"Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law?

by **David Krebs***
Juris Doctor, LL.M., Member of the Law Society of Alberta (Canada)

Abstract: Privacy by Design is a term that was coined in 1997 by the Canadian privacy expert and Commissioner for Ontario, Dr Ann Cavoukin, but one that has recently been receiving more attention in terms of its inclusion as a positive requirement into EU, US and Canadian data protection frameworks. This paper argues that the right to personal privacy is a fundamental right that deserves utmost protection by society and law. Taking privacy into consideration at the design stage of a system may today be an implicit requirement of Canadian federal and EU legislation, but any such mention is not sufficiently concrete to protect privacy rights with respect to contemporary technology. Effective privacy legislation ought to include an explicit privacy-by-design requirement, including mandating specific technological requirements for those technologies that have the most privacy-intrusive potential. This paper discusses three such applications and how privacy considerations were applied at the design stages. The recent proposal to amend the EU data protection framework includes an explicit privacy-by-design requirement and presents a viable benchmark that Canadian lawmakers would be well-advised to take into consideration.

Keywords: Data Protection, Canadian Privacy Law, Comparative Law, EU Data Protection Regulation, Right to Privacy

Recommended citation: David Krebs, "Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law?, 4 (2013) JIPITEC 2, para. 1.

A. Introduction

1 The threats to the individual right to privacy – or what is sometimes referred to as the right to 'informational self-determination'[1] or simply the 'right to be let alone'[2] – are currently being widely discussed, debated and analysed. This is particularly so where this right is impacted by new technologies or the incremental move of our daily activities online. New technologies that impact the way in which information about people, 'personally identifiable information'[3] ('PII'), is used, collected, stored and disseminated are appearing at a frequent and rapid pace. These may be 'apps', facial recognition technologies, smart electricity grids, Radio Frequency Technologies (RFID), cloud computing, mass and surreptitious surveillance, biometrics and private sector Internet marketing initiatives. Currently, for the most part at least, technology is being adjusted after the fact to patch privacy-related issues as they arise or after they have already had a negative impact.

2 To address these concerns and to move from a reactive to a proactive approach, Dr Ann Cavoukian, current Privacy Commissioner for Ontario, in 1997 had already developed the principles behind – and coined the phrase – 'privacy by design' (PbD). PbD recognizes that the deployment of technologies designed to achieve a certain commercial or public sector goal *without* having considered the privacy implications at the design stage of the technology[4] can result in personally identifiable information (PII) being used or disclosed in ways that harm privacy rights permanently. PbD embodies the merger of

two objectives: the protection and control of PII and privacy, and the advancement of the commercial application of technologies in a sustainable but competitive manner.[5] The *Protection of Information and Electronics Documents Act*[6] ('*PIPEDA*')[7] (as well as the *European Data Protection Directive*)[8] contains provisions relating to the adequacy of protective security measures and also, implicitly, privacy 'by design' requirements. At present, however, PbD is not an explicit part of the legislative scheme in Canada, the European Union (EU) or the United States of America (US), even though it is often cited as a best practice and perhaps even as the 'gold standard' in privacy protection.[9]

3 Calls for an introduction of PbD into legislative frameworks have been receiving more attention recently, for example, within the proposal for an EU privacy framework,[10] in proposed legislation in the US,[11] as well as a resolution at the *32nd International Conference of Data Protection and Privacy Commissioners* in Jerusalem. In Canada, there have been no such concrete proposals, only the vocal views of the Federal and Ontario Commissioners.

4 This paper argues that legislated PbD is the necessary next step in privacy law to protect a right that is fundamental to liberty, personal integrity and democracy. For this reason, PbD deserves explicit mention as a tenet of privacy and data protection law. However, the view that laws based on PbD principles alone would be sufficient in this regard is not tenable in a world of ubiquitous computing and transformative technologies. A broad, principled approach relies on organizations adopting appropriate measures without providing the necessary guidance necessary to *prevent* actions injurious to personal privacy such as data breaches, unwanted tracking or uncontrolled collection of ever-increasing amounts of PII. PbD needs to be incorporated into the privacy law framework in Canada (and elsewhere) as a general organizational requirement *and*, in appropriate circumstances, mandate specific technological solutions, such as 'privacy enhancing technologies'[12] (PETs), as well as the corresponding ability for the regulator to prevent a system or application from being initiated.

5 The first part of this paper will briefly describe the legal right to privacy in order to set the stage for why the design of systems that conform to this right is of such primal importance to its ultimate protection. The second part will turn to the current legislative framework to canvass the extent to which current provisions would satisfy the needs intended to be addressed by PbD. In this section, I will include examples from the EU framework because of its relevance to Canadian privacy laws. Canadian policy discussions often run in parallel[13] and Canada and Europe share many relevant socio-cultural aspects.[14] I will also be looking to the US, where there have been some significant developments in this regard. The third part will look at pertinent examples of systems to which PbD principles were applied, and without which the resulting systems would likely have been much more privacy-intrusive. The last part of the analysis will focus on the views of data protection authorities relating to incorporating PbD into legislative frameworks, including a close look at the legislative proposal from the Ontario Commissioner, Dr Ann Cavoukian, which was included as part of a very recent publication from her office.[15] The final part of this article will make some recommendations and suggested points for future research in this regard.[16]

B. Privacy by Design

I. The Right to Privacy

> [Code] will present the greatest threat to both liberal and libertarian ideals, as well as their greatest promise. We can build, or architect, cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear.[17]

6 This section is not intended to provide an exhaustive background to or a detailed comparative analysis of the right to privacy in Canada versus other Western jurisdictions.[18] Rather, it is intended to set the stage for the discussion of why a legislated PbD requirement might be a necessary addition to existing data privacy frameworks in order to protect the right to privacy as a fundamental personal and democratic right.

7 In some jurisdictions, privacy is an explicitly stated constitutional right.[19] In the EU, all Member States are signatories to the *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR),[20] which incorporates privacy as a fundamental right into EU law. Article 8 of the ECHR protects the "Right to respect for private and family life'[21] and forms the basis for modern privacy protection in Europe.

8 In Canada, the right to privacy is not a constitutional right as such; rather, the constitutional right to privacy is rooted in and protected by the Supreme Court of Canada's interpretation[22] of Section 8 of the *Charter of Rights and Freedom,*[23] the right to be free from unreasonable search and seizure. This protection is similar to the right afforded by the American 4th Amendment,[24] although one should not go too far in drawing parallels, as the jurisprudence in the US and Canada in this regard is certainly not uniform. Section 8 protects the liberty of the person but only in so far as the individual has a

'reasonable expectation of privacy'[25] in the conduct that is impacted by the intrusion or violation at the hands of the State, not applicable to intrusion by the private sector. Thus, constitutional protection of this privacy right is limited to where there is an infringement by the State of an individual's reasonable expectation of privacy.[26] It is by no means an absolute constitutional right.

9 Other than the protection of liberty, privacy rights have been stated to encompass two other values, informational privacy and dignity of the individual.[27] The Supreme Court of Canada in *R. v. Dyment*[28] noted that *Charter* privacy rights protect three aspects: spatial, informational and personal. Informational privacy rights in Canada are not constitutional rights. They are protected by private and public sector federal legislation such as *PIPEDA* and the *Privacy Act*,[29] respectively, as well as by relevant provincial and sector-specific legislation.[30] The European notion of privacy as the protection of dignity and democratic values[31] has been stated to exist as the third pillar of privacy protection in Canada and is related to the fact that the Canadian basis for privacy protection lies in the right to informational autonomy rather than solely in the right to liberty of the person.[32] It has thus been called the 'middle ground' or a compromise between the US and EU approaches.[33]

10 Privacy rights are clearly entrenched in Canadian jurisprudence and constitutional law. They are not rights that have been recently imagined but are deeply entrenched in Canadian and European culture. However, these laws stem from a time before most of the privacy-invasive technologies we are faced with today were a factor or even conceivable. They originated in a time before ubiquitous social media applications, before cloud computing, before Google Street View and before tracking technologies such as radio frequency identification devices (RFID)[34] existed or at least were in use; and although the principles may be sound, they cannot currently cope with systems and applications that were, for the most part, not designed with privacy protection as a main consideration. The key might lie in using the PbD approach to bridge the gap between ever-forward-moving technology and laws that (one could say inherently) lag behind. But before exploring why it might be necessary to include PbD within *PIPEDA* and other privacy legislation as an explicit requirement, the section below will outline the principles of PbD as well as salient examples of where these principles have been applied applications.

II. General Principles of PbD

11 PbD is no longer the exclusive domain of the Ontario Commissioner. As we will see throughout this paper, many other privacy experts have contributed to its definition, application and scope. That being said, the core principles enumerated by Dr Cavoukian are called the '7 Foundational Principles'[35] of PbD and still form the basis of what PbD encompasses. These include the following (not in order of importance): 1) proactive not remedialpreventative not reactive; 2) privacy as the default; 3) privacy embedded into design; 4) positive sum not zero sum; 5) end-to-end security; 6) visibility and transparency; and 7) respect for user privacy.

12 There is no hierarchy among these principles. Together they form the PbD objective in systems design: ensuring privacy, gaining control over one's information, and, for organizations, gaining a 'sustainable competitive advantage'.[36] The German Federal Commissioner for Data Protection and Freedom of Information ('German Commissioner'), Peter Schaar, himself a proclaimed 'PbD Ambassador',[37] recently distilled six PbD principles that should be taken into account in the design or acquisition of a processing system: data minimization, controllability (possibility of consent and objection supported by technological means), transparency, data confidentiality (security), data quality and possibility of segregation (in multi-user environments such as virtual machines and cloud computing).[38]

13 The German Commissioner has taken on the original foundational principles and to a limited, but I would argue important, extent altered or at least tweaked their meaning. For one, his PbD is prescriptive from a technological perspective. Secondly, the German Commissioner does not put as much emphasis on the 'win-win'[39] of technological advancement and the protection of privacy. PbD must first and foremost ensure that the principles of the EU Directive and the constitutional right to privacy are protected. Commercial interests are by no means a lone afterthought; rather, they seem to stand more on the periphery of the German Commissioner's notion of and purpose of PbD when compared with the description of the 7 Foundational Principles by the Ontario Commissioner.

14 In the United States, the debate surrounding PbD as a mandatory part of a legislative framework centres around organizational obligations, rather than embedded technological solutions to protect privacy by default, such as PETs.[40] The view that privacy is a right to be free from intrusion rather than a right to informational self-determination is more prevalent in the US than Europe or Canada. Underlying this rationale is the belief that commercial actors should have the freedom to control the means of processing data as long as they adhere to certain sound and proportional organizational principles. In the US, the term 'privacy' has more to do with harm, fear and the threat posed by computers than with the

general European view that to protect privacy is to protect personality and democracy. [41]

15 With the more pronounced 'positive sum' statement, the IPC – although at first glance aligned with the European approach, in particular when considering principle '3' of the PbD principles – lies somewhere in the middle of the purely organizational-measure and more prescriptive notions of PbD. The IPC states no official preference of whether a mandatory PbD requirement should be more organizational or technological, only that it encourages the adoption of PbD requirements into legislation in *some* form.[42]

16 Overall, PbD is still a relatively vague concept in terms of its translation into concrete systems design. Part of this is attributable to its relative novelty, at least in its widespread usage, and the other part to the gap that exists between regulators and systems engineers.[43] The 7 Foundational Principles, just as the US Federal Trade Commission's (FTC) and EU Commission's most recent interpretations, have been criticized as representing a 'non-technical' strategy to privacy that lacks technological guidance on PbD application.[44] While there may be many unresolved issues surrounding the practical implementation of PbD in certain instances, there are also numerous examples of feasible and successful applications from which important lessons can be drawn with respect to the utility, importance and implementation of PbD.

III. Current Practical Applications of PbD

17 PbD has a vast array of potential applications. In fact, any system that processes PII could benefit from or be the subject of PbD principles. This section will describe three examples of where PbD principles were considered in the design of systems that process large amounts of PII: the Smart Grid roll-out in Ontario, the use of biometrics for identification and the ELENA project in Germany, and the welfare application system in Ontario. I would argue that the application of PbD for all these systems was successful notwithstanding the very different practical outcomes for the introduction of the systems themselves.

1. Smart Grid

18 The term Smart Grid[45] refers to a system in which energy is delivered to the end-consumer in a way that allows for a more stable power supply, time-use pricing and demand management using state-of-the-art telecommunications to enable the 'smart' meter to communicate with the source.[46] The fact that energy supplies are decentralized to a much larger extent than years ago, while consumers have the ability to turn appliances off and on when they choose, creates the potential for energy supply-side instability. This is exacerbated where renewable energy is introduced into the system (as a less predictable supply of energy). This load-balancing could be achieved by creating the so-called 'Smart Grid', an intelligent grid that envisions two-way communication between demand (household) and supply (power source).[47] On account of its *ad hoc* ability to adjust the supply of energy, the Smart Grid can effect energy savings, and therefore also has positive environmental implications. It is estimated that by 2015 there will be 250 million smart meters installed worldwide.[48]

19 A more technical description of the Smart Grid is that it encompasses three aspects: Virtual Power Plants (VPP), Demand Side Management (DSM) and Control of Supply.[49] A VPP would be the backbone of the system, connecting a range of distributed and separate power supplies (windmills, solar or another other source of energy) that could then be managed according to demand. The VPP reduces the volatility of each individual power supply, as can be the case especially for renewable energy sources like wind and solar. The second part of the system is DSM, which is aimed at controlling demand. This control can either be initiated by the consumer (by reducing consumption) or by the supplier directly, whereby the consumer would agree to permit the operator to actively turn on and off certain appliances to balance energy use. The third piece of the puzzle is the control of the actual flow of power from the source to the end-user.

20 This intelligent system relies on information provided to the supplier by the household. This information is at least *prima facie* PII as it is naturally linked to a home, which in many cases will be owned and occupied by an individual. The type of information typically collected by the system (by way of 'Smart Meters'[50] installed at the home) will relate to the household's energy consumption patterns. Depending on the particular system and the incorporation of direct DSM or even 'Smart Appliances'[51], the information collected, however, will reveal a great deal more about the individuals than pure energy consumption. It may indirectly reveal criminal activities in the home, family living patterns, status of health, indications of physical activity in the home (types of machines) and so on. The use of the information is therefore not only relevant to the efficient control and supply of energy (utility services) but also for so-called 'edge services'[52] and law enforcement, insurance and market research purposes.[53]

21 Quite obviously, this system by its nature, and in particular if not designed properly, has immense negative implications for privacy and the protection

of the data entrusted into the system. Apart from the potential misuse of more traditional energy use data that is communicated via the system, the Smart Grid itself creates *new data*, not in existence before (e.g. relating to smart appliances), which is then also vulnerable and perhaps even more attractive for secondary uses. Beyond this, the National Institute of Standards and Technology (NIST) found in a Privacy Impact Assessment (PIA) conducted on Smart Grid systems that one of the major privacy risks of Smart Grids is the lack of consistent and comprehensive privacy policies among all the players whose actions affect PII (government agencies, utility companies and supporting organizations).[54]

22 For the Ontario Smart Grid implementation, the IPC and energy providers worked closely together to operationalize the system to include PbD aspects, that is, to design the way in which the system would operate and process PII throughout its life cycle. This project had and has implications for the design of Smart Grids elsewhere in Canada and internationally. The NIST has recently recommended the PbD approach as an appropriate methodology in this respect.[55]

23 This project focused on a number of issues that would need to be addressed operationally as well as technologically within the system and was described in great detail in a joint paper written by the system's operator, Hydro One, its partners and the Ontario Commissioner.[56] In this particular case (this method could also be applied to other systems), incorporating PbD meant that its principles needed to be part of the so-called Architectural Decisions document. This document defined the base policies and procedures that needed to be adhered to throughout the entire project and throughout all three 'domains' of the grid (the home domain, including smart appliances and meters; the services domain, including host data; and the grid domain, with the software backbone that automates and controls the distribution grid).

24 Including PbD into the entire system meant that

a) for the customer/home domain, no PII would persist on any device from the services to the customer domain (unless other services are explicitly purchased and consented to by the user); no PII will be sent from the services domain to the customer domain; and any interfacing online will include appropriate identity management and protection of information tools;

b) for the services domain, any and all access to devices in the customer domain from the services domain will be restricted and recorded; direct access must be authorized by the end-user; strict authorization-based access controls must be implemented whenever there is access to the customer domain; and all management of data storage would follow industry practices; and

c) for the grid domain, no PII will persist on any device in the grid domain; information regarding a device will be provided using authorized services; and access to a device must also be conducted through authorized services within the serviced domain.

25 Today, the Smart Grid is still in its relative infancy. Even in Ontario, a world leader in this regard (all residential homes have been equipped with smart meters), [57] the grid is not operational to its full capability.[58] Implementing PbD will thus be an on-going endeavour as the Smart Grid gets 'smarter' and more pervasive.[59] The design of these systems will require continuous evaluation in proportion to the granularity and amount of consumption data that is processed,[60] and the perils of the Smart Grid in terms of privacy impact are known and discussed on an on-going basis.[61] As it stands, however, the design of the Smart Grid in Ontario is by and large a positive example of how privacy considerations are being designed into a complex system from the outset. That is the strength of PbD: it is architected into the DNA of a system, and this is something that may not be fully guaranteed by laws that focus on principles rather than prescriptive standards.

2. ELENA

26 A second example of a system to which PbD principles have been applied is the 'ELENA' system in Germany. It stands for '*elektronischer Entgeltnachweis*' (electronic proof of earnings) and refers to a database system in Germany designed to store income information for all individuals employed in Germany for the purpose of streamlining applications for certain social benefits. ELENA as a process and system was designed as follows: Prior to applying for a certain benefit, an applicant would first obtain an electronic signature card with a smart chip containing a 'qualified electronic signature'[62] from a (government-certified) certification service provider. This step provides proof of an individual's identity. This unique signature card is then registered with the appropriate authority. The 'registry process' then links the certificate ID with the social security number of the applicant. On the ELENA database, then, employee personal data is not linked to the social security number of the applicant, but to the ID number of the certificate for the registered chip card. The card itself contains no information other than the name of the applicant and ID number of the registered chip card. All other information is stored in the central ELENA database.[63]

27 Due to the amount and sensitivity of PII, this database received considerable public attention. As noted previously, German privacy rights are explicitly entrenched in its Basic Law (*Grundgesetz*), and so this may have contributed to the German Commissioner being involved at a very early stage of the development process. The principles of German data protection law that were explicitly incorporated into ELENA included the following: encryption of all communication channels and data; separation between the central database and responsible administering body; logging of all database transactions; rigorous deletion of expired or unnecessary data; the principle of requiring the (qualified electronic) signatures of both data subject and administering body; and no access to security, tax or customs authorities.[64]

28 Ultimately, the application of PbD principles contributed to the current abandonment of the plans to bring the system online. Originally it was planned for ELENA to become operational as of 1 January 2012. Then, in July 2011, it was announced that the implementation of ELENA was to be abandoned[65] and that all PII collected to date was to be destroyed or deleted. The stated reason was that qualified electronic signature cards had not found widespread application. As a cornerstone of ELENA's functioning (and coinciding data protection and security standards), the widespread use and accessibility of the qualified electronic signature[66] was seen as an indispensable condition precedent to the system's implementation. According to most estimates, ELENA has cost Germany's taxpayers hundreds of millions of euros.[67]

29 The Smart Grid and ELENA systems are both examples of how PbD is and was applied and what the outcomes might be if the principles are applied appropriately. As we have seen, PbD can result in a system becoming a functioning data protective system, or it may result in the system being abandoned because its design cannot be reconciled with privacy principles.

3. Ontario Social Works Act

30 The third and final example of successful PbD application[68] is the welfare application system in Ontario. To combat abuse[69] of the social welfare system, in 1997 the Ontario government proposed certain changes[70] to the *Ontario Public Works Act, 1997*[71] and the *Ontario Disability Support Program Act, 1997*[72] enabling the ability to require welfare applicants to submit biometric data – here fingerprints – as unequivocal proof of identity when applying for benefits.[73] The privacy implications were grave since it would involve the collection and storage of sensitive, uniquely identifying data which would then be used in an assessment which is in and of itself of grave import to the individual applicant as it involves basic financial assistance.

31 With a view of balancing this processing of sensitive data with the need to combat fraud in the welfare system, the Ontario government worked with the IPC very early on in the process. After this consultation, it was decided that biometric data could be collected and used, but only if the concrete requirements relating to privacy and security of the information were followed. These are now entrenched in Section 75 of both pieces of legislation, and include requirements that any biometric information must be encrypted and destroyed after the encryption process, collected directly from the individual, only be released to third parties on warrant, and only retain address and sex alongside the encrypted biometric information.

32 Some of the above requirements now included in the legislation relate to processes, some to security measures and others to actual technology, but it is clear that not involving these measures at the outset[74] would have left this sensitive data exposed significantly more because a system architecture, once in place, is very difficult to re-design.[75] A system could be compliant with *PIPEDA* (or in this case, provincial public sector legislation) without fulfilling all of the principles of PbD, in particular when it comes to the requirement that all data would need to be encrypted and then destroyed after the process was complete, which is not an explicit requirement[76] under *PIPEDA*, leaving the data within the system more vulnerable to misuse and unauthorized access. It is important to note that the use of these systems was tabled in the public realm and therefore scrutinized before inception. For governments, this political pressure is a natural incentive to go beyond the letter of the law to protect citizens' privacy rights, but private companies that can implement systems out of the public's sight will not be subject to the same level of scrutiny, and one would expect deliberations to be based primarily on feasibility, cost and compliance with the law rather than the protection of privacy as such.

IV. Current Relevant Legislative Landscape

1. Canada

33 Canada's public and private sectors are governed by separate pieces of legislation both at a federal and provincial level. *PIPEDA* is federal legislation and governs private sector organizations, while the *Privacy Act* governs the public sphere. The Provinces each have separate public sector legislation, but only four (Alberta, Saskatchewan, Manitoba and

Ontario) have specific[77] health-sector legislation. Essentially, *PIPEDA* applies to the processing of personal information relating to all commercial activities where there is no provincial private-sector legislation, as well as to inter-provincial and international personal data flows, but it does not regulate activities related to the personal information of employees of provincially regulated organizations.

34 At a provincial private-sector level, only Alberta, Quebec and British Columbia have enacted their own pieces of commercial private-sector legislation, and within those Provinces, *PIPEDA* only applies to federally regulated organizations, including the personal information of employees of those federal organizations.

35 As a result, Canada does not have a uniform privacy framework. Compared with the EU (where Member States themselves – such as Germany, for example – may have a federal-provincial system comparable to that of Canada), however, these differences are still quite minor and one can speak of a relatively cohesive legislative landscape.[78]

36 Neither *PIPEDA* nor any of the provincial equivalents contains an explicit PbD requirement. What the legislation does require is adherence to the privacy principles of the *CSA Model Code for the Protection of Personal Information*,[79] which by *implication* may require data privacy considerations at the design stage of a system. A salient example of this would be Principle 4.7 regarding 'safeguards' (some of the suggested technological measures would need to be contemplated before bringing a system online) as well as Principle 4.4 regarding 'limiting collection'. This implicit application of PbD has become apparent during investigations of the Office of the Privacy Commissioner of Canada (OPC), for example, the *Google StreetView* Case,[80] in which Google was investigated for collecting PII in contravention of *PIPEDA*. Several of the remedial measures related to design-stage considerations (e.g. technical documents and evidence of appropriate processes and training ensuring that these are implemented when new systems are rolled out). The Commissioner applied Principle 4.4.1, which prohibits 'indiscriminate' collection of PII. As the collection of data is at the front end of any data processing, it is hard to imagine that this principle could be adhered to without giving thought to privacy considerations at the design stage.

37 All that being said, the requirements on Google to implement specific features *specifically* at the design stage would likely have been more explicit, and thus the protection of PII stronger, if a separate principle could have been relied on. As an example of this, on a number of occasions it was noted that privacy had not been considered sufficiently during the design of certain products, but the Commissioner did not have the ability to specifically state that a *PIPEDA* principle was breached. PbD remained an element of the ultimate recommendations, but only on the periphery.

38 A relevant feature of *PIPEDA* is the principle of "Accountability",[81] which requires organizations to designate individuals to "oversee the organization's compliance" with the principles contained in *PIPEDA*. Organizations need not notify the OPC of their PII processing activities (as in the EU, to be discussed below) but remain directly accountable for non-compliance under this principle. The OPC has the ability to audit such compliance. A weakness of *PIPEDA* from an enforcement perspective is that the Commissioner must initiate a complaint via the Federal Court, and only the Court may *force* an organization to correct its practices.[82] That is, *PIPEDA* currently does not contemplate the prevention of a system from being implemented, and this to be enforceable by the OPC, other than by the organization's accountable person to ensure that the Act is being complied with. Having a PbD requirement would obviously assist this individual in making an argument that certain requirements *must* be adhered to prior to going live with the processing.

39 Bill C-12, *An Act to Amend the Personal Information Protection and Electronic Documents Act*,[83] is currently in the first reading in the House of Commons and does not contain any mention of PbD as part of its amendments, which, apart from breach notification requirements, do not enhance the protection of PII in Canada but rather the ease of processing PII. As the analysis below will illustrate, this absence bucks the trend in other jurisdictions as well as to a certain extent the views of privacy commissioners and experts in this regard and may even be unsustainable[84] *vis-à-vis* a new EU data protection framework.

2. European Union

40 The basic data protection framework consists of the Data Protection Directive, the Directive on Privacy and Electronic Communications (e-privacy Directive),[85] the Data Retention Directive[86] and the 2009 e-privacy Directive.[87] All EU Member States have implemented the 1996 EU Directive. One must remember, however, that data protection law is by no means harmonized across the EU and that all statements about the 'European' situation must be viewed from this perspective. That is, the Directive is a guiding instrument (not a 'Regulation' with direct effect on local national law) and its intention is to harmonize the protection of PII within the otherwise free flow of information between Member States; in reality, however, there are many different laws and regulations (and underlying cultural aspects)

relating to the protection of personal data within the EU borders. Essentially, the EU has 27 similar but separate data protection laws. Sweden, as an example, views data protection law not as an equal guarantor for privacy and the free flow of information but primarily as a mechanism to ensure that a person's 'integrity' is not harmed by the use of PII (Section 1 *Personuppgiftslagen*[88]),[89] whereas this notion is not mentioned in the UK *Data Protection Act*.[90] Germany's federal law includes data breach notification provisions, which are not mandated by the EU Directive and provide a good example of the EU Directive provisions being a baseline of protections which local law may enhance under applicable circumstances.

41 The German Commissioner has pointed out on a number of occasions[91] that PbD is to a certain extent already regulated by the Directive by way of Article 46 of the recitals,[92] wherein it states:

> Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires *that appropriate technical and organizational measures be taken, 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; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, *taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected* (emphasis added).

42 I would argue that this is also implicit in Article 2 of the recitals:

> Whereas *data-processing systems are designed to serve man*; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals (emphasis added).

43 The Article 29 Working Party has opined that PbD should in fact become part of the revised Data Protection framework in Europe.[93] A closely related principle which also deserves explicit incorporation is the principle of 'accountability'. As noted, *PIPEDA* includes this principle as part of the *CSA Model Code*. This principle requires every organization to appoint one person within the organization to be accountable for the management of the organization's PII. The link to the PbD principle is that organizations would be required to ensure that this principle is being adhered to, as well as demonstrate compliance when challenged. The EU Directive also contains a notification requirement (Article 20). This obliges organizations to notify the appropriate DPA of PII processing in advance. In practice this means that a DPA may be able to prevent a system from going live, and this element of the Directive provides a complement to any PbD requirement as both are pre-emptive in their aims.

44 The European DPA wishes to not only see PbD included into the EU framework as a general principle but as a requirement for specific applications, specifically RFIDs, social networking applications, and browser applications. These requirements would be binding not only on data controllers[94] but also on processors, designers and purchasers of systems or applications.[95]

45 This approach is quite prescriptive and more what the Ontario Commissioner has called 'command and control regulation'.[96] It is clear from the EU DPA's perspective that loose principles will not suffice when systems with a potentially profound impact on privacy rights are concerned.

46 The very recently released first draft of the proposal of the European Commission to revise the EU Directive marks a big step toward the likely adoption of PbD into European (and other pieces) legislation. It is an ambitious attempt at harmonizing the EU legislative landscape. The proposed framework is suggested as a 'Regulation'[97] (with direct effect on Member States rather than a "directive which must then be transposed into local laws). This is in and of itself a major step toward harmonization. The Proposal includes a host of significant amendments, including doing away with the requirement to notify of processing[98] and replacing it with the obligation to maintain appropriate documentation surrounding the processing on controllers and processors (Article 28), explicit consent requirements (Article 1 – 'informed and explicit'), as well as a 'right to be forgotten' (Article 17) and a data breach notification requirement (Article 32). Most importantly for current purposes, the proposal includes a PbD requirement (Article 23) as follows:

> 1. Having regard to the size of the organization and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
>
> 2. The controller shall implement mechanisms for ensuring that, by default, only those personal

> data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.
>
> 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 *for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms* referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.
>
> 4. The Commission *may lay down technical standards* for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

47 Although it takes into account the state of the art and cost of implementation, it obliges the controller of PII to implement technical and general organizational measures at the design stages of PII processing, as well as privacy by 'default' settings, itself an integral component of PbD. Beyond these generalist principles it contemplates specific technical standards to be set by the Commission. While we do not know how this will be implemented in practice, it is certain that the Proposal goes beyond the self-regulation and principle-only approaches described previously herein. The Proposal also places the obligation to monitor application and implementation on a 'Data Protection Officer' (DPO). The obligation to appoint a DPO to represent public organizations and 'large enterprises or where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring is also among the proposed changes'.[99] This requirement is not new[100] for all Member States and builds on the current Directive which contemplates the possibility of DPO appointment. To complement these changes to the framework, the potential penalties associated with breaches were increased: up to two (2) percent of annual global turnover for the gravest breaches. The coming year will shed light on the reactions to the Proposal and will provide valuable guidance on the likely development of PbD and other aspects of international privacy law.

3. United States

48 At a federal level, the US does not currently have omnibus private-sector privacy legislation. The current framework in the US is a patchwork of sector-specific state and federal level legislation. The *Commercial Privacy Bill of Rights Bill of 2011*[101] is an attempt to introduce such legislation and was brought forward by Senators John Kerry and John McCain mid-2011 as an attempt to regulate the private sector's use of PII at the federal level. The Bill has received both praise[102] and criticism,[103] but notwithstanding this early controversy, it is so far the first piece of legislation in North America to include mention of 'privacy by design' as part of a mandatory privacy framework. Although it has recently stalled somewhat, the advent of the new EU Proposal may see a rejuvenated debate surrounding this Bill.

49 Section 103 specifically mentions the term 'privacy by design':

> Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information that it collects, implement a comprehensive information 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 [...]'

50 Whether the Kerry-McCain idea of privacy by design can be considered to fulfil the principles of PbD envisioned by the Ontario Commissioner is arguable; nevertheless, its mention signals the importance of privacy considerations implemented early on in the systems design process.

51 Another US example of design-stage privacy considerations is the FTC's decision regarding Google's Buzz social media application. The FTC, under Section 5 of the *Federal Trade Commission Act,*[104] has the power to prohibit unfair and deceptive trade practices. Non-adherence to privacy policies or deceptive privacy policies has been considered deceptive by the FTC under this section, most notably in the Google Buzz case.[105] In the FTC's order, Google was ordered to maintain a comprehensive five-step privacy program (auditable by the FTC for a period of 20 years):

> A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

> B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent's unauthorized collection, use, or disclosure of covered information, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) *product design*, development, and research.
>
> C. *the design and implementation of reasonable privacy controls* and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those privacy controls and procedures.
>
> D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate privacy protections.
>
> E. the evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

52 This 'privacy program' is also somewhat of an implementation plan for PbD in that it refers to the actual design stages of systems. In a recent publication by the FTC,[106] PbD was specifically enumerated as a cornerstone of the future of privacy protection:

> First, companies should adopt a 'privacy by design' approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy.

53 The US approach focuses on organizational measures while providing individual organizations a relative large amount of leeway regarding the translation of these design requirements. While this may call itself 'privacy by design', it may not actually be a huge step beyond those laws which already exist in the EU and Canada, at least when they are interpreted broadly. Privacy by design in the US does not mean the same thing as that very same term does in the EU or Canada, as evidenced by the Kerry-McCain Bill and the language used by the FTC. What the US approach does accomplish, however, is that it specifically mentions PbD and provides a solid basis for increased personal data protection at the design stage of personal data processing systems and associated products.

C. Current Views on Mandatory PbD

54 The debate surrounding a legislated PbD requirement can be characterized by three main perspectives: 1) having PbD features embedded into systems, including mandating certain technological features such as privacy by default and PETs within those systems (advocated, *inter alia*, by the Article 29 Working Party); 2) making PbD a legislative organizational requirement to the extent that it should be adopted as a general principle of data protection law, without requiring specific regulation of specific technologies (more or less the 'US approach' described in the previous section); 3) PbD is not to become part of a legislative framework but rather as part of a self-regulatory initiative and encouraged as an industry best-practice. Some of those who hold the latter view also consider PbD redundant as it is already contained in the current legislative framework in the EU (and so therefore also Canada) and no additional burdens should be placed on industry.

55 The view that PbD should not be part of a legislative scheme is based on three main arguments: it would stifle innovation and place a disproportionate burden on economic operations,[107] it is unnecessary because it is already contained in the current framework (under Articles 6 and 17 of the EU Directive), and a legislated PbD requirement would not achieve the desired outcomes of protecting privacy but would in fact stifle the innovation necessary to drive privacy protective technologies and practices forward:

> Similarly, privacy-by-design is not something that, in itself, can be mandated by regulation. But intelligently crafted regulatory incentives can be built to encourage this movement. Instead, in today's world of global data flows, organisations need to see the value of appointing an officer in charge of privacy programmes and compliance, or in an approach to privacy risk management that seeks to engineer solutions through better product design, rather than the legalistic 'bolt-on' approach favoured today by most lawyers. The Commission must think through the most effective options for incentivising

these decisions within organisations, not simply coming up with additional prescriptive rules.[108]

56 This view is not shared equally across industry, however. Some industry players see a certain value in including PbD within the framework, at least to a certain extent,[109] so long as it does not mandate 'technological outcomes' or certification schemes.[110] The main tenor of the ICT industry remains intact notwithstanding: self-regulation is to be preferred over mandated schemes. Government's role should be to provide incentives for their adoption.[111]

57 Data protection authorities for Canada, Germany, the UK and the EU, as well as the FTC in the US, have been clear that PbD is a concept that needs to be encouraged and that is vital to the proper progress of technology that will respect the privacy rights of its users or beneficiaries. In fact, at the 2009 International Conference of Data Protection and Privacy Commissioners, a resolution was passed that PbD is an 'essential component of fundamental privacy protection'. Not all DPAs, however, are univocal in their calls for *how* PbD ought to become part of legislative frameworks around the globe.[112]

58 The 2010 'Conference of the Data Protection Commissioners of the Federation and the Länder'[113] of Germany suggested that the German data protection legislation[114] should in the future, among several other key elements, include provisions to integrate privacy into 'products and processes'.[115] This entails that not only would data controllers and data processors be legally responsible for PII but also manufacturers and designers, who would then be required to integrate data protection principles into their products. DPAs should then have the ability to audit, provide certificates of approval as well as publicly name violators. PbD was specifically mentioned as a requirement for data controllers to ensure that privacy principles were sufficiently integrated into systems before their deployment. If they were not, the data subject should then have the right to base claims on that omission.[116] That being said, it has also been acknowledged that technology-specific regulation might be a 'difficult task'[117] and that PbD might be more appropriate as a general principle across all technologies, rather than a term that is to be understood based on the technology it is attempting to regulate.[118]

59 Generally, it is obvious that the German (federal and state) DPAs would favour a PbD principle that requires technological (i.e. PETs) and organizational elements at the design stage, rather than only organizational requirements. This view is shared by the European Data Protection Authority (DPA)[119], which has stated that along with including PbD as a general principle (in conjunction with the principle of 'accountability'), PbD should be regulated more specifically with respect to RFIDs, social networks and browser applications. The Article 29 Working Party has noted that as a fundamental right under Article 8 of the ECHR, PbD is to be 'embedded' into systems. Specifically, the Working Party calls for the incorporation of *binding* rules regarding not only security of data but data minimization, PETs, privacy-by-default settings, access controls and encryption and the ability of DPAs to enforce these provisions. These rules should bind system designers, producers and data controllers.[120] The Working Party was clear that a PbD in-principle-only approach would not be enough, and any European framework should include the possibility of regulations to mandate embedded design features.

60 The UK Commissioner's views are more closely aligned with those of the US and industry than with the more prescriptive proposals of the Article 29 Working Party, the German Commissioner or now the EU Proposal. High-level principles and self-regulation are to be preferred over prescriptive or technology-specific regulations. In 'The Information Commissioner's response to the Ministry of Justice's call for evidence on the current data protection legislative framework',[121] the Commissioner noted that PbD should be included into the *Freedom of Information Act 2000*[122] as a principle but did not elaborate further on specific provisions, powers of the DPA or rights of the individual in this regard.

61 In Canada, the views on PbD are, as with some other aspects of privacy protection, a middle ground between those of the continental European nations and the Anglo-Saxon (US and UK). The IPC views PbD primarily as a 'voluntary standard'[123] aimed at achieving a high-water mark of data protection and compliance. This, however, need not be the final extent to which PbD can be utilized to achieve excellence in privacy protection. Rather, the IPC is generally in favour of incorporating PbD into legislative frameworks but 'takes no sides'[124] in the debate on what legislated PbD requirements should ultimately look like – that is, whether PbD needs to be regulated so that certain technological measures are mandated or whether organizational requirements would suffice. The Canadian Commissioner's Office similarly considers PbD a 'fundamental component of privacy protection' but has so far remained silent on whether or not *PIPEDA* should contain in-principle-only, technology-prescriptive or any PbD provisions at all.

62 Notwithstanding this generally neutral approach to legislated PbD, the IPC does note the potential of regulating specific applications, as we have seen with the inception of the Smart Grid and the biometric identification system for the welfare application system in Ontario. Some private sector businesses share the Commissioner's view of having industry, DPAs and regulators work together to achieve best practices when it comes to designing systems, in

particular where sensitive data is processed in, for example, eHealth applications and smart-meters or smart appliances.[125]

63 In a very recent publication of her office, Dr Cavoukian offered a draft legislative framework intended to provide a 'flexible but enforceable' approach to privacy protection.[126] The paper outlines current legislative initiatives and applications of PbD, not unlike this paper, in the US, EU and Canada as a precipitant to its proposed draft framework.[127] This draft is prescriptive in that it mandates a 'Privacy by design program', including specific elements of such a program,[128] but does not go as far as mandating specific and enforceable technological solutions. The proposition also does not suggest mandatory 'privacy-by-default' settings:

> Whenever reasonably possible, provide for that privacy protection automatically, so that no action is required for individual users or customers to protect the privacy of their personal information [...]

64 This notwithstanding that privacy by default is a foundational principle of PbD. Perhaps in anticipation of the logical criticism, Dr Cavoukian writes:

> In *Privacy by Design*, Privacy as the Default is the ideal condition to strive for. However, currently, the industry standard of practice for online consumer marketing is opt-out. Privacy as the Default would require a shift to 'opt-in.' But an immediate shift to an opt-in model (which is the standard of practice for sensitive information, such as personal health information) could be both impractical and, perhaps, harmful to industry.
>
> As one of the 7 Foundational Principles, *Privacy as the Default must be read alongside the remaining principles.* The fourth principle of Full Functionality (Positive-Sum, not Zero-Sum), requires that *PbD* achieve a doubly-enabling, 'positive-sum' solution that provides a win-win result for both consumers and businesses – not one at the expense of the other.
>
> Taking into account the context involved – and context is key – it is possible to develop a two-step process for achieving the spirit of Privacy as the Default in situations where the existing industry standard of practice presents a barrier to achieving the principle directly, right from the outset.

65 While reasonable, the above justification is not entirely satisfactory. That all principles ought to be read alongside one another is a fair statement, but six of the seven principles speak directly to the protection of personal data; only one, the positive sum principle, speaks to the balancing of interests between privacy and other relevant areas. The way it is described in this proposal, however, suggests that all six principles protecting information must be viewed in the context of one principle, essentially creating a two-tier system of the foundational principles, because all other principles do not require a side-by-side reading, as they naturally work together. This approach has never been advocated before and, arguably, would be a departure from what is commonly understood as PbD. At least, there is no evidence that such an interpretative approach has been taken by any other advocates of PbD, most notably Peter Schaar.

66 Ann Cavoukian's proposal makes an appropriate distinction between sensitive and less sensitive PII, as well as organization size,[129] but missing is any and all mention of developers or manufacturers of technology being truly accountable for the systems they develop (from a privacy standpoint). This is an indication that the IPC's approach to PbD may be 'Canadian' but will draw its influences from the developments in the US rather than the EU. In fact, the proposal notes its influences as the Kerry-McCain Bill, as well as Massachusetts legislation, while failing to mention either the Article 29 Working Party or the German Commissioner's recommendations in this regard.

67 Feasibility[130] aside, PbD may not have much teeth if the obligations start at the user end of the life cycle. The German Commissioner notes that PbD principles need to be incorporated into products and services if PbD is to reach its full potential.[131] The IPC's proposition is silent on remedies or enforcement processes, so one could presume that the proposition would fit into the existing framework existing in, for example, Canada's *PIPEDA* or other European legislation. It does provide specific and helpful guidelines and processes for organizations to follow as part of a PbD program.[132]

68 For organizations, the additional administrative burden could be substantial, and it would require a major change for many organizations, at least from a North American perspective. For those organizations active in Europe, the EU Directive already requires notification requirements for all automated or partially automated systems that process PII.

69 In Sweden, for example, the obligation[133] is as follows (Section 36 Swedish Personal Data Act):

> Processing of personal data that is completely or partially automated is subject to a notification duty. The controller of personal data shall provide a written notification to the supervisory authority before such processing or a set of such

> processing with the same or similar purpose is conducted.[134]

70 Such notification requirements obviously make supervisory authority of a PbD program easier, but they would be a massive change for both Canadian organizations (as well as being questionable whether a conservative government would ever condone such requirements) and the regulator.

71 Ultimately, the framework proposed by the Ontario Commissioner is straightforward and practicable. It presents a manageable middle ground between corporate flexibility and prescribed data protection technology standards, and may therefore prove to be attractive for lawmakers. The underlying rationale is surely one that will surface during the debate and consultation process surrounding the EU Proposal.

D. Analysis

> Individuals may want cyberspace to protect their privacy, but what would push cyberspace to build the necessary architectures? Not the market. [...]. Collective Action must be taken [...] and collective action is just what politics is for.[135]

72 It is clear that PbD is, no matter which stakeholders you consult in this debate, viewed as a valuable tool to a) protect data and privacy and 2) build trust in the systems, which is ultimately part of the commercial and political goal of furthering technology and its widespread use in society.

73 In order to build PbD into data protection legislation, there are clearly open matters which would require swift resolution. First and foremost, a decision would need to be made as to the manner in which this is to be achieved. Does one follow the proposed US road of organizational requirements, self-regulation or at best an in-principle-only mention in legislation or, alternatively, should PbD become an explicit integral part of law and mandate technology and standards? Or should PbD become part of *PIPEDA* or any other Canadian law at all?

74 With the current government, it is highly unlikely that the Canadian federal framework will be adjusted to incorporate PbD any time soon. As noted, Bill C-12 includes nothing of the kind. However, if the EU Proposal moves forward to include prescriptive PbD requirements, Canada may find its hand forced to follow suit, at least incrementally.[136] Then the Canadian approach might very well be one that is firmly planted in the middle between the US and European ideas of PbD. The proposal by the IPC takes elements of both approaches into consideration. The problem, however, is that divergent approaches in this regard may not be very useful, given the borderless nature of modern computing. In the best-case scenario (from a privacy compliance perspective), an international company would adhere to the strictest standard, but given that the systems approach to legislated PbD requires all actors in the supply chain of the technology to embed PbD, this may become a very real practical problem. A European company could not easily source a system from the US if different legislative requirements applied to the technology and its application.

75 The question of how older systems would be treated would also arise. The Ontario Commissioner is advocating 'privacy by re-design',[137] and it is not clear how this would fit into the legislative framework. Notwithstanding the wide array of open questions with respect to PbD and its appropriate implementation, it is quite apparent that privacy experts view it necessary to consider and embed data protection at the design stage to protect the fundamental right that is privacy. For certain applications this would include specific technological guidance for developers and data controllers without which the system could not be implemented. Whether these applications should include those mentioned in the Article 29 Working Party recommendation and in the EU Proposal may be a source for future research, but from the examples of the Smart Grid, ELENA and the biometric recognition application it is clear that there are systems that require specific solutions at their design stage such as encryption technologies, advanced cryptography in identification verification and privacy-by-default.

76 An item of particular interest would be whether the assessment of a system according to PbD principles could lead to outright prohibition. A 'prior checking'[138] requirement already exists under the EU Directive (Article 20). France, for example, has translated this requirement into an explicit 'no-go' or prior authorization statement for systems processing certain categories of sensitive data. These categories include systems where biometric or genetic data is processed as well as corporate whistleblowing systems (as applications processing potentially incriminating data or containing information could have adverse effects on the career of employees).[139]

77 Canadian federal and provincial legislation does not require notification to the authorities of systems processing PII regardless of any sensitivity. Privacy Commissioners could therefore not *prevent* a system from being deployed based on, for example, insufficient privacy design. However, via the accountable-person requirement, *PIPEDA* indirectly could prevent a system from being deployed if the accountable person was not convinced that the system complies with *PIPEDA*. If PbD formed an explicit part of the legislation, the accountable person would need to ensure that any system took privacy considerations into account at the

design stage before allowing it to go live. If the legislator provided concrete guidance on how this is to be achieved for particular potentially intrusive systems,[140] it would allow for the accountable person to benchmark more precisely. Failing to do so could then be the source of an enforceable complaint.

78 What the foregoing analysis makes clear is that compliance with PbD could potentially become complex, resource-intensive and expensive. If organizations are complaining now about the minefield that is privacy law, PbD clearly will not make it any easier. For that reason regulators must find ways to use PbD to ameliorate the appropriate risks while not focusing solely on harm and risk. Recall that data protection can also be about democratic rights and the right to determine what is done to one's information. Additionally, seemingly non-sensitive information can in the aggregate become just that.

79 Going forward, regulators must take a clear position on the importance of PbD regarding the protection of privacy. To accomplish this, PbD must first become an explicit principle of privacy law. Secondly, where the natureof the systems and sensitivity of the datademands, specific technological requirements should be legislated on top of general principles. Making PbD an explicit part of legislation only may be an important first step but would likely not be enough to ensure the desired level of protection, not to mention the fact that in-principle only would perhaps not even be a significant change from the current framework, at least that of the EU.

E. Conclusion

80 The speed at which information is being moved into digital environments and from manual to automatic processes surely requires a re-thinking of how information about individuals is collected, stored, used and then protected in these novel environments. PbD as a concept is attractive in this regard as its aim is to prevent rather than mitigate harm to PII. Instead of focusing on patching systems when data is already at risk, its focus lies in designing the architecture of the system in a privacy-respective manner. Of course, this approach is not always feasible as many organizations use systems that have been built and developed over time, long before PbD was a term of art or even long before omnibus privacy legislation existed in the EU, Canada or elsewhere. In other words, whatever the reach of PbD will be in the future, systems will require on-going privacy patches. For PbD to have the required punch, however, it needs to be explicitly mentioned in privacy legislation as well as prescribing technology-specific solutions where required. It is not enough to have PbD as an organizational best practice. This especially holds true for Canada where law does not require notification of PII processing to Information Commissioners (or explicitly to the accountable person) and systems could therefore go live without having been vetted from a design perspective. PbD is too important and effective from a data protection standpoint to stand at the periphery of a legislative framework. It should be at the core.

81 Most importantly, any legislation would need to include a process through which a system or product could be prevented from going live until it is sufficiently data protective. This must be a part of the framework in the private sector. For this to work properly, before putting a system into operation, organizations would need to submit a proposal for how the system will process personal data and for what purposes. This is where a DPO can add significant value and accountability without the organization having to communicate directly with the authorities. Some organizations are already following this best practice and, as we have seen with ELENA,[141] the application of PbD principles can lead to the abandonment of a data processing application. In the public sector, these large projects are well-known before becoming operational, but in the private sector this is obviously not always the case. Companies can design or use applications that do not have adequate protection in their architecture. The public may only know about these systems when it is too late, when personal data has been lost on account of a breach, misappropriation or leak. Again, an accountable DPO (as stated in the EU Proposal) would be a valuable link between the organization and the law to ensure that systems are designed and used compliantly. For PbD to make any sort of real difference in the way that personal data is protected, every actor in the life cycle will need to be accountable for their systems and technologies from a privacy protection perspective. Products and applications need to be brought to market with PbD embedded from conception to finalization, and organizations need to use these products to design systems that follow those same principles. It is the regulator's mandate, however, to ensure that legislative requirements are sufficiently clear and that their adherence can be tracked (and enforced). Notwithstanding this obligation, the argument that any lack of clarity on the specific meanings of PbD in every context should mean that its legislative adoption should not be encouraged, cannot stand where the right sought to be protected is as fundamental as the right to informational self-determination and to be let alone.

■

* David Krebs is currently working as Compliance Counsel for an international company located in Sweden. This article was written as part of his LL.M. at Stockholm University. The paper was presented at the "1st International Research

Forum on Law and ICT/IP" on7th / 8th of November 2012 at Georg-August-Universität in Göttingen, Germany. The Colloquium is an annual event and provides the opportunity for young researchers to present the results of their scientific work and obtain valuable feedback from senior academics and practitioners in the field of ICT and IP Law.

1 This term stems from German privacy law ('*informationelle Selbstbestimmung*'). For more on the cultural aspects of global privacy laws, see Lee Bygrave, 'Data Protection in a Global Context', in *Scandinavian Studies in Law Volume 47: IT Law,* Peter Wahlgren (ed), (Stockholm: 2004) [Bygrave] and Lee Bygrave, 'Privacy and Data Protection in an International Perspective', in *Scandinavian Studies in Law Volume 56: IT Law*, Peter Wahlgren (ed), (Stockholm: 2010) [Bygrave 2].

2 See Samuel Warren and Louis Brandeis, 'The Right to Privacy', (1890) 4 Harv. L. Rev. 193.

3 The terms 'personal information' and 'personal data', stemming from Canadian and EU law, respectively, will be used synonymously, as will the EU term 'processing' referring to the Canadian terms collection, use and disclosure.

4 Facebook serves as a prime example of where privacy considerations have been added bit by bit but were never part of the original design. On the contrary, the design was such that would allow maximum sharing with very few automatic restrictions on data transfers.

5 Privacy By Design, online: http://www.privacybydesign.ca/about/principles/.

6 S.C., 2000, c.5.

7 *PIPEDA* is Canada's federal private-sector legislation. It applies to all commercial activities involving PII as well as to employee information for federally regulated organizations (e.g. banks). In provinces that have 'substantially similar' protections, *PIPEDA* does not apply other than to federally regulated undertakings or in relation to cross-border activities.

8 EC, Commission Directive 95/46/EC on the *protection of individuals with regard to the processing of personal data and on the free movement of such data*, 1995 O.J. (L 281) 31–39 (EC) (Oct. 24, 1995), online: EurLex http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [EU Directive].

9 *Ibid.*

10 EC, *Proposal for a Regulation of the European Parliament and Council on the Protection of individuals with regard to the processing of personal data and the free movement on such data (General Data Protection Regulation)*, 2012/0011(COD) [EU Proposal].

11 US, Bill S., *Commercial Privacy Bill of Rights Act of 2011*, 112th Cong., 2011.

12 Generally described as '[...] technologies designed to give the user more control' over personal information. For example, such PETs would allow a user to retain her online anonymity. Code 2.0, *supra*, at 223-224.

13 An example of this would be the bilateral adoption of breach notification requirements. See e.g. 'Top 11 Privacy Trends for 2011', Ernst & Young, online: www.ey.com/GL/en/Services/Advisory/IT-Risk-and-Assurance/Top-11-privacy-trends-for-2011---2--Breach-notification-requirements.

14 Bygrave, supra, at 340.

15 Dr Ann Cavoukian, 'Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers' (August 2011), Information and Privacy Commissioner of Ontario, available at: www.privacybydesign.ca [PbD Whitepaper].

16 Author's note: While this paper is written from a Canadian perspective, the aim is to approach PbD in a manner that takes other laws and viewpoints into account and therefore any recommendations are targeted not only at Canadian federal legislation.

17 Lawrence Lessig, *Code Version 2.0,* (New York, 2006) at 6 [Code 2.0].

18 For such an analysis, see Avner Levin and Mary Jo Nicholsen, 'Privacy Law in the US, EU and Canada: The Allure of the Middle Ground', (2005) University of Ottawa L.& T. J. 357.

19 For example, Brazil, Chile, South Africa, inter alia, see Byrgrave, *supra* at 341 -343.

20 EC, *Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms,* [1953], European Treaty Series No. 5.

21 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

22 See *Hunter v. Southam*, 2 S.C.R. 145, 159-60 (1984).

23 Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (U.K.), 1982, c. 11.

24 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.' For a discussion on the nature of this right regarding modern communications, see Daniel Solove, *The Digital Person* (New York: New York University Press, 2004), cited in Dr Ann Cavoukian, *Privacy and the Open Networked Enterprise,* (2006).

25 In an Opinion to the Privacy Commissioner former Supreme Court Justice La Forest notes that: 'Determining whether individuals have a reasonable expectation of privacy in a given context is a nuanced, contextual, and fundamentally normative enterprise.' Gerard La Forest, 'Opinion by Justice Gerard La Forest', (April 5, 2002), *Office of the Information and Privacy Commissioner*, available at http://www.priv.gc.ca/media/nr-c/opinion_020410_e.cfm.

26 See William MacKinnon, 'Do We Throw Our Privacy Rights Out With the Trash? The Alberta Court of Appeal's Decision in *R. v. Patrick'*, (2008) 46 Alta. L. Rev. 225 [MacKinnon].

27 See Levin, *supra*.

28 [1988] 2 S.C.R. 417 at para. 34.

29 R.S., 1985, c. P-21.

30 Alberta, British Columbia, Ontario and Quebec have private sector legislation, and most other jurisdictions have public and sector-specific legislation, such as in Saskatchewan, Manitoba, Ontario and Alberta where legislation protecting personal health information is in force.

31 See *Byrgave*, *supra*, at 326-331.

32 Levin, *supra*, at 392.

33 See Levin, *supra*, and Lanois, *supra.*

34 These tracking devices have a range of applications and can be found in consumer goods and used by retailers to track the supply chain, but also for highway tolls and in public libraries. The privacy implications stem from the fact that these tags can collect, store and transmit PII as well as track locational data of the device (and therefore, potentially, the individual associated with a device containing an RFID). For more on RFIDs and a detailed analysis of RFIDs and *PIPEDA*, see Teresa Scassa et. al, 'An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies', (April 28, 2005), University of Ottawa, online: http://commonlaw.uottawa.ca.

35 Information and Privacy Commissioner of Ontario, 'Privacy by Design: The 7 Foundational Principles, (August 2009, revised January 2011), Information and Privacy Commissioner of Ontario, online: http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

36 Dr Ann Cavoukian, 'The 7 Foundational Principles', Office of the Information and Privacy Officer, online: www.ipc.ca.

37 See a complete list of all ambassadors at Privacy by Design, online: http://privacybydesign.ca/ambassadors/individuals/page/3/.

38 Peter Schaar, 'Privacy by Design', (April 1, 2010), Springerlink, online: http://www.springerlink.com.

39 A good example of the win-win or 'positive-sum' approach advocated by the Ontario Commissioner's Office (IPC) is the use of advanced cryptography for user identification. Contrary to the often-advocated theory that security and privacy consideration are intrinsically at odds with one another – misconceptions often rooted in an ignorance of the modern technologies – modern technology can in fact cater to both sides of the coin. In this example, use is made of a trusted third party who, during a one-time certification stage, issues separate randomly generated ID tokens to be used vis-à-vis certain service providers requiring secure identification, and embeds all of these tokens (contained in a smart chip) with an invisible 'master' ID key. Where required, the IDs can be shared across service providers without any one party knowing or being able to trace the IDs back to the individual. Information is always a) controlled by the individual and b) limited to the identification parameters that the service provider requires. See Stefan Brands, 'Secure User Identification Without Privacy Erosion', (2006) University of Ottawa L.& T. J. 205 [Brands].

40 Such as the secure ID tokens described in Brands, *supra*.

41 See Bygrave 2, *supra*, at 169, for a comparative analysis of the cultural aspects underlying privacy laws.

42 Cavoukian, Ann, PhD, *Privacy by Design in Law, Policy and Practice: A Whitepaper for Regulators, Decision-makers and Policy-makers*, (August 5, 2011), online: http://privacybydesign.ca.

43 Seda Gurses et al., 'Engineering Privacy by Design', (2011), Computers, Privacy and Data Protection (CPDP 2011 Conference) available at http://www.cosic.esat.kuleuven.be/publications/article-1542.pdf [Gurses].

44 *Ibid* at 5.

45 Smart Grid Canada, available at http://sgcanada.org/smartgrid/what-is-a-smart-grid/: 'allows utilities to distribute conventional and renewable power to consumers more efficiently, reliably, safely and economically. It integrates two-way digital communication technology that analyzes, monitors and streamlines the system to maximize throughput, while promoting and enabling a reduction of overall energy consumption.'

46 Dr Ann Cavoukian, 'Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid', (2010), Privacy by Design, online: http://www.ipc.ca.

47 Sebastian Knab et. al. 'Smart Grid – the Central Nervous System for Power Supply', (2010), *Scientific Series of the Innovation Centre Energy at the Technische Universität Berlin, Vol. 2, University Press, Berlin, Germany,* available online at SSRN, http://ssrn.com/abstract=1531655.

48 BC Hydro, online: http://bchydro.com/energy_in_bc/projects/smart_metering_infrastructure_program/smart_meter_installation.html.

49 Knab, *supra*.

50 'Monitoring a consumer's energy use in near real time, a smart meter delivers incremental consumption data and pricing.' From Smart Grid Canada, *supra*.

51 IT Law Wiki, available at http://itlaw.wikia.com/wiki/Smart_appliance: 'A smart appliance is an appliance that may be configured to communicate information directly to the utility operator for efficient and more productive use of electricity.'

52 Elias 'Smart Metering and Privacy: Existing Law and Competing Policies', (2009), *University Colorado Law School – CEES*, Working Paper Series, available at SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1462285. These include services like energy efficiency monitoring and home load management.

53 *Ibid*, at 12.

54 National Institute of Standards and Technology, 'NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0', (January 2010) at 118-119.

55 *Ibid*.

56 Information and Privacy Commissioner of Ontario, 'Operationalizing Ontario's Privacy By Design: The Ontario Smart Grid Case Study', (February 2011), Privacy by Design, available at http://www.ipc.on.ca/images/Resources/pbd-ont-smartgrid-casestudy.pdf [Smart Grid Case Study].

57 In British Columbia, for example, meter installations began in July 2011, and it is estimated that by the end of 2012 all residential customers will have their meters upgraded to smart meters.

58 Ontario Smart Grid Forum, 'Modernizing Ontario's Electricity System: Next Steps. Second Report of the Ontario Smart Grid Forum', (May 2011, at 7-8).

59 For example, increasingly efficient and precise ways of collecting meter data for precise load forecasting.

60 See Smart Grid Case Study at 16.

61 'Privacy Concerns Surround Ontario's Smart Grid Plan', (11 May 2010), online: www.cbc.ca/news/technology/story/2010/05/11/cavoukian-privacy.html.

62 An electronic signature based on a qualifying certification agency's certificate. See Footnote 67 below.

63 Wikipedia, 'ELENA-Verfahren', Wikipedia, available at http://de.wikipedia.org/wiki/ELENA-Verfahren, last accessed on 15 October 2011.

64 Peter Schaar, *supra* note 27.

65 Press Release, 'ELENA Verfahren wird eingestellt' (translated: ELENA process will be discontinued), Bundesministerium für Arbeit (German Ministry of Labour), online: BMWi, http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=424742.html.

66 Defined as 'an advanced electronic signature based on a qualified certificate and created using a secure signature creation device' in Cecilia Magnusson Sjöberg & Anna Norden, 'Managing Electronic Signatures', *Scandinavian Studies in Law Vol. 47: IT Law*, ed. Peter Wahlgren, (Stockholm: 2004), at 84. An advanced electronic signature is one created using so-called Public Key Infrastructure, which ensures the integrity and authenticity of a signature using one private and one public key and a certification authority 'vouching' for the link between the private key and a flesh and blood individual.

67 'Bundesregierung beerdigt Arbeitnehmer Datenbank', T-Online, online: http://wirtschaft.t-online.de/elena-bundesregierung-beerdigt-arbeitnehmer-datenbank-elena-/id_48125142/index.

68 In that recommended changes were built into the DNA of the system and processes.

69 See Dr Ann Cavoukian, 'Privacy and Biometrics: An Oxymoron or Time to Take a 2nd Look?', (1998), Information and Privacy Commissioner Ontario, online: http://www.ipc.on.ca/english/Resources/Presentations-and-Speeches/Presentations-and-Speeches-Summary/?id=98: The City of Ontario at the time had been worried about citizens applying for benefits on multiple occasions on the same bases through the use of multiple identities.

70 *Social Assistance Reform Act, 1997, O.Reg. 226/98*.

71 1997, S.O., c-25, Schedule A.

72 1997, S.O., c-25, Schedule B.

73 *Ontario Works Act, s.74(3).*

74 This is the key difference between sensible security or privacy protective measures and PbD, which takes these sensible measures, forces their application on the design of the system and makes it a requirement that is done alongside the other technical design stages of a system.

75 Lawrence Lessig, *Code, 2.0, supra*, at 232.

76 It is an example of a way to satisfy Principle 4.7.1 (see e.g. PIPEDA Case Summary #2003-185) of *PIPEDA* but not an explicit requirement.

77 In British Columbia, for example, the private-sector act is intended to cover the health sector.

78 This statement must be viewed in the context of a comparison with the landscape in the EU. There are indeed differences within Canada as to how PII may be used, collected and disclosed, but the manner in which the private sector is regulated by *PIPEDA* and provincial legislation is cohesive in that common principles and a common culture underlie the regulations. See e.g. David Krebs, 'Regulating the Cloud: A comparative analysis of the current and proposed privacy frameworks in Canada and the European Union', (to be published in the Spring 2012 Volume of the CJLT).

79 Canadian Standards Association, online: http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code. The CSA is the Canadian agency responsible for the collection and publishing of applicable standards in Canada.

80 *PIPEDA* Report of Findings #2011-001. See also discussion in PbD Whitepaper, *supra* at 27. The Commissioner instigated the complaint for data collected without knowledge or consent of the individual, beyond the purposes required and without identifying and disclosing the purposes of the data collection by way of Google's Street View cars.

81 Principle 4.1.

82 Ss. 15-16.

83 1st Sess., 41st Parl., 2011.

84 In order to be able to transfer data outside of the EU, the recipient country must have 'adequate' data protection laws (Art. 25 EU Data Protection Directive). Currently, *PIPEDA* is considered 'adequate', but this could change if the two frameworks do not continue to be similar in their protections.

85 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002.

86 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006.

87 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

88 1998:204 PuL (Swedish Personal Data Act) [Swedish Personal Data Act].

89 Cecilia Mangusson Sjöberg et al., *Rättsinformatik*, (Studentlitaratur: Lund, 2011) at 31.

90 (UK), 1998, c. 29.

91 E.g. Privacy by Design, *supra*.

92 One must remember at this point that under civil law, recitals and even preparatory works have a higher legal status than under Canadian common law. In Sweden, for example, courts often consider these to carry a great deal of weight. See Samuel Engblom, *'Regulatory Frameworks and Law Enforcement in New Forms of Employment: National Report: Sweden'*, Report to the XIX World Congress of Labour and Social Security Law (Sydney 2009), TCO, online: http://www.tco.se/56e6d647-e578-41dc-947f-2775c4f8fcfe.fodoc.

93 WP 168.

94 Under EU law, a 'controller' is the legal person that identifies and determines the purposes of the PII that is processed. A 'processor' is a legal person that may process PII under the direction of the controller. Separate legal obligations apply depending on this determination. See definitions within EU Directive, *supra*.

95 WP 168 at 13.

96 PbD regulation at 19.

97 EC, *Proposal for a Regulation of the European Parliament and Council on the Protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation)*, 2012/0011(COD) [Proposal].

98 The current Directive states that 'Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes' unless a DPO is appointed who maintains a register of systems or 'where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored.'

99 Arts. 35 – 37.

100 This would not be new for all Member States. Sweden, for example, already has a similar requirement.

101 US, Bill S. 1, 112th Congress, 2011.

102 See 'Joint Statement on Commercial Privacy Rights', *Ebay Mainstreet*, (11 April 2011), online: Ebay Mainstreet, http://www.ebaymainstreet.com/files/Joint-Statement-on-Commercial-Privacy-Bill-of-Rights-April-12-2011.pdf.

103 'Consumer Groups Welcome Bipartisan Privacy Effort, But Warn Kerry-McCain Bill Insufficient to Protect Consumers' Online Privacy', *Consumer Watchdog* (12 April 2011), online: Consumer Watchdog, http://www.consumerwatchdog.org/newsrelease/consumer-groups-welcome-bipartisan-privacy-effort-warn-kerry-mccain-bill-insufficient-pr.

104 15 U.S.C. § 45.

105 Consent Decree, Agreement containing consent order, File No. 102 3136 http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

106 Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change', December 2010, online: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

107 See e.g. World Federation of Advertisers (WFA), *Submission to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, online: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm.

108 Vodafone, *Vodafone's Response to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm at 6.

109 See e.g. Microsoft, *Submission to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm: 'Microsoft supports an industry-wide PbD obligation applicable to the ICT industry to take account of privacy principles, including notions of data

minimisation, transparency, user control, use limitation, and related principles, in the development and deployment of new technologies. As with accountability generally, it is important that we reach a common understanding of what PbD entails, however. PbD obligations should not take the form of design mandates or technology preferences, for example. Indeed, it would be undesirable for privacy rules to dictate specific technological outcomes – including 'privacy by default' – which will only impede the development of new technologies without guaranteeing stronger privacy protections. PbD obligations for any given technology should be proportionate to the privacy risks to the consumer; program assurance should place an emphasis on trustworthy internal checks and balances and limit reliance on third party audits and mandatory privacy certifications, which often impose significant costs with little concomitant benefit (to the extent external validation is necessary, it should be reasonable in scope and affordable); and there must be clear benefits for those companies that submit to higher levels of validation to demonstrate trustworthiness.' Also see European Networks, Response to *the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm.

110 *Ibid*.

111 See e.g. Facebook, *Submission to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm.

112 I would contend that this is at least partially attributable to the notion of privacy *rights* and the differences across cultures. For more on this topic, see Bygrave, *supra*.

113 Conference of the Data Protection Commissioners of the Federation and the Länder, *Modern Data Protection for the 21st Century,* The Data Protection Commissioner of Baden-Württemberg (18 March 2010) [2010 Conference].

114 *Bundesdatenschutzgesetz*, (BGBl.I 1990 S.2954) [BDSG].

115 2010 Conference, at 6.

116 *Ibid* at 9.

117 Opinion of the Federal Commissioner for Data Protection and Freedom of Information, email correspondence with David Krebs (5 August 2011).

118 *Ibid*, opinion of the German DPA.

119 European Data Protection Supervisor (Peter Hustinx), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union'*, 14 January 2011 at para 114.

120 Art. 29 Data Protection Working Party, *The Future of Privacy*, 02356109/EN, WP168 (01 December 2009) [WP 168].

121 Available at Information Commissioner's Office, online: http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx.

122 2000 c. 36.

123 PbD Whitepaper, *supra*, at 21. These voluntary codes can, of course, be either in-principle-only or technology prescriptive.

124 Email correspondence with Gail Puder, OPC, (April 2011).

125 See e.g. General Electric Company, Submission *to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm at 10.

126 PbD Whitepaper, *supra*.

127 It was published before the EU Proposal was finalized and did not consider its implications.

128 'A comprehensive *Privacy by Design program* must include the following elements: (1) An organization shall establish a *Privacy by Design* leader and/or team by identifying the appropriate directors, officers, and managers responsible for developing, maintaining, implementing, and updating proactive *Privacy by Design* processes and practices; (2) Proactive *Privacy by Design* processes and practices shall: (A) Apply to the design and architecture of infrastructure, IT systems, and business practices that interact with or involve the use of any personal information; (B) Describe each of the core purposes served and main functions delivered by those infrastructures, systems and practices, including but not limited to the provision of security and the protection of privacy in personal information; (C) Incorporate data minimization and provide the highest degree of privacy protection for personal information possible while serving the other core purposes and delivering the other main functions; (D) Provide this degree of privacy protection by employing the maximum feasible means needed to ensure the security, confidentiality, and integrity of personal information throughout the lifecycle of the data, from its original collection, through to its use, storage, dissemination, and secure destruction at the end of the lifecycle; (E) Whenever reasonably possible, provide for that privacy protection automatically, so that no action is required for individual users or customers to protect the privacy of their personal information; (F) Ensure that infrastructure, IT systems, and business practices that interact with or involve the use of any personal information remain reasonably transparent and subject to independent verification by all relevant stakeholders, including customers, users, and affiliated organizations; and (G) Emphasize the design and maintenance of user-centric systems and practices, including strong privacy defaults, appropriate notice, and other user-friendly options.

129 'Each organization shall, in a manner proportional to the organization's size, scope, and resources and the size, type, and nature of the *personal information* that it collects, implement a comprehensive *Privacy by Design* [...]'.

130 This method of regulating raises a number of concerns. First, to what standard will organizations be held and how enforceable will this standard be? Further, how will the separate but connected obligations of system designers, purchasers and data controllers be enforced (that is, to what extent will a data controller be accountable for a designer's adherence to the systems)? External certifications and internal control processes will surely play a role in this, but given the complexity of the technology today, data controllers may well have to rely on system designers to guarantee that certain principles are adhered to. For example, when it comes to complex encryption technologies to ensure secure authentication and access controls, it may not be feasible to require the business to understand the algorithm underlying a Public Key Infrastructure encryption tool, but only a certificate that the algorithm meets the requirements of data protection laws.

131 Peter Schaar, *supra* note 27 at 1.

132 'In support of a comprehensive *Privacy by Design* program, an organization must: (1) Provide appropriate privacy and security training to its employees; (2) Implement a system for tracking all projects that regularly collect, use or store personal information; (3) Require project leaders to draft, maintain, submit and update Privacy Design Documents for all projects in order to help ensure product, program or service teams assess the privacy impact of their products, programs and services from inception through launch; and (4) Assign an internal audit team to conduct periodic audits to verify the

completion of selected Privacy Design Documents and their review by the appropriate managers.'

133 Although Sweden is not a jurisdiction that has traditionally enforced provisions such as the above, the PuL contemplates a fine or imprisonment of up to two years for grave breaches (Section 49).

134 Translation taken from Swedish Government Offices English language version of the Act, online: http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf.

135 *Code 2.0*, *supra* at 232.

136 The Proposal maintains the current restrictions (Art. 25 of the EU Directive, supra) on data transfers to countries that do not have 'adequate' legislation in place. Canada is currently considered 'adequate' and transfers to Canada can be conducted from EU Member States without any other special exemptions (BCRs, mandatory contractual clauses),, but it could be that in order to maintain this classification, Canada would need to move forward in the same manner.

137 See Privacy by Design, online: http://privacybydesign.ca.

138 1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof. 2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority. 3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

139 *LOI n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (Art. 25).

140 E.g. social networking, RFID, Smart Grid.

141 In France, a whistleblowing system was just recently struck down even despite its prior authorization from the French DPA (the 'CNIL'). See Hogan Lovells, online: http://www.hldataprotection.com/2011/10/articles/international-eu-privacy/french-court-of-appeals-reject-companys-whistleblower-system-despite-cnil-approval/.