontologies: A topological approach. In *The Multilanguage Complexity of European Law: Methodologies in Comparison*; Ajani, G., Peruginelli, G., Sartor, G., Tiscornia, D., Eds.; European Press Academic Publishing: Florence, Italy, 2007; pp. 195-210.
17. Pagallo, U. As law goes by: Topology, ontology, evolution. In *AI Approaches to the Complexity of Legal Systems*; Casanovas, P., Ed.; Springer: Berlin, Germany, 2010; pp. 12-26.
18. Cavoukian, A. Privacy by design: The definitive workshop. *Identity Inform. Soc.* **2010**, *3*, 247-251.
19. EU Working Party Art. 29 D-95/46/EC. The Future of Privacy. *Article 29 Working Party and the Working Party on Police and Justice, 02356/09/EN—WP 168*, December 1st 2009. Available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf) (accessed on 29 March 2011).
20. Kim, A.; Joffman, L.J.; Martin C.D. Building privacy into the semantic web: Ontology needed now *Proceedings of the WWW2002 International Workshop on the Semantic Web*; Hawaii, HI, USA, 2002.
21. Jutla, D.N.; Xu, L. Privacy agents and ontology for the semantic web. In *Americas Conference on Information Systems*, New York, NY, USA, 2004.

22. Breuker, J.; Casanovas, P.; Klein, M.; Francesconi, E. *Law, Ontologies and the Semantic Web*; Ios Press: Amsterdam, The Netherlands, 2009.
23. Zittrain, J. *The Future of the Internet and How to Stop It*; Yale University Press: New Haven, CT, USA, 2008.
24. Pagallo, U. Ethics among peers: File sharing on the internet between openness and precaution. *J. Inform. Comm. Ethics Soc.* **2010**, *8*, 136-149.
25. Pagallo, U.; Durante, M. Three roads to P2P systems and their impact on business ethics. *Bus. Ethics* **2010**, *90*, 551-564.
26. Flanagan, M.; Howe, D.C.; Nissenbaum, M. Embodying values in technology: Theory and practice. In *Information Technology and Moral Philosophy*; van den Hoven, J., Weckert, J., Eds.; Cambridge University Press: Cambridge, UK, 2008, pp. 347-348.
27. Floridi, L. Four challenges for a theory of informational privacy. *Ethics Inform. Tech.* **2006**, *8*, 109-119.
28. Nissenbaum, H. Privacy as contextual integrity. *Wash. Law Rev.* **2004**, *79*, 119-158.
29. Tavani, H.T. Philosophical theories of privacy: implications for an adequate online privacy policy. *Metaphilosophy* **2007**, *38*, 1-22.
30. Lessig, L. *Code and Other Laws of Cyberspace*; Basic Books: New York, NY, USA, 1999.
31. Ackerman, M.S.; Cranor, L. Privacy critics: UI components to safeguard users' privacy. Extended Abstracts of CHI; ACM Press: New York, NY, USA, 1999, pp. 258-259.
32. Shneiderman, N. Universal usability. *Commun. ACM* **2000**, *43*, 84-91.
33. Friedman, B.; Howe, D.C.; Felten, E. Informed consent in the Mozilla browser: Implementing value-sensitive design. In *Proceedings of 35th Annual Hawaii International Conference on System Sciences*; IEEE Computer Society: Washington, DC, USA, 2002; p. 247.
34. Katyal, N. Architecture as crime control. *Yale Law J.* **2002**, *111*, 1039-1139.
35. Katyal, N. Digital architecture as crime control. *Yale Law J.* **2003**, *112*, 101-129.
36. Borning A.; Friedman, B; Kahn, P. Designing for human values in an urban simulation system: value sensitive design and participatory design. *Proceedings of Eighth Biennial Participatory Design Conference*; ACM Press: Toronto, Canada, 2004; pp. 64-67.
37. Zittrain, J. Perfect enforcement on tomorrow's internet. In *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*; Brownsword, R., Yeung, K., Eds.; Hart Publishing: London, UK, 2007; pp. 125-156.
38. Potter, N. *What Is a Designer*; Hyphen Press: London, UK, 2002.
39. Nissenbaum, H. Protecting privacy in an information age: The problem of privacy in Public. *Law Philos.* **1998**, *17*, 559-596.
40. Yeung, K. Towards an understanding of regulation by design. In *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*; Brownsword, R., Yeung, K., Eds.; Hart Publishing: London, UK, 2007; pp. 79-108.
41. Casellas, N.; Torralba, S.; Nieto, J.E. The neurona ontology: A data protection compliance ontology. Paper presented at the Intelligent Privacy Management Symposium, 22-24 March 2010, Stanford University, Stanford, CA, USA, 2010.
42. Simon, H.A. *The Sciences of the Artificial*; The MIT Press: California, CA, USA, 1996.

43. Brey, P. Values in technology and disclosive computer ethics. *The Cambridge Handbook of Information and Computer Ethics*; Floridi, L., Ed.; Cambridge University Press: Cambridge, UK, 2010; pp. 41-58.
44. Hart, H. *The Concept of Law*; Clarendon Press: Oxford, UK, 1961.
45. Spinello, R.A. The future of intellectual property. *Ethics Inform. Tech.* **2003**, *5*, 1-16.
46. Nissenbaum, H. Privacy as contextual integrity. *Wash. Law Rev.* **2004**, *79*, 119-158.
47. Grodzinsky, F.S.; Tavani, H.T. Online file sharing: resolving the tensions between privacy and property interest. In *Proceedings of ETHICOMP2008 "Living, Working and Learning Beyond Technology"*; Bynum, T.W., Calzarossa, M., de Lotto, I., Rogerson, S., Eds.; Tipografia Commerciale: Mantova, Italy, 2008; pp. 373-383.
48. Clapham, A. A very short introduction. In *Human Rights*; Oxford University Press: Oxford, UK, 2007; pp. 108-118.
49. Grodzinsky, F.S.; Miller, K.A.; Wolf, M.J. The ethics of designing artificial agents. *Ethics Inform. Tech.* **2008**, *10*, 115-121.
50. Moor, J.H. Should we let computers get under our skin? In *The Impact of the Internet on Our Moral Lives*; Cavalier, R., Ed.; State of New York University Press: New York, NY, USA, 2005; pp. 121-139.
51. Epstein, R.G. *The Case of The Killer Robot*; Wiley: New York, NY, USA, 1997.
52. Floridi, L.; Sanders, J. On the morality of artificial agents. *Mind Mach.* **2004**, *14*, 349-379.
53. Pagallo, U. Robotrust and Legal Responsibility. *Knowl. Tech. Pol.* **2010**, *23*, 367-379.
54. Mills, E. *To Be Anonymous or Not to Be, That Is the Privacy Question*, News Blog, March 8, 2008, Available at [http://news.cnet.com/8301-10784\\_3-9889255-7.html](http://news.cnet.com/8301-10784_3-9889255-7.html) (accessed on 25 March 2011).
55. Berners-Lee, T. *Weaving the Web*; Harper: San Francisco, CA, USA, 1999.
56. Cerf, V. User-generated content is top threat to media and entertainment industry. Interview in *Accenture* on April 16th, 2007.
57. Floridi, L. Information ethics, its nature and scope. *Comput. Soc.* **2005**, *36*, 21-36.
58. Bynum, T.W. Flourishing ethics. *Ethics Inform. Tech.* **2006**, *8*, 157-173.
59. Adar, E.; Huberman, B.A. Free riding on gnutella. *First Monday* **2000**, *5*, Available at <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/792/701> (accessed on 27 March 2011).
60. Ruffo, G.; Schifanella, R. FairPeers: Efficient profit sharing in fair peer-to-peer market places. *J. Netw. Syst. Manag.* **2007**, *15*, 355-382.
61. von Ahn, L.; Maurer, B.; McMillen, C.; Abraham, D.; Blum, M. reCAPTCHA: Human-based character recognition via web security measures. *Science* **2008**, *321*, 1465-1468.
62. Garfinkel, S.; Spafford, G. *Web Security and Commerce*; O'Reilly: Sebastopol, CA, USA, 1997.
63. Sykes, C. The end of privacy. *The Attack on Personal Rights at Home, at Work, On-Line, and in Court*; St. Martin's Griffin: New York, NY, USA, 1999.
64. Garfinkel, S. *Database Nation. The Death of Privacy in the 21st Century*; O'Reilly: Sebastopol, CA, USA, 2000.
65. Holtzman, D.H. *Privacy Lost. How Technology Is Endangering Your Privacy*; Jossey-Bass: New York, NY, USA, 2006.

66. Kant, I. *Kant's Principles of Politics, Including His Essay on Perpetual Peace*; Hastie, W., Translator; Clark: Edinburgh, UK, 1891.
67. Kuner, Ch. *European Data Privacy Law and Online Business*; Oxford University Press: Oxford, UK, 2003.
68. Volkman, R. Privacy as life, liberty, property. *Ethics Inform. Tech.* **2003**, *5*, 199-210.
69. Schaar, P. Privacy by design. *Identity Inform. Soc.* **2010**, *32*, 267-274.
70. David, J.S.; Prosch, M. Extending the value chain to incorporate privacy by design principles. *Identity Inform. Soc.* **2010**, *3*, 295-318.

© 2011 by the author; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/>).