The Information Society, 30: 355–365, 2014
Published with license by Taylor & Francis
ISSN: 0197-2243 print / 1087-6537 online
DOI: 10.1080/01972243.2014.944730

Routledge
Taylor & Francis Group

PERSPECTIVE

A Strategy for Operationalizing Privacy by Design

Inga Kroener and David Wright

Trilateral Research and Consulting, London, United Kingdom

Recent controversies surrounding privacy have sparked a move by regulators toward the idea of privacy by design (PbD), a concept pioneered by Ontario Information and Privacy Commissioner Ann Cavoukian. Industry has also started to recognize the importance of taking privacy seriously, with various PbD corporate initiatives currently underway. However, some commentators have criticized PbD for being too vague. Using three case studies and a range of best practice examples of PbD, privacy impact assessments (PIAs), and privacy-enhancing technologies (PETs), this article addresses the gap between the abstract principles of PbD and their operationalization into more concrete implementation guidelines for software engineers.

Keywords privacy by design, privacy-enhancing technologies, privacy impact assessment

There has been increasing interest in the idea of designing privacy protections into technologies from the outset. Known as privacy by design (PbD), the concept was pioneered in Canada by Ann Cavoukian, Information and Privacy Commissioner for Ontario (Hustinx 2009). PbD is a proactive, rather than a reactive, approach to privacy protection that considers the privacy implications of new technologies during the design stage, rather than as an afterthought. PbD is not yet a part of legislation in any country, even though it is often cited as a best practice. Moreover, there are calls in the European Union (EU) and United States to include the PbD principle in legal frameworks. PbD is included as a principle under Article 23 of the proposed EU Data Protection Regulation and in the U.S. Commercial Privacy Bill of Rights Act. Also, the 32nd International Conference of Data Protection and Privacy Commissioners, held in Israel in 2010, unanimously accepted the concept of PbD as the "gold standard" in privacy protection.

Although there seems to be agreement internationally that PbD is an important element of protecting personal privacy, there are differences at the implementation level. We delve into these differences later in this article.

The first section concentrates on PbD, including an overview of its main principles, its acceptance and promotion as "best practice" by data protection regulators, and the main concerns of its critics. The second section focuses on issues of trust, accountability, and privacy, and the varying definitions of these terms. The next section outlines some elements of the PbD process, privacy impact assessments (PIAs), and privacy-enhancing technologies (PETs). The final section offers a set of guidelines for industry to implement during the life cycle of new technologies and systems. The annex includes a set of three case studies, to which we refer in the final section of this article, that spotlight the problems and issues currently faced by those trying to implement PbD.

A REGULATORY VIEW OF PbD

In recent years, privacy protections have been developed through state regulation or through industry self-regulation. State regulation has been criticized for being underfunded, not enforced, or enforced incorrectly. Industry self-regulation has been criticized for being inadequate for securing privacy. Spurred by these criticisms of state and industry regulation, PbD proponents seek to incorporate privacy protections into technological systems. On the one hand, regulators see in PbD an opportunity to strengthen privacy. On the other hand, industry has come to recognize PbD as a means to demonstrate that it takes privacy seriously (Guagnin et al. 2012).

One of the key thinkers behind the concept of PbD is Ann Cavoukian, Ontario Information and Privacy

Received 20 January 2014; accepted 25 June 2014
Address correspondence to Inga Kroener, Trilateral Research & Consulting, Crown House, 72 Hammersmith Road, London W14 8H, United Kingdom. E-mail: inga.kroener@trilateralresearch.com

Commissioner. She suggests that "the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation" Cavoukian 2009, 19). In line with the UK Information Commissioner's Office (ICO), Cavoukian argues that PbD needs to go beyond technology design to incorporate:

1. IT systems.
2. Accountable business practices.
3. Physical design and networked infrastructure.

A special issue of the journal *Identity in the Information Society* (2010), edited by Cavoukian, suggests that PbD initiatives need to be incorporated into the first stage of technology development, rather than added later as a patch (Schaar 2010). Contributors also argued that PbD could aid organizational accountability (Cavoukian, Taylor, and Abrams 2010) and enhance user trust in systems (Rooy and Bus 2010).

PbD got a major impetus in 2010 when the International Conference of Data Protection and Privacy Commissioners (ICDPPC), meeting in Jerusalem, adopted a resolution that emphasized the importance of PbD. The resolution recognized PbD as an essential component of fundamental privacy protection; encouraged the adoption of privacy by design to establish privacy as an organization's default mode of operation; and invited data protection and privacy commissioners to promote PbD in their jurisdictions. Some described the resolution as a "landmark" for PbD.

PbD also features in the proposed EU Data Protection Regulation, which, if adopted, will be directly applicable in the Member States. The Article 23 of the proposed regulation highlights the need for privacy protection to be part of the entire life cycle of a product.

PbD PRINCIPLES

Although the proposed regulation specifies a requirement for PbD, it does not go into any detail with regard to what it actually means. Cavoukian (2009), however, has specified seven principles for PbD, as follows:

1. Proactive not reactive; preventative not remedial action.
2. Privacy as the default setting.
3. Privacy embedded into design.
4. Positive-sum, not zero-sum, outcomes (i.e., no trade-off between different interests).
5. End-to-end security—ensuring full life-cycle protection.
6. A commitment to visibility and transparency.
7. Respect for user privacy—all developments need to remain user centered.

Recently Peter Schaar, the German Federal Commissioner for Data Protection and Freedom of Information until his retirement at the end of 2013, argued for six PbD principles that should be taken into account during the design stage of new technologies or systems that collect and process personal data: data minimization, controllability (consent and objection), transparency, data confidentiality, data quality, and segregation (e.g., in cloud computing). Drawing on, but also differing slightly from, Cavoukian's original seven principles, Schaar lays greater emphasis on the technological aspects and describes a more prescriptive process.

Furthermore, he moves away from the preoccupation with a "positive-sum" outcome for all parties involved. Rather than ensuring that neither the commercial nor privacy interests "lose," Schaar emphasizes the importance first and foremost of protecting the individual's right to privacy and complying with the data protection principles contained in the existing EU Data Protection Directive (95/46/EC). He strongly promotes a principle of data security, closely followed by a principle of data minimization. However, he also argues for a thorough analysis and assessment of vulnerabilities that may arise in the future with regard to originally secure technology. Furthermore, he suggests that certificates should not be valid for too long, emphasizing particularly the fast-paced nature of technological development in the area of computer systems. He suggests that further security gaps may only become apparent in the future and that system design must therefore allow for the possibility to add in or amend security features later on (Schaar 2010).

In 2008, the UK Information Commissioner's Office (ICO) launched its PbD program, stating that it would encourage public authorities and private organizations to identify and address privacy concerns at the outset of developing information systems that hold personal data. The ICO follows a principle of designing in privacy and data protection compliance and securing privacy throughout the entire lifecycle of a system. It suggests that PbD needs to go beyond design of technological systems, to also consider organizational changes. The ICO argues that there is a need to develop:

- An executive mandate for privacy by design.
- Privacy impact assessments throughout the system life cycle.
- Cross-sector standards for data sharing.
- The development of practical privacy standards.
- Promotion of current and future research into PETs.
- Establishing more rigorous compliance and enforcement mechanisms.

The ICO leans toward a set of "high-level principles and self-regulation" rather than the more "prescriptive

proposals of the Article 29 Working Party, the German Commissioner or now the EU proposal" (Krebs 2013, 12).

In the United States, the PbD debate concentrates on organizational obligations rather than on embedding of technological solutions in systems to protect privacy from the outset. The current proposal for a Commercial Privacy Bill of Rights includes a principle of PbD as "part of a mandatory privacy framework" (Krebs 2013, 10). The proposed Bill states:

> Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information that it collects, implement a comprehensive privacy program by 1. Incorporating necessary development processes and practices throughout the product life cycle that are designed to safeguard the personally identifiable information that is covered information of individuals based on (A) the reasonable expectations of such individuals regarding privacy; and (B) the relevant threats that need to be guarded against in meeting those expectations.

However, PbD has also been subject to criticism. Rubinstein and Good (2011, 1335–1336) argue:

> Presumably, the regulatory faith in privacy by design reflects a common sense belief that privacy would improve if firms "designed in" privacy at the beginning of any development process rather than "bolting it on" at the end. And yet there is not much relevant data in support of this view. . . . A few firms have adopted privacy guidelines for developing products and services but no one has conducted before and after studies to determine if they achieved better privacy results.

They go on to suggest that Cavoukian's seven principles do not offer anything beyond that already contained in Fair Information Practices (FIPs)[1] and that they lack a practical or operational element. They suggest instead that Cavoukian's approach remains aspirational. Cavoukian's approach also comes under fire for conflating PbD with other concepts such as "accountability," "risk management," and "privacy impact assessments," which tends to "dilute" the meaning of PbD, rather than to clarify it (Rubinstein and Good 2011).

This line of argument was also proposed by computer scientists at the 2011 international Conference on Privacy and Data Protection (CPDP) in Brussels, Belgium, who suggested that the seven principles do not make clear what PbD actually is and how the concept can be practically implemented into engineering practices. The inclusion of the term PbD in the principles themselves results in a "recursive definition"—"privacy by design means applying privacy by design" (Gürses, Troncosco, and Diaz 2011, 3).

In response, Cavoukian (2012b) argues that the FIPs are subsumed under PbD. She suggests that they are not the same thing but that PbD "significantly raises the privacy bar." Rubinstein and Good (2011) argue that regulators need to do more than promote the idea of PbD and recommend its adoption. The U.S. Federal Trade Commission (FTC) and European Commission have also recently been criticized for providing a strategy to privacy without any guidance on the application of PbD in a technological context (Krebs 2013). The FTC recently published its report *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, outlining a set of recommendations for best practices for businesses for protecting the personal data of consumers. The final report recommends that companies implement PbD, an option for consumers to decide what personal information held about them is shared (including a do-not-track mechanism), and a policy of greater transparency over the collection and use of consumer data (FTC 2012).

PbD principles have also been criticized for being "vague," with some suggesting that they "leave many open questions about their application when engineering systems" (Gürses, Troncosco, and Diaz 2011, 1). This includes warnings about the complexity of interpreting PbD principles when engineering systems and caution against the reduction of the methodology to a checklist for the purpose of compliance while ignoring the privacy risks that the idea of PbD is meant to address. The problems of translating PbD principles into systems design are clear in this literature. For Gürses et al. (2011), PbD is "posed as a non-technical strategy" and they argue that PbD is more than a simple matter of technological design; it also incorporates more abstract notions of data minimization, proportionality, and purpose limitation, as outlined in the EU Data Protection Directive 95/46/EC. These principles, as they suggest, are open to interpretation. In addition, they argue that PbD can become an umbrella term for privacy when organizations collect and process personal data and that there is a risk that it is reduced to a "series of symbolic activities to assure consumers' confidence" (Gürses et al. 2011, 6).

As we have seen in this section, PbD has been widely accepted by regulators. However, putting the principles of PbD into operation, in order for them to become meaningful for software engineers, is a challenge. Even within the term "privacy by design," there is an issue of what is meant by the terms "privacy" and "design." The next section of this article provides a brief overview of different approaches to understanding privacy.

UNDERSTANDING PRIVACY

Privacy is a complex topic with various definitions and encompassing a variety of meanings. The right to privacy has traditionally been argued as a "right to be let alone." However, privacy should be considered in relation to legislative definitions, particularly the rights accruing in relation to the space or place an individual inhabits, a need to protect the integrity of the body, a specific value placed

on the content and accessibility of information, and/or the constitution of a set of boundaries (Guagnin et al. 2012, 2). Various possible solutions for protecting privacy have been offered. These range from encouraging organizations to adopt Fair Information Practices (FIPs) to online privacy protections, seals, and certificates. However, there are also those who argue that "privacy is dead," or at least if it is not yet dead that it is impossible to protect in the face of rapid technological developments (Sykes 1999).

Privacy is certainly not a universal concept that can be applied across all technologies and all situations. Finn et al. (2013, 3) argue that current attempts to capture the complexities of privacy issues in post hoc frameworks are inadequate. They think that there is a need for a "forward-looking privacy framework that positively outlines the parameters of privacy." For this purpose, they build upon Clarke's influential four-part taxonomy of privacy, as it is no longer adequate for addressing the range of privacy issues that arise with new technologies. They identify seven types of privacy: privacy of the person, privacy of behavior and action, privacy of communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, and privacy of association.

Here, privacy of the person is defined as the right to keep body functions and body characteristics private. Privacy of behavior and action refers to sensitive issues such as political activities and religious practices. Privacy of communication relates to interception of communications such as recording and access to e-mail messages. Privacy of data and image entails the right of the individual to exercise control over personal data, rather than such data being available to organizations and others by default. Privacy of thoughts and feelings refers to the individual's right not to share her thoughts and feelings or not to have these revealed. Privacy of location and space encompasses the right of the individual to freely move about in public or semipublic space, without being monitored or tracked. Privacy of association refers to the right of the individual to associate with others without being monitored.

It is beneficial to keep this taxonomy in mind when thinking about PbD on two counts. One, it expands the discussion beyond data and personal communications, which has been the focus of data protection legislation, to different types of privacy. Two, instead of getting caught up in the myriad definitions of privacy, this taxonomy of seven types of privacy moves the debate forward and offers a structured approach to the analysis of privacy and PbD.

DISTINGUISHING BETWEEN PRIVACY BY DESIGN AND SECURITY BY DESIGN

Sarah Spiekermann notes that although PbD is proposed as a solution by regulators, it is "barely specified." She suggests that the first challenge for PbD is to engage an organization's management team in a discussion on the strategy for privacy management. Without this active engagement, privacy issues are excluded from any overarching organizational strategy for managing data and subsequently are dealt with as an afterthought. Furthermore, she argues that the effective implementation of a PbD process requires the "guts and ingenuity of engineers." However, she warns that even if these two challenges are met, there are other obstacles, include the differing interpretations of privacy. Spiekermann (2012) thinks that organizations need to first understand what they are trying to protect. The terms *privacy* and *security* are often conflated, which causes problems on two fronts. One, organizations lack clarity in knowing what they should be protecting and with what means. Two, privacy and security are often mistakenly weighted against each other in the traditional argument that to gain one is to lose the other, as losing personal privacy does not equate directly to a gain in terms of security or safety. Therefore, it is critical to have analytical clarity here, especially when PbD has recently been linked to the notion of security by design.

Gartner first proposed the idea of security by design in 2006. In his paper, he argues that security requirements need to be designed into the enterprise architecture from the outset. Cavoukian (2013) suggests that the two concepts can be complementary and convergent. She also argues that privacy is protected under this approach and that "identity propagation [is ensured] across heterogeneous vendors" (14) due to a number of key trends in mobile computing and cloud computing. Similar to the principle of incorporating privacy into the technology or system, security by design focuses on embedding security into the design and construction of the technology or system.

In sum, since "privacy" and "security" are often conflated, it is important to distinguish between them when thinking about operationalizing privacy by design. Although there are potentially lessons to be learned from approaches in security by design, privacy by design should be considered a separate concept. Designing in security does not mean that privacy has also been embedded into the design of a new technology or system.

DISTINGUISHING BETWEEN PbD, PRIVACY BY DEFAULT, AND DATA PROTECTION BY DEFAULT

As mentioned earlier, the proposed data protection regulation strongly promotes PbD, alongside the principle of data protection by default. For example, recital 75a of the regulation's preamble states: "The data protection officer should have at least the following qualifications: extensive knowledge of the substance and application of

data protection law, including technical and organizational measures and procedures; mastery of technical requirements for privacy by design, privacy by default and data security" (Unofficial Consolidated Version after LIBE Committee Vote in October 2013). The draft regulation (recital 61) makes a distinction between PbD and data protection by default, and defines the latter as follows:

> The principle of data protection by design requires data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimization and purpose limitation.

However, there is no explicit definition of PbD included in the draft regulation. Rather, the idea of PbD is implicit in various requirements, such as Article 23 and the obligation of the data controller to implement technical and general organizational measures at the design stage of data processing, in addition to privacy by default settings. Hence, for the European Commission, privacy by design (or, in its terms, "data protection by design") includes both technical and organizational measures. Elsewhere, the European Commission (2010) defines PbD as a principle that should be applied throughout the design stage and life cycle of a product, adding that relevant technologies should be implemented in accordance with that principle.

The Article 29 Working Party (2009), representing EU data protection authorities, also proposes embedding PbD into technological systems. It has previously advised that data protection and/or privacy regulation should include principles of data minimization, PETs, access controls, and encryption (and that these should be legally binding and enforceable by data protection authorities). The principle of data minimization has also been strongly promoted by the European Data Protection Supervisor (EDPS 2010). The EDPS states that alongside a general principle of PbD, data minimization should also be regulated more specifically with regard to browser applications, radio-frequency identifications (RFIDs), and social networks. Similar to the German data protection authorities, EU proposals in the area of PbD lean toward a principle of PbD that "requires technological (i.e., PETs) and organizational elements at the design stage, rather than only organizational requirements" (Krebs 2013, 12).

TRUST AND ACCOUNTABILITY

The idea of PbD is often linked with discussions of enhancing user trust in new systems and technologies. The issue of trust has become an important theme in EU-level policy conversations on information and communication technologies (ICT) and security and surveillance technologies. In March 2010, the European Data Protection Supervisor (EDPS) stated: "Trust, or rather its absence, has been identified as a core issue in the emergence and successful deployment of information and communications technologies. If people do not trust ICT, these technologies are likely to fail. Trust in ICT depends on different factors; ensuring that such technologies do not erode individuals' fundamental rights to privacy and to the protection of personal data is a key one" (EDPS 2010, 15). The EDPS therefore proposed to the European Commission that privacy by design be embedded into legislation and policymaking. This proposal contained the following four elements: the incorporation of a general provision for PbD in the legal framework for data protection, the inclusion of specific provisions in legal instruments, the inclusion of PbD as a guiding principle for Europe's Digital Agenda, and the introduction of PbD as a principle in other EU initiatives.

The EDPS also proposed that a principle of accountability be implemented based on the existing data protection directive. EU discussions on accountability suggest that current legal regulations for protecting privacy are inadequate and that without a change in the current direction, the problems of data protection are set to continue. Furthermore, commentators in the field have suggested that "accountability can form the focus for dealing with issues of scale in regulation, privacy risk assessment, self-regulation through certification and seals and foster an environment for the development of new technologies for managing privacy" (Guagnin et al. 2012, 3). Finally, accountability is tied together with legal compliance and the idea that those who control data should, on request, be able to show compliance with data protection legislation. Although these discussions place accountability at center stage, the practicalities of achieving accountability in practice are left open to further debate.

One of the oldest sets of guidelines for international data protection, the Organization for Economic Cooperation and Development (OECD) 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, states, under the 14th guideline—the "Accountability Principle"—that "a data controller should be accountable for complying with measures which give effect to the principles stated above." These principles include those that are now familiar in data protection legislation: collection limitation, purpose specification, use limitation, and security safeguards. These guidelines discuss accountability further in relation to the data controller and state that accountability for complying with privacy rules should rest with the controller (even in the case of third-party data processing). Under these guidelines, therefore, the

term "accountability" becomes synonymous with responsibility and/or liability (Raab 2012, 16).

The Article 29 Data Protection Working Party (2010) suggests that the concept of accountability is complex and difficult to define, stating that responsibility and accountability are essentially synonymous and both essential requirements for good governance. They go on to state that the term cannot be easily translated into other European languages and that for this reason the risk of misunderstanding or inconsistency is high. As Raab (2012, 6) points out, there is an element of "being sensitive to the distinctions" in trying to define the term in the first instance. However, he also notes that the Article 29 Working Party gives up any attempt to refine the term as they consequently state:

> 2.2 One may also suggest that accountability refers to the implementation of data protection principles.
>
> 2.3 In this document, therefore we focus on the measures which should be taken or provided to ensure compliance in the data protection field.

The term is, therefore, once again used in the context of responsibility for compliance with the law.

In 2011, the EDPS defined the "accountability principle" as:

> Data controllers should be mandated to be more active and to take all those measures which are necessary to ensure that data protection rules are complied with. This is the principle of accountability that would require data controllers to be able to demonstrate that they have taken all appropriate measures to ensure compliance. (EDPS 2011, 5)

This definition suggests that accountability is defined as compliance with data protection principles, as well as the ability of the data controller to provide evidence of this compliance.

Mulgan (2002, 55) argues that the term "accountability" performs a wide range of "analytical and rhetorical tasks." He argues for a distinction between the internal and external aspects of accountability. *Internal accountability* can refer to a sense of responsibility for the public interest from civil servants, or public discussion between citizens. *External accountability* involves being held to account by an authority. It involves a process of social interaction and exchange—one side seeks "answers and rectification" and the other (being held to account) "responds and accepts sanctions." For Mulgan (2000, 562), there is a clear distinction between "having to account to someone else for one's actions and not having to do so." Bennett (2012, 33) also argues that accountability means more than responsibility and suggests that it "implies a process of transparent interaction, in which [an external] body seeks answers and possible rectification." The involvement of an external body is therefore imperative—a means by which the other body is called to account. Drawing on Mulgan's work, Bennett argues that the external body is there to seek redress and impose sanctions. He states that if there is no external demand to alter practices then there can be no accountability. In terms of accountability and privacy protection, he argues that there is a real need for a common understanding of "*who is accountable, for what, and to whom*" (emphasis in original), which he suggests is missing from current policy discussions (2000, 34). In relation to operationalizing PbD, thinking about accountability is important in terms of the process of holding an organization, system or technology to account. Operationalizing PbD becomes a process that should include an element of reflexivity and accountability. We return to this point later in this article.

THE PbD PROCESS

In our view, PbD is more than a set of principles: It is also a process, which is intimately tied to the design process. For process guidelines, we invoke the privacy impact assessment process. A privacy impact assessment can help identify privacy risks. Identification of risks can spotlight areas where PbD principles can be employed to develop effective solutions.

PIAs should not be considered as simply legal compliance checks. Nor should they be considered the same as privacy audits, used to assess existing technologies, although, as Wright (2011) argues, a PIA can enable an organization to demonstrate compliance with legislation in the case of a privacy audit or complaint. Undertaking a PIA can "provide evidence that the organisation acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation" (Wright 2011, 55). However, they are not simply used to warn against potential risks but also to mitigate these risks, and to change the development process accordingly. PIAs, therefore, move beyond the legal compliance to also assess and address moral and ethical issues of the proposed system (Flaherty 2001). The Ontario Data Protection guidance states that the entire information life cycle needs to be supported by relevant policies and procedures and that any risks need to be identified and reduced or minimized if they cannot be eliminated entirely (Cavoukian 2010). A privacy impact assessment is one of the ways that the information life cycle can be managed and privacy risks minimized.

Wright (2011) suggests that there is currently an increasing interest in the use of privacy impact assessments in Europe. The United Kingdom introduced the first PIA methodology in 2007, although PIAs have been used in Australia, Canada, New Zealand, and the United States since the mid 1990s. Conducting a PIA is now mandatory for government agencies in the United Kingdom, Canada,

and the United States (Wright 2011). It is obvious that some organizations will avoid undertaking privacy impact assessments unless they are mandatory. In terms of best practice, Wright (2011) concludes that a PIA process should include:

- An assessment of privacy risks an organization might face in relation to a new project (although he cautions that a PIA on its own will not highlight all privacy risks and/or issues associated with a new project).
- A process of engaging stakeholders.
- Recommendations and an action plan.
- Publication of the PIA report (redacted, if necessary).

This is followed by the recommendation that a third-party review and/or audit of an organization's PIA be conducted to ensure longer term commitment to the process and suggested changes (Wright 2011). In terms of best practice, Wright also suggests that, in addition to a third-party review, accountability mechanisms, such as mandatory reporting requirements, should be implemented. Finally, he argues that tying PIAs to budget submissions for new projects and programs can ensure a greater number of PIAs are actually undertaken, as well as enhancing accountability.

PbD TECHNOLOGIES

There is no widely accepted definition of privacy-enhancing technologies (PETs).[2] The Enterprise Privacy Group, which authored the 2008 "Privacy by Design" report for the ICO, defined PETs as technology that:

1. Reduces or eliminates the risk of contravening privacy principles and legislation.
2. Minimizes the amount of data held on individuals.
3. Empowers individuals to retain control of information about themselves at all times.

The Information Commissioner's Office (2006, 2) defines PETs as "any technology that exists to protect or enhance an individual's privacy, including facilitating individuals' access to their rights under the Data Protection Act 1998." The Commission (2007, 2) defines PETs as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system."

Cavoukian (2008) suggests that by applying privacy-enhancing features to a surveillance technology, for example, the minimization of collection of personal data, both privacy and security can be maintained. However, Le Métayer (2010) warns against making PETs synonymous with PbD, arguing that PETs are often not "privacy-compliant." This is an important point. Operationalizing of PbD should include the development and/or use of PETs; however, these need to be assessed against privacy criteria in the form of a PIA. The strategy for operationalizing PbD should therefore become a cyclical process involving PbD principles, a PIA process, and a menu of PETs. The PIA process should be ongoing and prevalent throughout the technology or system design life cycle.

The snag with PETs is that they are not widely used. The ICO (2008) suggests that organizations are hesitant to adopt PETs in case they become obsolete as technologies develop. However, this may not be the only reason that PETs have not been widely used. As Koops et al. (2013) argue, although European regulators have adopted PbD, there is a lack of incentive for organizations to use them in practice. They also suggest that there are "conceptual difficulties . . . translating flexible legal norms into more rigid technology-embedded rules" (677). Nevertheless, they suggest that there are many technical solutions that can help to protect privacy "if they are part of a wider and integrated strategy of privacy by design. Such an approach might benefit from privacy design strategies, which can help bridge the gap between the abstract notion of privacy by design and the concrete tools of privacy-enhancing technologies" (Koops et al. 2013, 678).

With regard to operationalization of PbD principles, Cavoukian says that more work needs to be done to develop specific guidelines for applying the principles. She suggests that "there is a long road ahead in the journey of translating PbD's 7 foundational principles into concrete, prescriptive requirements, specifications, standards, best practices, and operational performance criteria" (2012a, 56). She concludes that this process must involve not only executives but also software engineers, risk managers, privacy officers, and so on.

The international standards body OASIS (the Organization for the Advancement of Structured Information Standards) has recently set up a new technical committee in an attempt to develop and promote standards for PbD in software engineering. The committee (PbD-SE) suggests that although the idea of PbD has been widely accepted there is a lack of detailed guidance regarding how software engineers can execute PbD principles throughout the software development life cycle. The PbD-SE states that it will fill the gap left by the Privacy Reference Management Model (PMRM) and the OASIS eXtensible Access Control Markup Language (XACML). The PbD-SE suggest that neither PMRM nor XACML "address[es] a future standard for privacy extensions to software modelling tools that engineers can use to embed privacy into their systems and services analyses, software designs, and documentation" (OASIS 2012, 5).

Standards

There are various international privacy and data protection standards that can be factored into a strategy for operationalizing PbD. Although not legally binding, regulators often refer to these standards, developed by the International Organization for Standardization (ISO), as examples of good practice. ISO/IEC 27001/2005 is an information security management system that details requirements for organizations to examine security risks and vulnerabilities, and to aid in the design and implementation of security controls. Organizations that adopt ISO/IEC 27001 can in turn be audited to verify compliance with the standard. The ISO/IEC 27001 standard is often implemented in conjunction with other standards, such as ISO/IEC 27005, which provides guidance to support the information security management system, in the form of risk assessment, monitoring and review, and risk management.

The ISO is also developing a standard on privacy impact assessment (the draft is numbered ISO/IEC WD 29134), which will provide a set of guidelines for the conduct of PIAs. In terms of the process for an organization conducting a PIA, the following stages are currently outlined in this draft standard:

1. Determine whether a PIA is necessary.
2. Identify the PIA team and set the terms of reference, resources, and time frame.
3. Prepare a PIA plan.
4. Determine the budget for the PIA.
5. Describe the proposed project to be assessed.
6. Identify stakeholders.
7. Describe the information flows and other privacy impacts.
8. Consult with stakeholders.
9. Check the project complies with legislation.
10. Identify risks and possible solutions.
11. Formulate recommendations.
12. Prepare and publish the report.
13. Implement the recommendations.
14. Third-party review and/or audit of PIA.
15. Update the PIA if there are changes in the project.
16. Embed privacy awareness throughout the organization and ensure accountability.[3]

As this standard is still in its draft stage, the document has not yet gone into greater detail in relation to measures or processes to be implemented to ensure accountability.

CONCLUSIONS

The gap between the principles of PbD espoused by regulators and the operationalization of these principles by industry is due, at least in part, to a lack of guidelines for transforming the abstract principles into concrete methodologies and tools.

Cavoukian strongly argues that all seven principles of PbD must be taken into account—it is not a list from which to pick and choose. The examples of IBM and Startmail show projects that apparently have taken the seven principles into account at all stages of development. However, without a set of clear criteria or guidelines, it is difficult (if not impossible) to rigorously assess whether all of them have indeed been implemented. In effect, without policy and guidelines against which to assess these sorts of projects, the notion of PbD continues to be abstract rather than enforceable. A third example, the ELENA system in Germany, shows a more stringent process for the implementation of the seven principles of PbD from the outset of the design process. Here, since it was not possible to operationalize the principles and still develop the system, assessment of the system took place at the same time as the development of the technology. But the assessment was conducted against a set of principles rather than a robust set of criteria or guidelines. In effect, the problem of assessing the system against set criteria remains.

In order to facilitate effective operationalization of PbD, we call for focus on three main elements—a set of principles, process guidelines, and a menu of technology solutions. With regard to principles, we do not see any need to make a choice between Ann Cavoukian's seven principles of PbD and those put forward by Peter Schaar. Both have merit. For process guidelines, we invoke the privacy impact assessment process. It helps identify privacy risks and thereby helps pinpoint areas where PbD principles can be applied and where possible technological solutions embedded. The ISO PIA standard that is currently under deliberation appears to offer an effective process.[4] The third element is a menu of technology solutions that can help to embed privacy in the design of new technologies, systems and services. The menu can be updated as new privacy-enhancing technologies become available.

Under Article 23 of the proposed EU Data Protection Regulation, PbD would become a requirement. The same legislation also aims to make privacy impact assessments mandatory. While these measures can be seen as a step forward in terms of privacy regulation, simply proposing principles is not enough. Ensuring accountability in relation to privacy needs to include more than principles, responsibility, or liability. It requires a process of one body holding another body to account, which should include a process of rectification if the first body is found to be lacking in terms of compliance. Accountability provides the "teeth" for PbD; it assures that privacy by design is more than stated intentions.

NOTES

1. FIPS are designed to cover how much data an organization holds, the reliability and accuracy of those data, the uses to which those data are put, and accountability and transparency practices. For more on FIPS, see Bennett and Raab (2003).

2. PETs include privacy management tools such as cookie blockers, spam filters, pop-up blockers, anti-spyware, and pseudonymization tools.

3. The draft standard draws heavily on the work carried out by Trilateral Research & Consulting, Vrije Universiteit Brussel, and Privacy International for the Privacy Impact Assessment Framework (PIAF) project. See Wright (2013).

4. Those who have more pressing requirements need not wait until the standard is finalized. The process draws on the PIAF project, the documents for which are already publicly available.

FUNDING

This article draws on research that in part was undertaken in the context of the EC-funded PRIPARE project (the acronym stands for PReparing Industry to Privacy-by-design by supporting its Application in Research), grant agreement 610613. The views expressed in this article are those of the authors alone and are in no way intended to reflect those of the European Commission.

REFERENCES

Article 29 Data Protection Working Party. 2009. *The future of privacy: Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*. Technical report 02356/09/EN WP 168. Brussels, Belgium: European Commission.

Article 29 Data Protection Working Party. 2010. *Opinion 3/2010 on the principle of accountability*, 13 July, paras 21–3. Brussels: European Commission. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf (accessed June 18, 2014).

Bennett, C. 2012. The accountability approach to privacy and data protection: Assumptions and caveats. In *Managing privacy through accountability*, ed. D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland, and H. Postigo, 33–48. Basingstoke, UK: Palgrave Macmillan.

Bennett, C. J., and R. Grant. 1999. *Visions of privacy: Policy choices for the digital age*. Toronto, Canada: University of Toronto Press.

Bennett, C. J., and C. D. Raab. 2003. *The governance of privacy—Policy instruments in global perspective*. Hampshire, UK: Ashgate.

Cavoukian, A. 2009. Privacy by design: The Definitive Workshop Workshop. Madrid, Spain. http://www.privacybydesign.ca/content/uploads/2009/11/2009-11-17-PbD-Madrid-Program-web.pdf
(accessed December 11, 2013).

Cavoukian, A. 2010. *Privacy risk management: building privacy protection into a risk management framework to ensure that privacy risks are managed by default*. Toronto, Canada: Information and Privacy Commissioner.

Cavoukian, A. 2012a. *Operationalizing privacy by design: A guide to implementing strong privacy practices*. Toronto, Canada: Information and Privacy Commissioner. http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf (accessed June 18, 2014).

Cavoukian, A. 2012b. A regulator's perspective on privacy by Design, http://www.futureofprivacy.org/wp-content/uploads/A-Regulators-Perspective-on-Privacy-by-Design.doc (accessed December 7, 2013).

Cavoukian, A., and M. Chanliau. 2013. *Privacy and security by design: A convergence of paradigms*. Toronto, Canada: Information and Privacy Commissioner.

Cavoukian, A., S. Taylor, and M. E. Abrams. 2010. Privacy by design: Essential for organizational accountability and strong business practices. *Identity in the Information Society* 3(2): 405–13.

Enterprise Privacy Group. 2008. Privacy by design: An overview of privacy enhancing technologies, http://www.ico.org.uk/upload/documents/pdb_report_html/pbd_pets_paper.pdf (accessed December 3, 2013).

European Commission. 2007. Communication on promoting data protection by privacy enhancing technologies (PETs). COM(2007) 228 final, Brussels, 2. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0228:en:NOT (accessed November 28, 2013).

European Commission. 2011. EU-US negotiations on an agreement to protect personal information exchanged in the context of fighting crime and terrorism. Memo 11/203, Brussels, Belgium.

European Data Protection Supervisor. 2010. Opinion on privacy in the digital age: "Privacy by Design" as a key tool to ensure citizens' trust in ICTs. Brussels, Belgium. http://www.legi-internet.ro/fileadmin/editor_folder/pdf/edsp_EN.pdf (accessed December 18, 2013).

European Data Protection Supervisor. 2011. *Annual report 2011*. Brussels, Belgium: Publications Office of the European Union. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2011/AR2011_EN.pdf (accessed December 17, 2013).

Federal Trade Commission. 2012. Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers. http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (accessed December 7, 2013).

Finn, R., D. Wright, and M. Friedewald. 2013. Seven types of privacy. In *European data protection: Coming of age?*, ed. Serge Gutwirth, Yves Poullet et al., 3–32. Dordrecht, the Netherlands: Springer.

Flaherty, D. 2001. Privacy impact assessments: An essential tool for data protection. In *The Personal Information Protection and Electronic Documents Act*, ed. S. Perrin, H. H. Black, D. H. Flaherty and T. Murray Rankin. Toronto, Canada: Irwin Law.

Guagnin, D., L. Hempel, C. Ilten, I. Kroener, D. Neyland, and H. Postigo (eds.). 2012. *Managing privacy through accountability*. Basingstoke, UK: Palgrave Macmillan.

Gürses, S., C. Troncoso, and C. Diaz. 2011. Engineering privacy by design, http://www.cosic.esat.kuleuven.be/publications/article-1542.pdf (accessed June 18, 2014).

Hustinx, P. 2009. Privacy by design: Delivering the promises, Speech given by the European Data Protection Supervisor, at "Privacy by Design: The Definitive Workshop," Madrid, November 2. https://

secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-11-02_Madrid_privacybydesign_EN.pdf (accessed June 18, 2014).
Information Commissioner's Office. 2006. *Data protection technical guidance note: Privacy enhancing technologies (PETs)*. Wilmslow, UK: Information Commissioner's Office. http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.pdf (accessed July 15, 2012).
Information Commissioner's Office. 2008. *Privacy by design*. Wilmslow, UK: Information Commissioner's Office. http://www.ico.org.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf (accessed December 6, 2013).
International Organization for Standardization and International Electrotechnical Commission. 2005. ISO/IEC 27001/2005. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en (accessed June 26, 2013).
Koops, B.-J., J.-H. Hoepman, and R. Leenes. 2013. Open-source intelligence and privacy by design. *Computer Law & Security Review* 29(6): 676–88.
Krebs, D. 2013. Privacy by design: Nice-to-have or a necessary principle of data protection law? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2: 4–20.
Le Métayer, D. 2010. Privacy by design: A matter of choice. In *Data protection in a profiled world*, ed. Serge Gutwirth, Yves Poullet and Paul de Hert, 323–34. Dordrecht, the Netherlands: Springer.
Mulgan, R. 2000. Accountability: An ever-expanding concept? *Public Administration* 78(3): 555–73.
OASIS. 2012. *Call for participation: Privacy by design documentation for Software Engineers (PbD-SE) Technical Committee*. https://www.oasis-open.org/news/announcements/call-for-participation-privacy-by-design-documentation-for-software-engineers-pbd (accessed October 12, 2013).
Raab, C. 2012. The meaning of 'accountability' in the information privacy context. In *Managing privacy through accountability*, ed. D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland and H. Postigo, 15–32. Basingstoke, UK: Palgrave Macmillan.
Rooy, D., and J. Bus. 2010. Trust and privacy in the future Internet—A research perspective. *Identity in the Information Society* 3(2): 397–404.
Rubinstein, I., and N. Good. 2011. Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technology Law Journal* 28: 1333–413.
Schaar, P. 2010. Privacy by design. *Identity in the Information Society* 3(2): 267–74.
Solove, D. 2011. *Nothing to hide: The false tradeoff between privacy and security*. New Haven, CT: Yale University Press.
Spiekermann, S. 2012. The challenges of privacy by design. *Communications of the ACM* 55(7): 38–40.
Sykes, C. 1999. *The end of privacy*. New York, NY: St. Martins Press.
Wright, D. 2011. The state of the art in privacy impact assessment. *Computer Law & Security Review* 28(1): 54–61.
Wright, D. 2013. Making privacy impact assessment more effective. *The Information Society* 29(5): 307–15.

APPENDIX: CASE STUDIES

The first case study is IBM's incorporation of PbD into predictive analytics, a project noted for initiating the process in the design stage. The second case study is that of Startmail. While this project is still under development, it promotes a strong case for employing PbD principles in a rigorous and methodological manner in the design stage of a technology or system. The third case study is the ELENA system in Germany. In this instance, the application of PbD principles resulted in the abandonment of the project.

IBM

IBM recently released G2, a version of "sensemaking" technology, which allows organizations to gather and process data from a variety of sources in real time. Various PbD features were embedded into this technology, including the ability to anonymize data in the host system, before they are shared and combined with other data. Jeff Jonas, Chief Scientist of the IBM Entity Analytics Group, states:

> One of the Privacy by Design methods I've been building, called selective anonymization, allows you to anonymize things like social security number or driver's license number or date of birth, whatever the features the company has, at the source system before you move it to the table where the puzzle pieces would come together to see how they relate. But even if a person sees those puzzle pieces, or steals those puzzle pieces, they can't actually see your Social Security number or your date of birth. Because it's non-human readable . . . Our goal is not to hide the identity of the person. Our goal is to protect the values that you wouldn't want to be revealed. (Jonas cited in Foege 2013)

Names and addresses are visible under this system but the personally identifiable information is hidden to be non-human readable and nonreversible, known as a one-way hash. The features are therefore anonymized prior to any matching of data taking place.

Jonas states that various other PbD features were also embedded into the software, including a tamper-resistant auto-log and a "full attribution" feature, which attributes every piece of data to its source, rather than combining the data and not keeping track of the source. Jonas concludes by stating:

> The number one thing I've learned from the privacy community—if I were to synthesize into the fewest number of words what I've learned—is, avoid consumer surprise. Collect the data and use the data in a way that, if revealed and on the front page of the paper, it would not create any consumer surprise. And that's mainly a law and policy point of view, not much of a technology statement. For an organization to be competitive today, they'd better figure out how to make sense of their data, or they're not going to be in business. And then the next thing after that is, how can you do it in a way that's more responsible and reduce the risk of misuse that might damage their brand? (Jonas cited in Foege 2013, online)

Startmail

Startmail is a pay-for subscription e-mail service currently under development. To date, it has been beta-tested by 50,000 volunteers. Paid-for Startmail accounts are due to be launched in 2014. Startmail is promoted as a "private email service." In a December 2013 presentation at the IAPP Congress in Brussels by Alexander Hanff (formerly of Privacy International), he stated that Startmail has been developed according to the following privacy-focused principles:

> No IP addresses recorded.
> No record is made of your searches.
> No identifying or tracking cookies used.
> All communications with both sites are encrypted by default over a Secure Socket Layer (SSL/HTTPS) with highest-level encryption including Perfect Forward Secrecy and supporting TLS1.1 and 1.2.
> No logs are retained of any personal information.
> No personal information is being sent to third parties (no search leakage).

Hanff suggests that the system pays heed to all seven principles of PbD. For example, Startmail is said to have full functionality by developing a "feature rich solution" to users, providing them with a "Positive-Sum service." Furthermore, Startmail is said to provide "end-to-end security" through a variety of encryption methods. Privacy is embedded into the design, with privacy as the default setting. Hanff argues that "data is not the only currency" and that "freemium is not the only model."

ELENA

ELENA stands for "*elektronischer Entgeltnachweis*" (electronic proof of earnings) and was designed as a database to store income information for individuals employed in Germany. Its purpose was described as streamlining applications for social benefits. It was planned that ELENA would go live on 1 January 2012; however, the system was disbanded prior to its becoming operational (July 2011).

Peter Schaar (2010, 10) describes the following data protection principles built into the system:

> 1. encryption of all transmission channels and all data files in the database;
>
> 2. spatial, organizational, technical and personnel separation between the central database and the body responsible for registering participants and processing their data;
>
> 3. rigorous separation between the body storing the data and the body responsible for administering the master key. The German Bundestag assigned me, as Federal Commissioner for Data Protection and Freedom of Information, the responsibility of administering the master key;
>
> 4. keeping a log of all database transactions, retrievals, etc., in order to document all data processing operations for examination by the data protection supervisory authorities;
>
> 5. immediate and targeted deletion of data when they are no longer necessary;
>
> 6. internal technical separation and isolation of all organizational units involved in the system, and defining an inner and outer layer of security, each with its own physical barriers and oversight mechanisms;
>
> 7. principle of requiring two signatures to retrieve data (the retrieving body and the data subject must always authorize data retrieval by presenting a signature card bearing a legally mandated qualified signature);
>
> 8. only authorized agencies and their staff may retrieve the parts of the data file necessary to carry out the task at hand (subject to both content and time restrictions);
>
> 9. technical measures to ensure that data are used only for the purpose for which they were collected, and in particular that no access is given to the security authorities, tax authorities, Customs, and the like.

Data protection authorities were involved in the planning of the system from an early stage. The reason given for the eventual disbanding of the system was that "qualified electronic signature cards had not found widespread application" and that "as a cornerstone of ELENA's functioning (and coinciding data protection and security standards), the widespread use and accessibility of the qualified electronic signature was seen as an indispensable condition precedent to the system's implementation" (Krebs 2013, 7). Ultimately, the application of PbD principles to the ELENA system meant that the design could not "be reconciled with privacy principles" and culminated in the abandonment of a system that had cost hundreds of millions of euro.