Privacy-invading technologies : safeguarding privacy, liberty & security in the 21st century

Klitou, D.G.

10 Overall conclusions & policy recommendations

10.1 CHAPTER INTRODUCTION

Section 10.2 outlines the challenges lawmakers face in order to keep up with technological development. Section 10.3 further explains how PBD, as the critical combination of law and technology, is a solution. Section 10.4 clarifies that PBD is not a substitute for law. Section 10.5 explains the need to balance flexibility with specificity. Section 10.6 proposes PBD legislation as a radical solution to counter the radical capabilities of the latest PITs. Section 10.7 and Section 10.8 provides an overview of the mechanisms and steps for implementing and enforcing the proposed legislative solution. Section 10.9 proposes a certification-scheme for PBD. Section 10.10 explains the requirements for designing for privacy, while Section 10.11 outlines what constitutes adequate PBD. Section 10.12 outlines the negative effects of overregulation and overprescribing the PBD solutions. Section 10.13 argues how PBD could increase the deployment and innovation of technologies. Section 10.14 sums up how PBD can jointly safeguard and enhance privacy, liberty and security in the 21st Century. Section 10.15 clarifies the continued need for privacy-friendly alternatives, regardless of PBD. Section 10.16 counters some potential criticism of PBD. Section 10.17 outlines some recommendations to overcome the practical challenges of PBD. Section 10.18 explains the need to engage stakeholders and other relevant actors to further overcome the challenges and realize the potential of PBD. Section 10.19 clarifies that PBD, while it may be an effective solution, is not a panacea. Section 10.20 sums up the final overall conclusions of the dissertation.

The overall problems, root causes, objectives, recommendations and countermeasures addressed by this dissertation are mapped out and summarized in an *A3 Report* (see: Annex I). Once again, it is important to note that the A3 Report was developed only after the overall research findings and conclusions were established. Moreover, the overall conclusions, which are elaborated in more detail and brought into focus in the subsequent sections, are based on the analysis and conclusions from the case studies.

An overview of the intrusive capabilities of the specific PITs addressed and the corresponding most relevant laws and self-regulations, legal deficiencies, and proposed key recommended legal and technological solutions are outlined in a summary table (see: Annex II).

10.2 KEEPING UP WITH THE TECHNOLOGY.

PITs, with ever-greater intrusive capabilities, will likely always evolve faster than privacy/data protection laws. The speed of lawmaking has essentially been (and will likely continue to be) slow, while the speed of technological development, innovation and deployment has been increasingly rapid. A single innovation can lead to multiple innovations, which in turn can lead to exponentially more innovations. And, for every new, innovative PIT developed/deployed, the law is even further behind the technology.

Privacy/data protection laws, applicable only to data controllers and users of PITs, are probably much less able to withstand the new technological developments. However, the rapidly changing and advancing nature of technology is not a justification for not being able to equip the law with the practical means of standing a better chance of adequately defending the right to privacy and other civil liberties. For far too long, the difficulty of keeping up with technology has brought some doubt over the ability of lawmaking/policymaking to do something concrete to ensure privacy. This skepticism has also perhaps partially led to politically delegitimizing or foiling, especially in the US, legislative attempts to pass new and comprehensive privacy laws.

On the other hand, as demonstrated through the case studies, privacy/data protection laws, directly applicable to the manufacturers/developers of PITs, are better suited to more effectively safeguard privacy and liberty against the threats posed by existing technologies and future and emerging technologies. But, before the adoption of new policies and laws can be achieved, lawmakers and policymakers need to be influenced and convinced, through concrete solutions and validated real-life demonstrations, that privacy can be engineered into PITs. By providing the actual ability to take concrete steps, PBD can offer the necessary preconditions for addressing privacy concerns on a political and economic level (Agre and Rotenberg, 1997).

10.3 PBD: A CRITICAL COMBINATION OF TECHNOLOGY AND LAW

Privacy is not just a policy, theoretical or legal issue that can be maintained with purely legal or policy-orientated solutions. Privacy laws are only as good as the controls, means or measures for implementing those laws and, therefore, in order to realize the promise of the privacy laws, the practical implementation is required. If not effectively implemented, law, no matter how strict or comprehensive, is just a 'paper tiger'. As the Article 29 Working Party similarly argues, "[d]ata protection must move from 'theory to practice'. Legal requirements must be translated into real data protection measures".[916] Or, as Reidenberg (2000) argues, "law is necessary to establish the public policy objectives, but insufficient to assure the implementation of fair information practices".

The minimization of the threats/risks posed by the highly intrusive capabilities of PITs will likely continue to prove farfetched and difficult to realize, without practical measures and by relying solely on the behavior of people to comply with the law and to appropriately use PITs. After all, no matter how strict and comprehensive privacy laws are formulated and how unambiguously the right to privacy is delineated and interpreted, there will always be attempts to violate those laws and infringe upon the right to privacy. In response, practical measures in the form of technological and design (PBD) solutions can bolster the law and better ensure or even almost guarantee its compliance. Solutions or fixes based on technology, code and architectures are, therefore, critical.

Essentially, in terms of privacy and other civil liberties, technology can be both a threat and a solution. In other words, technology can provide the powerful instruments of surveillance and privacy intrusion, but also the effective controls over these activities. For all four PITs (i.e. case studies) specifically addressed, technical or design solutions/measures played an important, often essential, role in regulating and minimizing the threats to privacy and individual liberty. Indeed, the proposed recommendations to enhance the legal frameworks in the US and UK are based heavily on technological or design solutions for implementing existing privacy principles and laws, and the creation of new laws that require these solutions be implemented.

For body scanners, it is essential that the devices do not generate images that are unnecessarily graphic, which can be accomplished using software algorithms, and that the devices have restricted storage capabilities. For CCTV microphones, it essential that the technology used is not capable of recording conversations out in public, without first being legitimately triggered by certain sounds using artificial intelligence. For CCTV loudspeakers, it is essential that their design does not give control room opera-

---

[916] Article 29 Data Protection Working Party, WP 173, Opinion 3/2010 on the principle of accountability, 13 July 2010, p. 3.

tors the capability to say whatever they want from afar and out loud. It is also important that their use is automatically tracked and logged. And, for HIMs, marketed and sold for human implantation, without technological approaches, protecting the privacy of RFID or GPS implantees will be incredibly difficult. It is essential that RFID implants possess strong encryption and it is important that the privacy principles are incorporated at the "reader-to-tag protocol level". It is also important that implantees are able to set 'privacy preferences', where appropriate, which is only possible through technological approaches.

Furthermore, the ubiquitous information society, which HIMs and other RFID applications could form a key part of, will bring about difficulties to preserve privacy without PBD solutions or built-in privacy awareness (see Langheinrich, 2001). PBD will especially be imperative in a ubiquitous information society, where it will likely prove difficult to determine all the responsible entities and to enforce privacy/data protection laws in the traditional way. PBD will also be evermore important as ICT becomes increasingly pervasive and entrenched within society and everyday life, from the deployment of smart electricity meters and smart electricity distribution grids[917] to e-health, e-commerce and e-government applications.

Privacy is just too important to solely rely on operators of PITs and data controllers to uphold the principles of privacy. Technology more than likely can do a better job. Operators and data controllers comply with privacy laws and principles irregularly, inconsistently, subjectively, manually and with errors. Operators or controllers, whether private or public, and service providers are either prone to make mistakes in handling personal data or are prone to abuse or misuse the powerful intrusive capabilities of PITs, both of which have reportedly occurred countless times, not to mention those incidents that have gone unreported. Technology, on the other hand, in theory, can apply privacy laws and principles constantly, consistently, objectively, mechanically and without errors, improving both the rate and quality and effectiveness of privacy compliance. Rather than solely regulating the ways in which the capabilities of technology is used, with PBD those capabilities are regulated and minimized in the first place.

In addition, as the Article 29 Working Party again similarly points out, data controllers (i.e. private enterprises and public sector bodies) are often merely users of ICT and

917 The white paper from the Future of Privacy Forum, *SmartPrivacy for Smart Grids: Embedding Privacy into the Design of Electricity Conservation* (November 2009), argues in favor of implementing PBD for smart grids and warns about the threats to privacy posed by smart grids. For example, as the white paper points out, by revealing what appliances and devices a household uses, how much and when, the electricity provider can determine personal habits, behaviors and lifestyles. There are indeed legitimate privacy concerns surrounding smart grids that should not be simply overlooked, but the full privacy implications of smart grids are unknown, and therefore PBD here is a key preventive measure.

can hardly be considered in a position to take any relevant security or data/privacy protection measures by themselves even if they wanted to.[918] More appropriately, therefore, requirements should fall on the ICT manufacturers/developers.

Besides, in an emerging ubiquitous information society, where ICT deployment and use is increasingly pervasive, it will only become even harder to know who are all the data controllers and, thus, more difficult to always determine who should be held accountable. The enforcement and effectiveness of privacy laws, like in any legal field, requires the capacity to allocate responsibility to the appropriate parties for complying with the relevant regulations and to hold those accountable who fail to comply. Therefore, not being able to determine the responsible data controllers in an increasingly ubiquitous information society will substantially weaken the function and meaning of the privacy laws and principles.

Shifting the focal point of obligations to the developers/manufacturers of PITs and putting less weight on the operators and data controllers is also particularly important in public surveillance terms, for example with regards to CCTV microphones and loudspeakers and RFID/GPS implants, since there seems to be no clear way of determining the extent to which privacy exists in public, especially when public surveillance technologies are so widespread and many argue that there is no privacy out in public. Furthermore, PBD will become even more critical as the deployment of ubicomp, AmI and the Internet of Things/Internet of Persons becomes a reality causing the extreme difficulty of implementing the legal requirements and the privacy principles, such as the principles of consent/choice and notice/awareness, within public settings. Essentially, exercising choice in an unregulated (or inadequately regulated) ubiquitous information society means making a decision between going out in public or staying home or becoming a "digital hermit",[919] and this is not really a choice at all.[920]

PBD is also especially critical for protecting privacy in a world of increasing cross-border data flows, for example, as a result of the increase in 'cloud computing', global databases and online social networks. This problem is especially accentuated, since different legal jurisdictions have different degrees of adequacy in data protection rules. As Reidenberg (2000) points out, "the inevitability of conflict between comprehensive legal standards, as found in Europe, and ad hoc protections, as seen in the United States, place the issue of fair treatment of personal information at the center of global information

---

[918] see Article 29 Working Party, The Future of Privacy, 1 December 2009, WP 168.

[919] see Cave, J., et al. *Trends in connectivity technologies and their socio-economic impacts*, Final report of the study: Policy Options for the Ubiquitous Internet Society, (RAND Europe, July 2009), p. 19.

[920] *Ibid.*

transfers". PBD can better ensure the consistent protection of personal data, to a certain extent, regardless of geographic location, legal jurisdiction or the adequacy of the legal framework, since "mechanisms that automate the implementation of data policies will facilitate uniformity across the areas of law and marketplace" (Reidenberg, 2000).

Therefore, in summary, PBD is imperative when the legal questions are left wide open, the legal solutions are ambiguous or extremely difficult to enforce/implement or when essentially there are no applicable laws or those laws are inadequate.

Nevertheless, at present the technical emphasis, found both in law and industry standards (such as ISO/IETF 27000-series, ISO/IEC 17799:2005(E) and ISO/IEC 13335-1:2004), is all too often focused on data security. While data security is an important element in privacy protection, it is just one principle of protecting privacy and not the whole picture. As a result, there is a lack of guidance, rules and established industry standards on the technical solutions to ensuring privacy overall,[921] whether concerning one's body, activities or behavior out in public.

There are indeed legal provisions that mandate technological solutions, but, for the most part, they emphasize only data security. An emphasis on data security is especially not sufficient to address the type of threats posed by the latest PITs. As outlined, many of the latest PITs pose a threat to privacy beyond the consequences of unauthorized access to personal information. The ability to see through clothes or walls, listen and record public conversations, conduct wide-area aerial surveillance, perform brain scans or get into people's heads, and constantly track people's movements are just a few examples of privacy threats that data security nor information privacy alone can nowhere near adequately address. Moreover, given the legal requirements for safeguarding privacy and the different privacy risks, the law must significantly go beyond legal provisions that only mandate technical solutions for data security (Borking, 2010). Therefore, *privacy* by design is what is called for and not just data security by design. Besides, a mere emphasis on data security alone to address privacy threats implies that it is basically always legitimate to collect personal data, as long as it is kept secure.

Where applicable, a holistic approach must be taken, whereby all the privacy principles are incorporated into the design of the system or device concerned. As opposed to only emphasizing on the security of personal data, the technical solutions should, for instance, also control what personal data may be collected or accessed, when and how it may be collected and accessed, for how long it may be stored, and provide data subjects the means to access their stored personal data.

---

[921] see Online consultation comments on the European Commission staff paper "Early Challenges to the Internet of Things", Comments submitted by CA, Inc., p. 6, available at: http://ec.europa.eu/information_society/policy/rfid/library/index_en.htm

Without taking into consideration the other principles of privacy, within the design and functionality of the relevant system or device, a diminishing realization or viability of those principles will eventually result. For example, with regards to the access/participation privacy principle, while a data subject's right to request access to the information stored on them by a data controller is provided for within, e.g., Directive 95/46/EC, the implementation of this right will likely be too difficult, impractical or costly, if the relevant system has not been designed or developed in the first place to execute this request efficiently and cost-effectively.

The principles of privacy protection must be built into PITs all at once, where applicable, before their deployment and activation, as opposed to merely bolting them on in a piecemeal, incremental approach sometime after the threat arises. As van Blarkom, G.W. et al., argue "the postponement of dealing with personal data implications 'until a later phase', may easily lead to an information system that is contrary to privacy adaptations" (van Blarkom, G.W. et al., 2003, p. 8). "Certain measures may have been necessary very early on when developing the system before much of this system has been 'cast in stone'" (*Ibid.*). We have already seen the problem with, for example, Google Street View's approach to ensuring privacy by blurring faces and license plates after the images were generated, the service was put online, complaints were made and the damage had already been done. Unsurprisingly, this approach still more than likely leaves tens of thousands of people still potentially identifiable, especially if the ability to zoom in extensively exists. The zoom in capability also allows users to look into people's homes. Instead, a method of ensuring all the privacy principles, where applicable, should have been automatically applied at the moment *when* the images were being generated by the special cameras on Google's Street View vehicles.[922] We have also already seen the consequences of developing the Internet without privacy and security issues fully taken into consideration at the very beginning. Perhaps, if the Internet was designed and developed with privacy/security taken into consideration, some of the significant cyber-security challenges we increasingly face today would have been minimized. As ICT increasingly becomes evermore pervasive, hopefully the ICT industry will not repeat the same mistake with the development and deployment of RFID applications, neurotechnology applications, software agents, intelligent transportation systems and smart electricity distribution grids.

PBD can potentially address almost any threat to privacy at the earliest possible stage of a PIT's lifecycle – i.e. during the research, design and development stages. Accordingly, the built-in technical solutions should be realized before the PIT is deployed

[922] The lack of privacy considerations when developing Google Street View has also likely brought about the fact that Google's Street View vehicles have also reportedly collected data transmitted on private, non-secure Wi-Fi networks.

and in use, rather than addressing the corresponding privacy threat with a hodgepodge of technological band-aids hastily stuck on after the injuries to privacy could occur or have already occurred. In other words, PBD is not about decorating a cactus tree to look like a Christmas tree that will likely prick you anyhow; it is about growing that Christmas tree. As argued in the European Disappearing Computer Privacy Design Guidelines, which forms a part of the 'Ambient Agoras' project coordinated by the Integrated Publication and Information Systems Institute (IPSI) of the German Fraunhofer Gesellschaft (FhG), "[p]rivacy enhancement is better obtained by actively constructing a system exactly tailored to specific goals than by trying to defend ex-post a poor design against misuse or attacks".[923]

However, neither law nor technology alone can ensure privacy is maintained and both are not self-sufficient (Reidenberg, 2000). As Reidenberg (2000) further argues, both *forms of regulation* "embody inherent limitations that preclude adequacy for effective protection of privacy". Therefore, a combination or mixture of law and technology is required to safeguard privacy. PBD is that *critical combination* of law *and* technology.

10.4 NOT A SUBSTITUTE FOR LAW

Indeed, while PBD may significantly ease the dependence of privacy/data protection on user-level regulations and the compliance thereof, legislative instruments or other legal instruments will not simply become obsolete with technological solutions. As Bruce Schneier, a renowned security technologist and author, similarly points out, while technology is key to protecting privacy, in the end, as Schneier emphasizes, privacy boils down to the existence of laws and legal protections.[924] PBD solutions (nor computer code) are not a substitute or replacement for law, but rather are complementary to law. Advocates of PBD do not propose to replace lawmakers with computer programmers or engineers. Similarly, computer code, when used to enforce privacy/data protection laws, does not become law, but remains as the technical means to enforce the laws (see Dommering, 2006). For instance, as Schwartz argues, a technical solution like P3P is necessary to provide the machine-to-machine protocol to enable a web browser and website to negotiate privacy standards, but laws are also necessary to require that those

---

[923] Lahlou, Saadi. and Jegou, Francois. *European Disappearing Computer Privacy Design Guidelines*, Version 1, Ambient Agoras Report D15.4, Disappearing Computer Initiative (Oct. 2003), p. 4.

[924] Schneier, Bruce. "Strong Laws, Smart Tech Can Stop Abusive 'Data Reuse'" (Wired News, 28 June 2007), available at: http://www.schneier.com/essay-175.html

negotiations take place (2000, p. 759). Besides, PBD should be based on law (see, e.g., Hildebrandt and Koops, 2010).

As far as possible, technological/design solutions for protecting privacy aim to minimize the intrusive capabilities of the technology concerned and to realize the fundamental principles of privacy. The solutions, however, will often not be able to entirely eliminate the privacy-intrusive capabilities of all PITs, and some solutions will be vulnerable to hackers. Moreover, since certain PITs will need to be intrusive, e.g. for law enforcement purposes/surveillance activities, constitutional and other legal protections will, thus, still need to be significantly relied upon.

Thus, PBD solutions, in the end, are just as important as the laws, rules, regulations, principles and norms that mandate or require these solutions be implemented, influence the end result of PBD, provide the legal control mechanisms to intervene in the chain of production, specify the liability of not complying, punish those who illegally hacked or intentionally circumvented the PBD-based solution, ensure transparency and establish the enforcement and audit mechanisms. There will also certainly still be a need to regulate human behavior or the ways in which PITs are deployed and used. In addition, the law altogether must be capable of ensuring that the inappropriate or unlawful development and use of PITs is not committed with impunity and that there are explicit penalties for violations, available remedies for victims and enforcement mechanisms in place.

Regulating the design and manufacture of PITs alone, therefore, is not enough. Regulations on the deployment and use of body scanners, HIMs and enhanced CCTV capabilities are still required. For this reason, throughout the dissertation, an assortment of different legal proposals was targeted at both the manufacturers/developers of PITs and the operators/users of PITs and/or data controllers.

Yet, the nature and content of these user-level regulations can still depend on the design of the PIT concerned, and vice-versa. For instance, laws that specify when the use of body scanners may be reasonable and according to what level of suspicion, in accordance with the Fourth Amendment, are dependent, for instance, on the final design and specifications of the body scanners, i.e. their level of intrusive capability in the first place.

Even though HIMs and the system thereof can be designed in a way that aims to secure the privacy of the implantee, this does not mean all people should be required to have a HIM implanted or that their implantation should be a condition of exercising other rights. In addition, HIMs, even with integrated PBD solutions, will still collect location information. The law must, therefore, also clarify what are the appropriate circumstances surrounding the use of HIMs and the location information generated by them.

Although CCTV microphones can be designed to only detect and record certain sounds that we all agree are threatening, this does not mean that the law should not

regulate what can be done with those recordings afterwards. While developing CCTV loudspeakers in a way that does not permit operators to freely say what they want prevents abuse and reduces the power to disturb and agitate the right to be left alone, the law must still specify where the loudspeakers may be deployed and when their use is justified and/or proportionate to legitimate aims.

10.5 FLEXIBILITY VS. SPECIFICITY

The law, in terms of privacy protection, is often enhanced either with greater specificity through additional specific legislation or additional specific provisions/amendments in existing laws. Specificity helps to allow the law to be predictable and consistent, removing ambiguity, and is also necessary for ensuring enforceability. However, *both* greater precision and clarity and sufficient room for flexibility is needed. Flexibility allows for the adjustment to new circumstances or the emergence of new technologies, which is especially required in a world of constantly advancing PITs. But, where PBD and existing legislation might not provide adequate safeguards for the most privacy-intrusive and disruptive technologies, further specific regulations should also not be overlooked.

Sometimes flexibility in law is effective, while at other times more specificity is required. For instance, the legal definition of personal data and the definitions of what constitute PITs, location information and tracking devices require flexibility, in order to ensure all applicable technologies, devices, etc. are broadly covered now and in the future. On the other hand, the definition of location information also requires a certain level of specificity, in order to cancel any doubts or close any legal loopholes concerning the privacy of location information. Moreover, stipulating where and when location tracking is lawful and stipulating which particular sounds and words, for example, may activate CCTV microphones to begin recording clearly require a certain degree of specificity.

Potential PBD legislation, in particular, also requires flexibility, since it is nearly impossible to delineate every design and technical requirement and also unhelpful to overly prescribe the PBD solutions. The goal indeed, therefore, is for the potential PBD legislation to be as broad and comprehensive as possible when mandating the implementation of PBD solutions. Nevertheless, the PBD solutions will also need to consider the specific characteristics and privacy threats/risks of the different devices, systems or technologies concerned.

10.6 RADICAL CHANGES FOR RADICAL CAPABILITIES

The dissertation research has shown that although body scanners, HIMs and CCTV microphones and CCTV loudspeakers pose a significant threat to privacy and liberty, this threat is not insurmountable. New and enforceable regulations can help to ensure that the development, deployment and use of the latest PITs are regulated adequately.

While the specific legal and technical solutions recommended for body scanners, HIMs and CCTV microphones and CCTV loudspeakers can potentially address the unique threats posed by each PIT, it is, nonetheless, not realistically possible and may indeed be impossible for lawmaking to always keep up with technological developments through *ex-post* lawmaking. It is neither feasible nor ideal to legislate for each and every new technology after it has been deployed or has hit the market or to legislate for every subject matter or domain in terms of privacy protection on a case-by-case basis. This approach will likely continue to result in the adoption of legal solutions that are, for the most part, too little too late and inadequate within years, and vulnerable to the wording and interpretations of the provisions. It is also neither feasible to rely on closing all the relevant legal loopholes or solving all the deficiencies in the law, where applicable, with legal amendments or additional sectoral, technology-dependent laws. Besides, the legal framework in the US, for instance, is already excessively fragmented. Moreover, *ex-post* lawmaking often takes considerable time and, for certain activities and technologies, it may already be too late.[925] New and radical technologies (and corresponding new and radical capabilities) require *new and radical changes to current approaches* for safeguarding privacy.

Although formulating comprehensive, technology-independent data protection/privacy legislation, in the traditional sense, is certainly a great start, such legislation can neither possibly cover all threats to privacy posed by the latest technologies in existence, let alone those yet to be developed or imagined. Essentially, the most comprehensive and far-reaching privacy legislation in the world, Directive 95/46/EC, cannot even address all the present and future threats to privacy, and for that reason the European Commission has proposed a new General Data Protection Regulation to replace Directive 95/46/EC. Moreover, as Reidenberg (2000) points out, enforceability is another limitation on the efficacy of comprehensive legislation, in the traditional sense. While Directive 95/46/EC establishes enforcement mechanisms, global data processing poses significant challenges to their effectiveness (Reidenberg, 2000).

---

[925] see, e.g., Cave, J., et al. *Trends in connectivity technologies and their socio-economic impacts*, Final report of the study: Policy Options for the Ubiquitous Internet Society, (RAND Europe, July 2009), p. 17.

The RISEPTIS Advisory Report rightfully advocates for ensuring that the development of law is "closely interlinked to technological progress", however, rather erroneously argues in favor of doing so in a reactive manner (2009, p. 31). In order to genuinely stay ahead of the game and to overcome the difficulty of legislating and keeping up with the development of technology, lawmakers need to be proactive and not reactive, looking forward rather than backward, in addressing the implications of PITs beyond tomorrow. Instead of reactively interlinking law with technological progress, in the words of US Secretary of State Hillary Clinton, "we need to synchronize our technological progress with our principles".[926] The law must steer the development of technology, and not the other way around, through *ex-ante* lawmaking, in combination with *ex-post* laws. As Cave et al. (2009) argue "rapid and potentially disruptive technological development and the possibility of profound and irreversible impact upon human characteristics and development call for a careful balance of *ex ante* and *ex post* regulation" (Cave et al., 2009, p. 16). On this basis, legislators can and should 'future-proof' lawmaking pertaining to technology, and should develop *ex-ante* solutions for protecting privacy and ensuring other democratic principles/values that stand a far better chance of being adequate in the long-term and are better equipped for withstanding the test of time.

Going forward, a fresh, one-size-fits-all (legal wise) and technologically neutral/technologically independent legal method is required, as far as possible. The PBD approach to upholding privacy (and other civil liberties) can be potentially applied to just about any PIT and is arguably a feasible solution to the difficulty of keeping up with technology. PBD is a more practical substitute to legislating for each and every new technology, whether already deployed, in the R&D stages or yet to be imagined, that poses a threat to privacy, irrespective of the legal framework.

Although each technology (i.e. PIT) may require specific, individualized PBD solutions in their own right and, therefore, the PBD solutions cannot be technologically neutral, the underlying neutral approach is to require any technology (system, device, service, etc.) to be designed in a way that incorporates all the principles of privacy,

---

[926] see the prepared text of the speech US Secretary of State Hillary Clinton delivered at the Newseum in Washington DC on the topic of Internet Freedom (21 January, 2010), available at: http://www.state.gov/secretary/rm/2010/01/135519.htm

Similarly, European Commissioner Viviane Redding, formerly of DG Information Society & Media (DG INFSO), and now responsible for DG Justice, Fundamental Rights and Citizenship, stated, during a DG INFSO staff general assembly on 12 February 2010, "although I am not going to be your commissioner anymore, I am going to be still your policy maker". What this means, I think, is that Commissioner Redding believes that ICT research and technological development, an area she was previously responsible for, should be aligned with the principles of justice and fundamental rights, an area she will now be responsible for.

where applicable, through built-in technical and design safeguards. Thus, PBD should be viewed as the core of permanently defending privacy against the threats to privacy and liberty posed by PITs, rather than temporary fixes at the periphery. While there may be some distinctions on how different actors (governed by different laws and needs) may be involved in using the same technology for different purposes, especially in light of creating PBD policies/requirements, the PBD approach is applicable regardless of the technology, legal framework or activity concerned. Overall, the PBD approach, therefore, should be technologically, entity and activity-neutral.

The law should move away from focusing primarily on data controllers and the users/operators of PITs, and should instead impose PBD requirements/obligations on the manufacturers/developers to constrain the privacy-intrusive capabilities of PITs in the first place. Accordingly, new and comprehensive PBD legislation should be adopted, mandating that the principles of privacy must be engineered into all PITs (with certain exceptions) manufactured/developed for private use and/or commercial sale *and* government use in the jurisdiction concerned. On the other hand, once again certain technologies/devices, such as surveillance technologies, strictly used by governments/competent authorities for law enforcement and/or military purposes, for example, may still need to be designed in way that *more* effectively violates privacy, while still complying with the relevant laws and constitutional protections concerning their development, deployment and use. Nevertheless, PBD requirements/obligations should overall still be applicable for technologies developed for law enforcement purposes.[927]

Comprehensive legislation mandating PBD could also potentially refer to ISO standards on data security, as Agre recommends (1997, p. 25), which is known as the "co-regulation model", whereby standardization is used to complement regulations. Alternatively, explicit PBD provisions could instead be further incorporated into existing (privacy/data protection) legislation for different domains and technologies. Moreover, PBD provisions/requirements could also be incorporated into existing legislation on

[927] Importantly, this is consistent with the EC's Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012. Article 19 requires Member States to ensure that data controllers are complying with obligations arising from *data protection by design* and p*rivacy by default*.

defective products and the liability of manufacturers thereof.[928] However, adding some specific provisions to existing legislation may not be sufficient.

Either way, the legal requirements to implement PBD should be applicable, where relevant, to *both* private and public entities and *both* manufacturers/developers of hardware *and* software (i.e. technology providers) and data controllers/service providers.

Accordingly, Article 23 of the official draft EU General Data Protection Regulation,[929] which proposes *data protection by design* (i.e. PBD) requirements, should further stipulate that these requirements also apply to the manufacturers/developers of the products and services in question. The application of Article 23 (paragraphs 1 and 2) to manufacturers/developers could bring greater legal clarity and purpose to paragraph 3 of Article 23, which empowers the EC to adopt delegated acts specifying appropriate technical measures/mechanisms (i.e. PBD solutions) for implementing PBD for products and services.[930] As a result, the draft proposal should also include a definition for "manufacturers" and "developers", in order to diminish any legal ambiguity.

For all practical reasons, however, it will be difficult, for the most part, to apply PBD legislation retroactively, i.e. to existing (or already developed and deployed) devices/products/systems. PITs previously developed and deployed before the enactment of PBD legislation will certainly continue to exist in society and originations, and will thus need to continue to be regulated primarily by user-level and *ex-post* regulations, where applicable. Thus, there will be a period of transition before achieving the new reality and specific objectives PBD promises. To address this limitation, the concept of "*Privacy by ReDesign"* was developed to apply PBD to existing systems by '*rethinking, redesigning* and *reviving*' these existing systems in a way leading to the end goals of PBD.[931] Additional shortfalls, constraints and limitations of the PBD approach are explained in section 10.19.

---

928 Consumer Product Safety Act of 1972; Consumer Product Safety Improvement Act of 2008; Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

929 see Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft.

930 Article 23, para. 3, could potentially have an indirect effect on the manufacturers/ developers, since the specification of appropriate measures/mechanisms for implementing PBD for product and services would likely put pressure on the manufacturers/developers of those services/products to conform.

931 Seminar of the 33rd International Conference of Data Protection and Privacy Commissioners, *Privacy by ReDesign* Workshop, Mexico City, Mexico, November 1, 2011.

Ideally, both the US and EU, and beyond, should adopt PBD legislation, given the global nature of the privacy problems/threats at hand and of the Internet. For instance, PBD legislation in the EU would be pressed to regulate any Google services, for example, that utilize servers based in the US. Nevertheless, even if only the EU initially passes fully-fledged PBD legislation (or incorporates additional PBD requirements into the draft General Data Protection Regulation), for regulating PITs (or initially just ICTs and digital services) manufactured/developed for use and/or sale and/or marketed in the EU, this would also have an impact in the US and on companies that do business in the EU. Furthermore, EU PBD legislation could alter US legislation. For example, REACH, the EU regulation on the safe usage of chemicals,[932] has had an extra-territorial impact on US companies and has influenced US regulations, since entering into force in June 2007.[933] Moreover, the mere existence of PBD legislation in the EU will likely also put pressure on the US Government to pass similar legislation.[934] In any case, as Cannataci points out, EU-compliant ICT/information systems could eventually develop into the *de facto* standard for most devices, infrastructure, systems etc. deployed in the US (Cannataci, 2011, p. 185). But, without common standards, between the US and the EU, interoperability issues will further emerge.

As outlined earlier, codes of conduct, voluntary best practice guidance, guidelines, privacy policies or other self-regulatory schemes are not absolute alternatives to binding law. There is ample evidence to indicate that laws should not and cannot be ditched in favor of industry self-regulations. For example, we have seen the negative consequences of this within the banking sector. Industry self-regulation has also arguably failed to regulate online privacy. Accordingly, while PBD legislation could form the basis of binding corporate rules, PBD requirements cannot and should not be laid down in more voluntary codes of conduct or self-regulations, but rather must be mandated by binding 'hard' laws. Similarly, we should not and cannot rely solely on companies (or government bodies) to always voluntarily comply with self-regulations. Technical

---

932 Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC

933 see, e.g., Black, Harvey. *Chemical Reaction: The U.S. Response to REACH* (Environmental Health Perspectives 116, March 2008).

934 For further discussion on possible explanations for the convergences in data protection policies/laws between the US and Europe, see Bennett, Colin. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992).

solutions cost money and avoiding or delaying compliance may be the easy way out. Companies and governments do not enjoy a reputation of always volunteering to absorb these costs or to grasp the additional undertaking in the name of privacy or data security. The confidence of consumers and citizens in governments and particularly in companies, with regards to privacy and data protection, is already far from ideal.[935] While the trust and confidence of consumers and citizens can also partly be achieved through potentially enforceable codes of conduct or self-regulations, hard legislation has the highest positive impact due to the stronger possibility of enforcement.[936] Although codes of conduct, privacy policies, self-regulations, etc. on PBD can be potentially enforced through supervisory authorities with enforcement powers, there are still no guarantees that these industry codes, policies or self-regulations will be adequate or compatible with the fundamental principles of privacy.

Besides, PBD should be implemented through 'hard' laws developed by political representatives, since this would be more consistent with the values of a democratic society, which require that "rule-making through technology must be shaped by public policy goals and debate" (Reidenberg, 2000). Therefore, if computer code can have the same, if not greater, effect in practice, then technological development must be brought into democratic processes.

10.7 IMPLEMENTATION, ENFORCEMENT, MONITORING AND EVALUATION

In line with the typical phases in policymaking/lawmaking, once PBD legislation and policies are put in place and the measurable and feasible objectives/targets are fully formulated and established, the legislation must then be gradually implemented and enforced accordingly, subsequently monitored and, after a certain period of time, evaluated on its effectiveness. Perhaps, a High Level Working Group (composed of mem-

935 Though consumers'/citizens' trust in public institutions to handle their personal data appropriately and their level of confidence in privacy policies is not perfect, according to a Eurobarometer survey in 2008, more than a majority of EU citizens do have this trust and confidence in different types of public institutions. However, considerably less than a majority of EU citizens have this trust and confidence in companies, such as credit card companies, travel companies, market research companies and mail order companies. see Flash Eurobarometer Series #225, Data Protection in the European Union - *Citizens' Perceptions* Survey, conducted by the Gallup Organization Hungary upon the request of the Directorate-General Justice, Freedom and Security of the European Commission, Analytical Report, February 2008.

936 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification "RFID Privacy, Data Protection and Security Recommendation" {C(2009) 3200 final}

bers from different public authorities and various stakeholder representatives) could be established to monitor, oversee and guide the initially complicated implementation/enforcement of the PBD legislation.

The diagram below outlines the implementation/enforcement steps for PBD legislation, including the main causes and effects, some of the preliminary indicators for measuring the enforcement, effectiveness and realization of the policy objectives/targets, and the links with other relevant key policy instruments/laws in the US and UK that serve as its basis.

The implementation/enforcement mechanisms, consisting of certification bodies, privacy audits, conformity declarations, recalls and sanctions, are briefly explained further in the following sections.

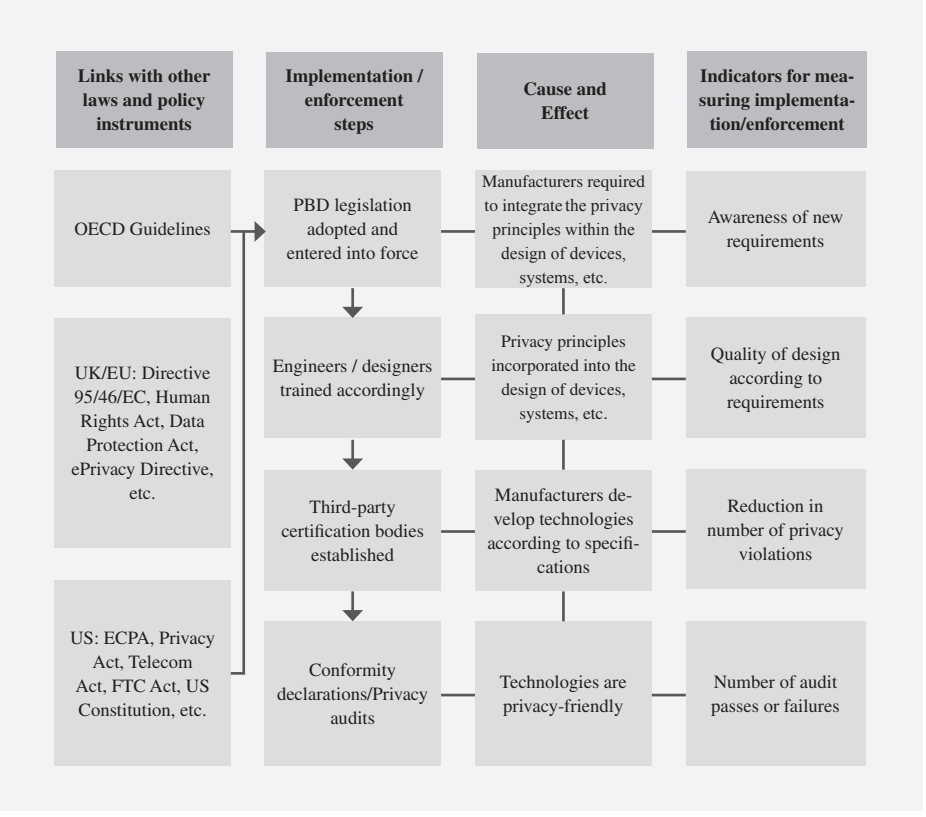

Figure 4: PBD implementation/enforcement

After a certain period of time, e.g., 3-5 years, a review process should be externally commissioned to evaluate/assess the status of the implementation/enforcement and the effectiveness of the PBD legislation, in order to determine if any adjustments and/or further policy measures/instruments are needed.

The overall long-term responsibility for monitoring the implementation/enforcement of the PBD legislation should reside with governmental data protection/privacy supervisory authorities.

10.8 ACCOUNTABILITY, SANCTIONS AND RECALLS

Manufacturers/developers (i.e. technology providers), in particular, should be held accountable/liable for failing to incorporate adequate and verifiable PBD solutions/technical measures that do not include both privacy and security functions, where required and applicable.[937] Likewise, manufacturers/developers should be held accountable/liable, under a similar liability structure, for 'privacy defective' devices/products *and* services that result from demonstrated negligence/fault and cause significant damages to a person as a consequence.[938]

The legal accountability of the manufactures/developers can come through the application of sanctions and product recalls, where deemed necessary. Sanctions could be imposed on the responsible manufacturers/developers and the individuals substantially affected may also be entitled to receive compensation.

In addition, where and when privacy/security failures emerge or non-compliance is discovered after the fact, whether intentionally or unintentionally, if the effects of the failure or non-compliance pose threats or risks to privacy and/or data security deemed to be serious, a recall of that product, device, etc. should also be enacted. A company's desire to prevent or avoid the risk of needing to initiate a recall of their products, devices, etc. could provide the necessary incentives to fulfill their obligations.

In the absence of an applicable manufacturer/developer within the concerned legal jurisdiction, then the designated official importer could also be potentially held respon-

---

[937] For instance, Senator Patrick Leahy previously introduced S.1490, entitled "the Personal Data Privacy and Security Act of 2009", which aims to hold software companies liable for security flaws or vulnerabilities and mandates that business entities implement data privacy and security technical and physical safeguards in the system's design and imposes civil penalties on entities that fail to do so. While the legislation essentially covers 'information privacy', as opposed to the protection of privacy overall, this proposal has some similarities to the proposed PBD legislation.

[938] A perfect example of a privacy defective device/service includes certain models of the Trendnet home security cameras that were discovered to have flawed firmware allowing anyone to access online live feed without requiring a password.

sible for publicly declaring that the device, product, etc. complies with the relevant PBD requirements/laws.

Nevertheless, the liability of manufacturers/developers should be subject to certain exemptions. For starters, manufacturers/developers should not be held liable for the unlawful use and/or modification of their products/services, whether by government or other private entities. Furthermore, under certain exceptions, if manufacturers/developers can prove that the privacy violations are not the direct result of inadequate PBD solutions or the lack thereof, they may also be exempted from liability. Finally, the so-called "state of the art defense"[939] should also exempt manufactures/developers from liability.

10.9 CERTIFIED PRIVACY-FRIENDLY

While privacy protection cannot necessarily be measured or quantified in the normal or traditional sense, a privacy compliance audit of the design of the PIT concerned could be conducted after the technical and/or architectural design solutions are built-in. The audit could serve to re-examine any residue privacy threats/risks and to determine or verify the quality and adequacy of the solutions in meeting certain objectives and complying with the principles of privacy and relevant laws.

Serving as a quality assurance mechanism for PBD, a privacy certification scheme may be effective in verifying that a PIT has been designed adequately in terms of privacy protection and incorporates adequate technical solutions. However, the principles of privacy provide the goals that need to be met with PBD, but do not actually provide the methodologies for achieving these goals, nor for evaluating the adequacy of the end result of PBD. The certification scheme will, thus, require its own evaluation criteria and measurement techniques for determining the validity and adequacy of the PBD solutions for the devices, systems and services concerned.

The certification scheme for PBD, however, should equally not only be based on a voluntary self-certification/self-declaration scheme, such as the 'Safe Harbor' scheme in the US. Instead, the scheme should be independent, external, mandatory and managed/supervised by either a quasi-governmental or governmental certification body, preferably in conjunction with accredited private certification bodies, but not by pri-

---

[939] For example, Article 7 of the EU Directive 1999/34/EC explains the "state of the art defense" exemption. Manufactures can be exempted from liability, if they can prove "*that the state of scientific and technical knowledge at the time when the product was put into circulation was not such as to enable the defect to be discovered.*"

vate entities alone.[940] The privacy certification scheme should apply to just about any system, device or service capable of posing a threat to the right to privacy, and not just ICT devices or IT-based/digital services. The accredited certification bodies should be composed of privacy auditors qualified to verify that any device or system has the appropriate built-in safeguards, design/architectural features and technical specifications, based on the principles of privacy and compliant with the relevant laws, and that these safeguards, features and specifications are not easy to bypass.

But, as a first step, developers/manufacturers could potentially or initially avoid external intervention by signing binding 'declarations of conformity'. If subsequently determined to be additionally required, external privacy auditors could conduct an evaluation of the devices, systems or services in question. In addition, random checks/audits could also be carried out.

PITs or any other technology, device or system either presumed or verified to have the required/appropriate built-in safeguards, design features and technical specifications could be certified 'privacy safe', 'privacy-compliant' or 'privacy-friendly' and could be marked with a standard privacy logo or seal.[941] In Europe, for example, the certification scheme EuroPriSe, initiated by the data protection authority of Germany and funded by the EC, has already adopted a 'European Privacy Seal', which is used to reveal to consumers that an IT product or IT-based service has been certified privacy safe and complies with the applicable EU data protection rules/principles. Other privacy seals include the Carnegie Mellon Usable Privacy & Security Lab's so-called "nutrition label for privacy". As the Article 29 Working Party points out, "[a]s certain seals become known for their rigorous testing, data controllers are likely to favour them insofar as they would give more compliance 'comfort' in addition to offering a competitive advantage".[942] An additional way of communicating the degree of privacy-friendliness of a device, technology or system could include the use of "privacy scores", based on the results of the PBD certification audit, similar to the "privacy scores" developed by PrivacyChoice for websites.[943]

Any privacy certification scheme, however, is only complementary to PIAs and should not be considered as the same thing. PIAs, for instance, are intended to be conducted *before and/or during* the development of the technology (or service) concerned,

---

940 A similar approach is used in the EU for the certification of organic products.

941 A similar approach is used in the EU for implementing 'ecodesign' requirements for energy-using appliances.

942 Article 29 Data Protection Working Party, WP 173, Opinion 3/2010 on the principle of accountability, Adopted on 13 July 2010, p. 17.

943 see http://www.privacyscore.com

in order to assess the potential threats to privacy posed by that technology. Moreover, as Cannataci points out, PIAs could induce the implementation of technical measures to safeguard privacy (2011, p. 182) and, therefore, PIAs can still play an important role.

Privacy certification audits, on the other hand, are conducted, for the most part, *after* the technology has been developed with the relevant laws and privacy principles systematically taken into consideration during the research, design and development/ manufacturing phases. Thus, before the development stage, the developers/designers, together with privacy experts, will first need to carry out a PIA to carefully identify all the foreseeable privacy threats and vulnerabilities of the device, system or service, as far as possible, and assess the potential risks involved and set benchmarks for removing/minimizing these threats/risks.

Furthermore, while there are established industry standards, implementing measures and audit mechanisms for ensuring data security, and, on top of that, comprehensive guidelines/checklists for conducting general and specific PIAs,[944] additional standards, methodologies, indicators and mechanisms for auditing the adequacy, performance and quality of PBD still need to be established, which embody all the principles of privacy, where applicable, in an integrated approach. ISO has so far at least set up a working group to establish a standard for "privacy technologies".[945] The EC has also called for the introduction of a "European certification scheme for "privacy-aware" technologies, products and services".[946] As the European Organisation for Security (EOS) recommends, the criteria for assessing/evaluating the adequacy of PBD solutions should equally be clear and precise.[947]

---

944 see, e.g., the ICO PIA Handbook for guidelines on conducting PIAs, available at: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html;
Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, available at: http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf

945 see JTC 1/SC 27/WG 5: Identity management and privacy technologies

946 COM(2009) 262 final, Communication from the Commission to the European Parliament and the Council - An area of freedom, security and justice serving the citizen.

947 see Pasic, Aljosa. "Privacy by Design: An industry perspective on the challenges and opportunities of privacy", available at: http://www.eurescom.eu/?id=531

10.10 DESIGNING FOR PRIVACY

It is now increasingly understood that, in order for citizens to enjoy adequate protection of privacy, in light of the digital age, the rapid advancement of technology and the challenges facing existing laws, manufactures/developers need to implement PBD solutions. This should not come as a surprise too many. Designing for an outcome is essential in just about all things. For example, if you want speed, safety and fuel efficiency in a car or airplane, then you must apply the principles of aerodynamics and safety during the design stages, which are then tried and tested. Moreover, if you want productivity and eco-friendliness, then you must design for it. The same concept and approach should possibly apply to privacy protection.

However, while the benefits of PBD are imaginable, it should also be noted, once again, that there is currently no widely accepted methodology or approach for specifically translating privacy/data protection laws into technological/design solutions and there are no accepted standards for auditing the adequacy and quality of PBD. However, valuable research has been conducted to progressively formulate a process. In general, a plausible process is to first analyze the legal framework to determine the required human behavior and then implement those requirements through technological/design solutions (van Blarkom, G.W. et al., 2003). After the PBD solutions are executed or physically realized, a privacy audit is subsequently conducted to determine if those requirements are fulfilled. Nonetheless, even though a common process is helpful, no single fixed methodology or approach is required, or even desirable, as PBD solutions should be somewhat tailored to the specific PIT concerned and, once again, should not be overprescribed.

Since the degree of privacy reasonably expected from the use of PITs is relevant to the degree of privacy the design of those PITs affords, inadequate and poor quality design specifications will only negatively affect or lower our reasonable expectation of privacy. Take, for example, a bathroom stall or changing room door. Clearly, existing privacy laws cover privacy in a bathroom stall or changing room and prohibit the spying or unauthorized observation of a person inside one. But, that prohibition is only as good as the design of the bathroom stall's or changing room's door. If the doors are below 5 feet (1.5 m), for example, or made of see through glass, then by simply walking past them, a person can easily and unintentionally see over the doors or right through them. Hence, any degree of privacy would be non-existent or unreasonably expected in these bathroom stalls or changing rooms simply because of the design of the doors, regardless whether the law clearly stipulates privacy in a bathroom or changing room.

In addition, any technological solution or architectural design for the sake of privacy must seek to transcend time, and therefore designers must attempt to anticipate, as

much as possible, the threats to privacy and other civil liberties posed by the technology (device, system, etc.) in question. As Sollie and Düwell (2009) wisely point out, an anticipatory outlook is required when addressing new technologies. The ultimate goal is to develop technological solutions and/or architectural designs that are 'future-proof' for the longest period of time possible to counter-balance the difficulty of 'future-proofing' *purely* legal solutions.

However, while the purpose of PBD is to effectively safeguard privacy and put into practice the principles of privacy, it must also not hinder or terminate the desired purpose, effectiveness and utility of the device, product or service concerned, thereby rendering it useless or ineffectual. Again, the right balance needs to be struck. Designing for privacy should also take into consideration the effects of over-engineering, which can cause a device or system to be more complicated than necessary and decrease its effectiveness and efficiency.

Although the law preferably need not overly prescribe what PBD solutions need to be adopted and implemented, what is essential is that those solutions are goal-orientated, adequate and focused on the minimum expected outcomes. As a final point, when it comes to designing for privacy, some common sense would also do some good. Consider, as an example, the previously explained analogy regarding bathroom stall/changing room doors.

10.11 ADEQUATE PRIVACY BY DESIGN

On the surface, the PBD solutions are adequate as long as they uphold all the privacy principles, where applicable, implement the relevant regulations, and ensure the minimum expected outcomes. The technical solutions, as much as possible, must also not be capable of being bypassed and must be up-to-date and relative/proportionate to the privacy threat at hand.

When determining adequacy, we should assess the extent to which the PBD solutions suitably match the threats to privacy, and the consequences thereof, posed by the technology concerned, evaluate the probability of the pertinent threats still occurring even after the PBD solutions are implemented, and assess the sensitivity of the personal data that may be processed. Hence, this is the reason why an assessment of the privacy threats/risks posed by the technology concerned (i.e. a PIA) must be conducted *before* and/or *during* the technological design/development.

In addition, the technical solutions should also take into consideration the implementation of other civil liberties, where applicable, and not just the right to privacy.

10.12 OVERREGULATION

Specific technical solutions were recommended for each of the four PITs addressed. But, the law should not overly prescribe these solutions, in order to prevent the drawbacks of overregulation. While the law should firmly mandate that public and private entities take the necessary steps to implement technical solutions when designing and developing PITs, it would be advisable for lawmakers not to get involved in determining and mandating exactly which are those solutions, and let the responsible industry players and other stakeholders work that out. But, in any case, those solutions must strictly be based on the defined privacy principles, norms and legal framework.

There are not necessarily single fixed solutions that work for all PITs all the time. Each PIT might require different solutions, based, once again, on the specific characteristics and privacy threats/risks of the technology concerned, and these solutions will also need to evolve as the technology evolves. Moreover, one-size-fits-all PBD solutions could create resistance to innovative and more effective solutions. In this regard, privacy law and the approaches to PBD could learn extensively from environmental law/regulation and the approaches to 'green by design'.

As Hirsch notably argues, 'command-and-control regulation' applied in environmental law, is not necessarily suitable for protecting privacy (2006, p. 33). In environmental law, "regulators identify the best currently existing technology for controlling pollution in that industry (known as the "reference technology")" and "either direct all facilities in the industry to install the chosen technology (this is known as a "design standard")" or require that the facilities do not exceed the rate of pollution they would emit if they had used the reference technology (this is known as a "rate-based standard") (Hirsch, 2006, p. 33).

As Hirsch (2006) further points out, with regards to environmental protection, "command-and-control also deters innovation in pollution prevention and locks in the current state of pollution control technology" (Hirsch, 2006, p.35). The same may hold true, as Hirsch (2006) argues, for privacy protection technologies.

While the "rate-based standard" may make somewhat more sense for protecting privacy than the "design standard", since it may permit different methods or means for achieving the same goal, the "rate-based standard" still relies, in effect, on the reference technologies on which the rate is based, as Hirsch points out, and "almost all [companies] choose the reference technologies so as to avoid any misunderstanding about compliance" (Hirsch, 2006, p. 34). As Hirsch further argues, "[b]y requiring firms to meet the best existing level of control technology, it gives them no incentive to exceed this level" and "the method is too slow for rapidly evolving industries" (2006, p. 35). Therefore, as Hirsch (2006) argues, both standards are just different types of command-

and-control regulation and, as a result, both would likely not hold up against the rapidly evolving technological means of privacy intrusion.

The EDPS recommends that PBD could potentially adopt the 'Best Available Techniques' (BATs)[948] approach.[949] However, BATs, which are also based on command-and-control regulations, can impel companies to adopt technologies that are already available (Hirsch, 2006, p. 35), thereby diminishing the outlook for developing more innovative technologies that are not yet available.

Moreover, overprescribing the technical/PBD solutions to address the privacy threats of PITs could discourage the continuous development or enhancement of new solutions that could progressively achieve even better results. Unlike the EC's draft General Data Protection Regulation, which gives the EC authority to mandate specific technical measures/solutions and standards, the proposed PBD legislation, as the US Department of Commerce similarly argues,[950] should instead focus on ensuring the realization and implementation of the principles of privacy as a *policy objective* or outcome.[951] If privacy laws are too prescriptive, as Hirsch also argues, they could stifle technological innovation for protecting privacy (2006, p. 36). Similarly, as the US Department of Commerce also points out, "by requiring a particular technology, a regulator may preclude the implementation of better privacy solutions and stifle innovation that benefits consumers and the economy".[952]

---

948 The term BAT (Best Available Technique or Best Available Technology) is another example of a concept that was first developed in the context of environmental protection, but its extension into other fields may be appropriate and constructive. Council Directive 96/61/EC of 24 September 1996 concerning integrated pollution prevention and control defines BATs as "the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing in principle the basis for emission limit values designed to prevent and, where that is not practicable, generally to reduce emissions and the impact on the environment as a whole" (Art. 2.11). Techniques include the use of technology.

949 see European Data Protection Supervisor Opinion on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, 22 July 2009, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

950 see US Department of Commerce, Informal Comment on the Draft General Data Protection Regulation and Draft Directive on Data Protection in Law Enforcement Investigations (16 January, 2012).

951 *Ibid*.

952 *Ibid*.

Likewise, "[e]nhanced privacy protection will depend on the development of new technologies" (Hirsch, 2006, p. 36) and the success of PBD is equally dependent on the availability of the technology to bring about that success. The PBD method or approach to protecting privacy, therefore, benefits from the further development of technology and, as Hirsch emphasizes, "[t]his development requires regulatory methods that encourage innovation, not those that constrain it" (*Ibid*., p. 36). Furthermore, as the US Department of Commerce points out in response to the EC's draft General Data Protection Regulation, "granting the [European] Commission the power to specify technical mechanisms may have the significant unintended consequences because technology developments outpace government regulation".[953]

Instead, the decisions on the specific technical measures/solutions and standards should be left open to a multi-stakeholder process.[954] Companies and other entities should also be allowed to collectively and/or individually select and develop their own method, as long as the selected method is strictly based on the defined fundamental privacy principles and applicable laws. In addition, PBD could also potentially benefit from open technical standards and open collaboration/open innovation.

The smart implementation of privacy protection measures will, thus, require smart regulations. If written smartly, regulations need not slow or halt the innovation of even better technical solutions for the benefit of privacy. Accordingly, PBD, and the privacy laws thereof, should adopt the next-generation regulatory approach, as opposed to an overly prescriptive command-and-control approach (Hirsch, 2006). Next-generation standards, such as Porter's performance-based standards for promoting innovation in environmental protection (see Porter and van der Linde, 1995), which move away from both design standards and rate-based standards, are not based on reference technologies and may, therefore, potentially help to promote the innovation of PBD solutions for protecting privacy by encouraging companies to select/develop their own methods (see Hirsch, 2006, pp. 38-40). The Environmental Management Systems (EMS) may also offer a helpful model for the protection of privacy and the implementation process of PBD, as argued by Hirsch, since EMS often entails continuous improvement practices (2006, pp. 60-63).

---

953 *Ibid.*

954 *Ibid*.

10.13 FURTHERING DEPLOYMENT AND INNOVATION

Some might raise the argument that *ex-ante* regulations on technological development could jeopardize or stifle innovation (Cave et al., 2009, p. 17) or hamper technology deployment and, therefore, could, in the long-run, also impede economic growth and competitiveness (*Ibid*.). Similarly, some might argue that regulating the development of RFID and GPS applications, body scanners, and enhanced CCTV capabilities, among other technologies that are also in their initial phase, will present barriers to their deployment and further advancement. The same argument often supports developing the technology first and asking questions and adopting guidelines later, and maybe, just maybe, if there is no other choice, and as the last resort, adopting relevant regulations only after a serious problem or incident arises.

While the ability to innovate without permission should not be compromised, there is a need for re-adjustment. Instead of applying resistance to the inertia of technological development, a more 'guided hand' approach is needed for steering technological development along a path that does not contradict privacy and other civil liberties and democratic values. This could move us away from the laissez-faire or "invisible hand" approach that has resulted in today's current situation, particularly in the US, surrounding the unrestrained development of PITs, as it has also, to a certain extent, arguably resulted in the ongoing banking/financial industry crisis.

On the contrary, the hurdles to the substantial further deployment, innovation and mainstream take-up of GPS and RFID applications, including location-based services, for example, are partly due to the general perceptions, mistrust and concerns of the public, privacy activists and civil society as a result of the grave threats to privacy posed by these latest technologies and the disbelief in the adequacy of the legal framework to defend against the corresponding privacy threats/risks.

The societal acceptance of the latest technologies is partly interlinked with the public's trust that privacy is respected, and the societal acceptance is often a prerequisite for the deployment and use of the latest technologies. The further development, deployment and use of the latest ICTs is now arguably being held back, to a certain extent, due to the opposition of consumer protection organizations, the lack of trust among consumers/citizens concerning the privacy/data protection issues and the hesitation of manufactures. This hesitation is likely due to these uncertainties and the resulting investment risks. And, once again, the lack of trust can also potentially lead to missed business opportunities and stalled innovation (Williams, 2009, p. 78).

RFID technology, in particular RFID implants, is a perfect case in point. If technologies or devices, such as RFID implants, are to succeed in achieving mass market take-up, the appropriate legal framework and technological architecture is certainly required

to earn the critical trust of consumers/citizens. The anxieties of consumers/citizens can potentially be overcome with not just public relations, which aim to persuade the public of the benefits of adopting certain technologies, but also with an adequate legal framework and the appropriate privacy safeguards. Actions often speak louder than words. Moreover, as a result of these perceptions, anxieties and legal deficiencies, manufacturers and service providers are faced with ensuing uncertainties, which could be seriously holding back the mass deployment and further innovation of RFID applications.

Lawmakers can alleviate the resistance and backlash to new technologies and facilitate their roll out and mass market take-up through the adoption of an appropriate and predictable legal framework. Citizens/consumers can be afforded with sufficient safeguards and rights, and developers/manufacturers, data controllers or service providers with clear rules to follow. Specific and up-to-date regulations and PBD solutions will enable companies and governments to earn the long-lasting trust and confidence of consumers/citizens over the use of PITs, thereby facilitating their widespread deployment and use, which in turn could further promote the necessary investments in innovation. Without specific and up-to-date regulations and safeguards, credit cards, for example, would not be able to flourish or function and e-commerce would not be what it is today, as consumers would not have had the required trust in these products or services when they were first launched.

Specific legal regulations on the design, development and manufacture of PITs could also enable the developers to design and manufacture them without concerns or uncertainties over the future legality and liability of their investment. Without specific regulations, the developers have no definitive standards to follow. In addition, the absence of specific regulations could further stifle innovation and lead to uncertainties and confusion for both industry players and consumers alike. As the RISEPTIS Advisory Board also points out, with regards to e-services, appropriate technical and legal infrastructures will remove barriers to innovation, as businesses will only invest in e-service solutions if the legal obligations are clear (RISEPTIS Report, 2009, p. 14).

Moreover, some PBD solutions or concepts could perhaps be innovative in themselves and could lead to further innovation in other related or even unrelated areas. For example, the innovative technology behind Brijot's 'intelligent detection engines' or L-3's automatic threat recognition (ATR) capabilities for body scanners, developed to better ensure both the privacy and security of air travelers, could also potentially have additional applications and/or could open up additional business opportunities.

Therefore, in addition to protecting privacy, PBD could potentially overall play an essential role in establishing a legal environment that facilitates greater investment in new technologies and, as a result, further innovation, by sending a clear signal to manu-

facturers/developers on how to move forward with certainty, backed by the confidence, trust and acceptance of consumers/citizens.

10.14 SAFEGUARDING PRIVACY, LIBERTY AND SECURITY

Numerous technologies/infrastructures, which have already been deployed (e.g. body scanners, UAVs, sensor networks, data centers, CCTV cameras, GPS tracking devices, etc.), clearly pose a threat to privacy/liberty. But, these technologies also offer security gains that cannot be ignored, and their deployment may be justified in many respects.

However, protecting privacy and maintaining national/public security is not necessarily a zero-sum game and a choice does not need to be made between protecting privacy and maintaining security (Cavoukian, 2009). Just like there are strong arguments in favor of achieving economic growth in an environmentally-friendly manner, national/public security can evidently also be maintained in a privacy-friendly manner.

Similarly, complying with laws, ethical values or norms does not necessarily cancel the security utility of technologies. Even the most morally questionable technologies can be designed to be 'value sensitive', while still maintaining their effectiveness. For example, missiles/bombs designed in a 'value sensitive' manner, in order to enable military leaders to better comply with the Geneva Conventions, certainly does not cancel their ability to destroy targets. Bombs/missiles are designed and manufactured to kill enemy combatants on the opposing side during a war or to cause immense destruction to the enemy's infrastructure (evidently in the name of security). For a long time, bombs/missiles were designed and manufactured to kill indiscriminately and were not designed to ensure attack precision. That ability to ensure precision was not available. Today, bombs/missiles are still developed to kill and cause destruction. But, at least now most bombs/missiles dropped or launched by the US, for example, during a military operation, are designed to strike a target with precision using GPS guidance, while minimizing the destruction of civilian infrastructure and lives. These bombs are commonly known as "smart bombs". This approach has proved to not only better comply with international laws of war and with overall human values; it has proved to be more beneficial for achieving certain military objectives.

The idea is that we do not always need to think in terms of privacy/liberty vs. security. In fact, in many ways, privacy/liberty vs. security is an increasingly false dichotomy, and we can achieve both at the same time. Especially, through PBD and certain choices of architectures used, the trade-off argument between privacy/liberty and security is less and less valid (Cavoukian, 2009). Privacy/liberty does not need to be sacrificed and

we can implement certain boundaries, without losing the security benefits or utility of PITs. There are clear technological examples demonstrating this to be true.

As deducted from the case studies, designing and developing body scanners, HIMs and CCTV microphones and loudspeakers, along with other PITs, in a privacy-friendly manner, in order to better comply with privacy laws and principles, not only does not cancel the national/public security benefits these PITs can provide, the proposed PBD solutions can potentially help to better realize or amplify those benefits.

The automatic employment of privacy algorithms/software solutions when body scanner images are generated, together with intelligent detection engines or ATR capabilities, can (potentially) help airport screeners/security officers to detect/locate threats by highlighting objects and reducing human errors. At the same time, these measures better protect the privacy of the human body (passengers) by reducing the unnecessary level of graphic detail contained in the images and/or potentially doing away with the need for remote human operators to directly view the images. Built-in limitations on storing, printing and transmitting the body scanner images can also better ensure the privacy principles are implemented. Regulating the design and manufacture of body scanners, and thereby limiting their intrusive capability, will arguably lead to their greater deployment and employment at airports (and maybe at other areas/locations on a case-by-case basis, e.g. train stations or major sports stadiums), which may be beneficial for security overall.

Strong encryption in RFID implants, which prevents 'cloning' and the unauthorized access to the information contained on the implants, and protocol-level controls, which can ensure that only authorized readers are able to read RFID implants, also allows for the security benefits of electronic identification and tracking to be realized, where and when appropriate.

Designing and developing CCTV microphones to pick up only on dangerous sounds, such as gun shots, explosions and breaking glass, allows the microphones to only focus on the sounds and scenes worthy of being detected and recorded, and deserving of the immediate attention of CCTV operators. The potential sound detection capability of microphones attached to CCTV cameras can enhance the ability of the cameras and CCTV operators to aid in criminal investigations and support public security, remove the blind spots of CCTV cameras and reduce the number of cameras needed to cover a larger area, while at the same time can facilitate a certain level of privacy out in public and minimize the unnecessary intrusion upon the public interactions of citizens. Moreover, this system can more effectively and efficiently employ/deploy CCTV control room operators for the sake public security.

Designing and developing CCTV loudspeakers in a way that enables their use to be registered and prevents abuse, for instance, also allows the operators to accurately

document and analyze where and how the loudspeakers can be more effectively used and deployed.

Therefore, PBD can provide potentially effective means for avoiding the (false) dichotomy of *privacy vs. security* (Cavoukian, 2009)[955] and, for that reason; PBD may be a pragmatic and integrated approach for safeguarding privacy, liberty and security in the 21st Century.

10.15 PRIVACY-FRIENDLY ALTERNATIVES

Even though body scanners, HIMs and enhanced surveillance capabilities may arguably be the most effective in preserving security in their respective field or domain, and the threats to privacy they pose can be minimized, there may be alternative devices or means available that are more privacy-friendly (or privacy-compliant), but arguably also provide similar benefits. Many of these alternatives were described in the previous chapters, and some should be further explored in future studies to definitively determine their pros and cons in more detail.

In any case, the least privacy-invasive technology overall should be used, in accordance with the principle of proportionality, as long as it is capable of providing similar benefits, for example, in terms of security. If the more privacy-friendly alternative is not used, the legal and factual reasons for not doing so should be justified accordingly.

10.16 COUNTERING POTENTIAL CRITICISM OF PBD

In response to potential criticism (see section 9.11), PBD does not rely excessively on individual "privacy control". Indeed, PBD is an answer to Schwartz's (2000) criticism of "code as law", since PBD can serve as the means of *automatically* realizing the principles of privacy. In other words, PBD aims to implement the mandatory and default rules/principles of privacy protection primarily in a self-executing manner, i.e. without the constant involvement of individual choice or human intervention.

Moreover, while politics and market dynamics should obviously not be ignored, the effectiveness of PBD is not overly contingent on finding the "optimal mix" of the different modalities/dimensions of regulating technology development. Indeed, one of the main reasons for mandating PBD is to overcome current market failures and, above

---

[955] see also Ann Cavoukian's "7 Foundational Principles of *Privacy by Design*", Originally Published: August 2009, Revised: January 2011, available at: http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

all, PBD is about the implementation of privacy laws/principles primarily through technological/design solutions.

The PBD approach is also compatible with the way lawmakers, legal practitioners and courts operate in the real world. After all, the concept behind PBD already has a legal basis in the US and EU, and the EC's draft proposal for a General Data Protection Regulation proposes PBD requirements. While the current (and proposed) privacy/data protection laws *primarily* apply to data controllers/processors, and not technology developers/manufacturers, there is, nevertheless, also a legal basis for this approach. Patient safety, automobile safety and consumer and environmental protection laws, for instance, already regulate how certain products are designed and developed/manufactured.

Given that PBD will require traditional legal approaches and is not a substitute for law or lawmakers, but is rather meant to enforce existing laws, norms and principles (see section 10.4); there is also little or no reason to assume it is incompatible with democracy. As Schwartz similarly argues, the application of the privacy principles (or FIPs) ensures the involvement of our democratic institutions, and since PBD is based on the principles of privacy, lawmakers are already involved in the process of shaping the technological requirements and solutions (Schwartz, 2000, p. 787).

Furthermore, Grimmelmann's warranted analysis that computer code/software is also *malleable* and *vulnerable*, and is not the same as physical architecture,[956] is offset by the fact that PBD includes *both* physical design/architectural solutions and technological/software solutions. PBD does not aim to equate the two types of solutions.

10.17 OVERCOMING SOME OF THE CHALLENGES

First of all, in order to ensure that the necessary PBD solutions can be developed appropriately, the underlying PBD requirements mandated through PBD legislation will need to be clarified precisely and consistently.[957]

Furthermore, as the European Organisation for Security (EOS) also proposes, research-funding programmes should fund studies that aim to identify and address the needs for the development of concrete, specific and viable PBD solutions.[958] In line with these views, the European Commission (Trust & Security unit) plans to fund, un-

---

[956] Grimmelmann, James. *Regulation by Software* (Yale Law Journal, Volume 114, 2005), pp. 1719-58.

[957] For further discussion, see Pasic, Aljosa. "Privacy by Design: An industry perspective on the challenges and opportunities of privacy", available at: http://www.eurescom.eu/?id=531

[958] *Ibid*.

der the Seventh Framework Programme (the EU's main research-funding programme), projects that aim to facilitate the interplay between various stakeholders and actors, in order to preliminarily establish best practices, standards and a roadmap for promoting and implementing PBD.[959]

Companies, researchers and other stakeholders could also receive public funding to develop and validate a variety of PBD solutions, and then identify and exchange best practices and lessons learned for implementing PBD solutions, based on established facts/evidence and pilot demonstrations. This could also help to provide the required inspiration, driving force and knowledge/evidence for developing/adopting PBD legislation and for developing a sort of checklist for PBD procedures. Subsequently, public funding could also be made available to establish dedicated PBD training programs for computer programmers/engineers and to communicate the identified best practices and lessons learned.

In addition, a rewarding scheme for the best PBD solutions could stimulate excellence in PBD and the engagement of highly qualified and creative designers and engineers. Adding PBD as a category to the International Design Excellence Awards (IDEA), for example, could help to stimulate the required excellence in PBD.

10.18 ENGAGING RELEVANT STAKEHOLDERS AND OTHER ACTORS

The success of PBD will also require the engagement, inter-communication and information/best practice exchange between a variety of relevant stakeholders and actors, from the manufacturers of PITs, and their engineers, programmers and designers, to lawmakers, regulators, policymakers, privacy commissioners, privacy officers, lawyers, certification bodies, certified PBD trainers, privacy certification auditors, research bodies, data controllers/processors, operators, service providers, law enforcement agencies, privacy law scholars and social scientists. For the most part, engineers and designers will require certified training in PBD, and manufacturers/developers of PITs will require privacy law experts to further guide and advise their designers and engineers on the steps that are legally required for compliance.

In order to reflect public concerns and public policy considerations, the involvement/participation of citizens and/or of consumers/users, perhaps mostly through representative organizations, in the design of PITs, should also play an important role in the adoption of the final product. As Reidenberg argues, "citizen participation is neces-

---

[959] Indeed, at a networking session at the ICT Event 2010 in Brussels, which I attended, European Commission staff from the Trust & Security unit expressed their preference or intention to fund a Coordination Action that brings together stakeholders for the purpose of facilitating PBD.

sary so that public values and goals are consistent across the three spheres of law, technology and market behavior and activities" (Reidenberg, 2000). Moreover, PBD could potentially benefit immensely from methods of collaborative design and production with interested citizens and/or consumers, where applicable, appropriate and feasible. The involvement of citizens and/or consumers could also facilitate the legitimacy and trustworthiness of the relevant PITs.

Civil society and privacy commissioners can also help to advocate for the necessary greater public and private investment and cooperation in the R&D of PBD solutions (Cavoukian, 2009) and help to raise public awareness of the emergence of new technologies that pose a threat to privacy and other civil liberties.

If successful, PBD in the end could serve as a bridge between lawmakers, policymakers, practitioners, engineers/designers and academics, and thus potentially evolve into a policy instrument for overcoming the separation of the variety of relevant stakeholders and actors, for minimizing the excessive division of their efforts to protect privacy and for identifying the concurrences, synergies and overlaps of their endeavors.

10.19 LIMITATIONS AND CONSTRAINTS OF PBD

While PBD may be critical for protecting privacy against the intrusive capabilities of the latest technologies, in practice the approach is *not* a panacea for preventing all problems/issues related to privacy intrusion. Certainly, legally mandating that technical solutions be implemented at the earliest stage of development is no magic bullet, not to mention the criticism of PBD (see section 9.11) and the challenges of implementing PBD (see section 9.12). There is simply no magic bullet for completely guaranteeing privacy, nor any single way to completely ensure that governments, companies, data controllers and operators of PITs comply with all privacy laws and principles all the time.

There will certainly still be moments when companies and governments violate privacy and design devices or systems that threaten privacy, whether deliberately or unintentionally, lawfully or unlawfully. After all, PITs are not the really causality of privacy infringement, but rather the means. Human behavior is the cause, and privacy invasion is the effect. It is for that reason why PITs must be designed in a way that regulates human behavior and minimizes the effects of that behavior. But, PBD will certainly not remove the need for doing so.

No matter how PITs are designed/developed, their widespread deployment and use will likely always present concerns over the protection of privacy and liberty. Law does not perfectly regulate behavior and neither does technology. The PBD approach cannot entirely prevent every privacy violation conducted either accidently or intentionally. Just

like designing bombs/missiles to be 'smart' may be an effective way of better putting into practice the Geneva Conventions on the prohibition of killing civilians indiscriminately during a war, it does not mean that mistakes based on poor intelligence, for example, will not occur, or that militaries will never intentionally use 'smart bombs' to kill civilians.

PBD neither can answer nor solve all the critical legal questions. For example, while PBD can aim to develop location-based services and related products for consumer use in a privacy-friendly manner, it cannot determine the lawfulness in the US of warrantless GPS tracking conducted by law enforcement agencies or determine the privacy protections afforded to location information generated by HIMs (or mobiles phones and other PLDs) or the level of privacy afforded to citizens/consumers out in public.

Again, as Sollie and Dowell (2009) argue, an anticipatory outlook is required when addressing new technologies. However, given that the ability of the designers and engineers to imagine or anticipate all future scenarios is limited (Albrechtslund, 2007, p. 72), it is unlikely that all the intended and unintended eventual uses of a particular PIT, and the privacy threats thereof, can be foreseen at all times during the design and development stage or even after a PIA and privacy audit is conducted. For instance, predicting every privacy threat now and in the future will be particularly difficult in a 'ubiquitous information society'. Any uncertainty or unawareness of all the privacy threats and implications of the technology in question is equally a predicament for PBD, particularly if the technology, device, infrastructure, system or service has never been deployed and used yet. Therefore, since the development of new technologies regularly occurs under conditions of uncertainty, as Sollie and Düwell (2009) point out, then the effectiveness of PBD may equally be uncertain and limited at times.

In addition, as data controllers/processors and service providers increasingly use so many different technologies, devices, tools and systems, determining the specific technical problem or defect, identifying the responsible/liable party and establishing a link between the problem, defect or malfunction and the privacy damage is less and less obvious.[960] For example, a RFID system could be composed of different types of RFID tags and readers, databases, fixed and mobile computing devices and software.[961] As a result of the (potential) lack of a clear understanding of responsibility/liability, the enforcement of PBD requirements will equally face obstacles and constraints.

---

[960] see *Trust in the Information Society: Research and Innovation on Security, Privacy and Trustworthiness in the Information Society*, A Report of the Advisory Board RISEPTIS, 2009, p. 13. (RISEPTIS was composed of more than 30 experts and was supported by an EC-financed 'Coordination Action' project, THINKTRUST, whose objective was to develop a research agenda for Trustworthy ICT).

[961] see Cannataci, Joseph A. *Recent developments in privacy and healthcare: Different paths for RFID in Europe and North America?* (International Journal of RF Technologies, Volume 2, 2010/2011), pp. 173–187.

While PBD can potentially better minimize the impact of the use of PITs by controlling/minimizing the intrusive capability of the technology in the first place, care should be taken not to give the impression that technology developed under certain legal requirements is no longer susceptible to future ethical dilemmas or future technological advancements (Albrechtslund, 2007). PBD is susceptible to the inclination that PITs, or any technology for that matter, are often never really finished developing. As new capabilities are added, further unforeseen privacy implications may result. Though the goal is to design technology to be privacy-friendly in a way that transcends time, however, PBD must be an ongoing process that requires continuous advancement and re-assessment as PITs constantly advance. If PBD is not as dynamic as technological advancement, then just like laws, the PBD approach will also fall behind. For this reason, as pointed out earlier, Hirsch argues that EMS may be a helpful model for PBD, since EMS often entails continuous improvement practices (Hirsch, 2006, pp. 60-63). Even with the methodical implementation of PIAs and PBD, unforeseen threats to privacy could still be encountered. Some PBD solutions themselves might later on result in unexpected privacy implications, as the technical solutions further advance.

In addition, not all PBD solutions will be effective at present or in the future. Some solutions, even those based on the BATs at the time and designed in a way to be 'future-proof' as far as possible, could prove deficient or insufficient later on or end up being susceptible to circumvention or even end up failing. As experience has shown, there is no absolute guarantee that any system or device is completely free of vulnerabilities or privacy risks, just as there is essentially no absolutely impenetrable security system or level of software encryption or error-free computer code. Specifically, for instance, as Grimmelmann points out, "software is vulnerable to failure in three related ways: It is *buggy*, it is *hackable*, and it is *not robust*" (Grimmelmann, 2005, p. 1742). Clearly, if a (PBD) software solution is hacked or somehow circumvented, the solution has not acted as an effective constraint (*Ibid*., p. 1731). A number of PETs, for example, developed for ensuring privacy and data security on the Internet, have already failed. During the initial phase, many of the new PBD solutions developed will likely fail or be circumvented.

While PBD solutions for protecting privacy aim to minimize the intrusive capabilities of the technology concerned, PBD cannot address every privacy threat posed by every PIT, since not all privacy threats posed by the latest technologies can be designed or engineered away. As a case in point, PBD is understandably not an all-encompassing solution to dealing with the very complex and dynamic privacy issues surrounding the greater use and advancement of DNA analysis and neurotechnology. Similarly, as Grimmelmann (2005) points out, technology/software cannot implement every rule. Consequently, there are certainly some privacy threats outside the scope of PBD solutions, at least for the time being.

As outlined earlier (see section 10.4), technical and/or PBD solutions alone cannot in practice guarantee privacy, and Lessig's other dimensions/modalities for regulating technology will also play an important role in the success of PBD. For starters, laws that mandate these solutions be implemented, specify the liability of not complying, provide for audit and enforcement mechanisms, provide legal remedies, provide the legal mechanisms to intervene in the chain of production, require the notice and consent of data subjects, and regulate the general deployment and use of PITs are still required. Moreover, PBD alone cannot implement all of the relevant legal requirements. For instance, administrative processes, such as the requirements of organizational accountability and notification requirements, cannot be implemented through PBD (van Blarkom, G.W. et al., 2003, p. 50).

The market dynamics, which in a free market are normally beyond the control of the government, can also limit the success of PBD. The implementation of PBD depends, in part, on the willingness of manufacturers to comply. Since PBD solutions come at an additional cost, in order for PBD to be employed or implemented at an acceptable rate, the developers/manufacturers of PITs must also be convinced and fully aware of the value and financial justification or business benefits in complying and the financial costs, risks and liabilities of meager privacy controls/safeguards. As Borking points out, from a business perspective, it makes no sense to invest in a privacy protecting solution if the actual costs of the solution are greater than the value it actually offers (Borking, 2010, p. 260). The value will increase as consumers increase their demand for privacy-friendly products and services. If consumers persistently continue to demand that their privacy be protected, then so too will the demand for devices, systems and services that are designed in a privacy-friendly manner. However, the success of PBD will require not only companies to view the protection of privacy as profitable or financially justifiable.

The political determination of lawmakers will also decide the extent to which PBD is realized. Reaping the benefits of PBD will equally require constructive political choices in addition to technical choices. Therefore, radically changing the way companies and governments design, develop and procure PITs will require, not just new technological and legal solutions, but the basis to overcome economic and political reservations. Economic reservations can come from the extra costs and burdens of PBD and the political reservations will likely come in the form of hesitations in intervening further in the production chains of free enterprises in a market-driven, laissez-faire economy. Significant investment and resources from both the private and public sector will need to be allocated to carry out the necessary R&D and innovation, in order to realize effective PBD solutions, tools and methods to implement and enforce the relevant privacy principles and laws thereof.

In order to induce politicians to take the necessary steps to pass new comprehensive laws requiring the implementation of PBD in PITs, politicians will need to further recognize the protection of privacy as an additional source of political legitimacy and recognize that it is indeed possible to engineer privacy into PITs. Moreover, like with environmentally-friendly devices, systems and services, the demand for privacy-friendly devices, systems and services will also need to come from governments, and not just consumers. Since governments are significant buyers of PITs, the adoption/implementation of policies in support of the public procurement and pre-commercial procurement of privacy-friendly devices and systems could set a good example and further influence the design and development of PITs. Essentially, as long as the business case and business model is weak and the political will is absent, PBD will not take off, regardless of the legal framework in place.

Finally, the continuation of privacy values and norms and an expectation of privacy are required. Apparently, the "Internet Generation" (or the "Millennial Generation") increasingly has less appreciation and expectation for privacy, and today's teenagers could grow up to future adults who do not care a great deal about their privacy. The Founder and CEO of Facebook, Mark Zuckerberg, also suggested that privacy is already no longer really a social norm and that sharing information instead has become the new norm,[962] without basing his claim on any empirical evidence or statistics.[963] However, Zuckerberg has a vested interest in making this claim, which was anyhow proven, for the most part, erroneous or at least premature, as demonstrated by the uproar of Google Mail (Gmail) users just days after the launch of Google Buzz. Nonetheless, if Zuckerberg's claim ends up proving true, the demand for privacy-friendly devices and services, as a result, could significantly decline. This could also end up diminishing the widespread support and implementation of PBD.

In sum, the general conclusions and policy recommendations of this dissertation, in support of PBD, are indeed limited by the ability of designers and engineers to envi-

---

962 Gaudin, Sharon. "Facebook CEO Zuckerberg causes stir over privacy" (Computerworld, 11 January 2010), available at: http://www.computerworld.com/s/article/9143859/Facebook_CEO_Zuckerberg_causes_stir_over_privacy?taxonomyId=16

963 A recent poll has perhaps contradicted Zuckerberg's statement. The Pew Research Center's Internet & American Life Project found that young adults (ages 18-29) in fact are not indifferent about their online reputation. For example, 71% of young adults who are social networking users have changed their account privacy settings in order to limit what they share online. The results were based on data from telephone interviews conducted, between August and September 2009, among a sample of 2,253 young adults in the US. see: Reputation Management and Social Media, Pew Internet and American Life Project, May 2010.
(But, the survey targeted young adults (ages 18-29) and not teenagers. Moreover, there is still relatively little empirical data on society's overall perceptions of privacy and how, why and when it is most valued.)

sion the threats posed by PITs, their ability to design and engineer away the threats to privacy, their ability to keep up with the ever growing threats and intrusive capabilities of PITs, the ability of the legal framework to ensure implementation and compliance, the market dynamics, the consumer demand, the political will of lawmakers, and the persistence of key privacy values and norms.

10.20 FINAL CONCLUSIONS

PBD is the critical combination of technology and law that can potentially propel a legal framework forward to address not just information privacy and the new threats posed by body scanners, RFID/GPS implants and CCTV microphones and loudspeakers, but also the incredible threats to privacy posed by other privacy-intrusive technologies. Adequate technical and design solutions, based on the well-established principles of privacy, can potentially convert the unrestrained, radical privacy-intrusive capabilities of these technologies into prudent, privacy-friendly commercial and security gains.

For far too long, manufacturers/developers of PITs have been generally ignored by data protection/privacy legislation and, as a consequence, the laws have often fallen behind new technological developments and have failed to address the privacy-intrusiveness of the technologies concerned at the design stage. Instead, new laws should mandate that the designers and developers of these technologies implement PBD solutions, where appropriate, and punish those who fail to do so. Accordingly, more burdens will be placed on the designers and developers of these technologies, rather than overly relying on the goodwill and compliance of the data controllers, service providers and operators/users of these technologies. As a result, the legal framework may be better equipped to stay apace with the rapidly changing and advancing technological threats to privacy.

Moreover, for far too long, the protection of privacy in the US and UK has been at the mercy of the legal interpretations of courts to fill-in the gaps and/or to address the legal issues or deficiencies of existing data protection/privacy legislation. Instead of excessively relying on the sometimes altering and inconsistent legal interpretations of courts, comprehensive PBD legislation can bring about the required consistency and permanence.

In conclusion, PBD is arguably the best option there is, at present, to balance the (potential) trade-offs between privacy and liberty, on the one hand, and public security, convenience and commerce, on the other. While it is not necessarily possible to prevent every conceivable violation of the right to privacy or fully address every threat to privacy, it is reasonably evident that practically any device or system is more likely not to jeopardize privacy and liberty if it is legally required to be designed and manufactured with the relevant privacy principles built-in than if it is not required so. Although

technology/technical solutions cannot completely guarantee privacy and liberty, it can at least provide the circumstances and environment in which privacy and liberty stand a much better chance in the modern world. At the same time, technology will certainly still present challenges to privacy and civil liberties, albeit these challenges can be better managed and addressed through PBD.

Nonetheless, the dire reality is that the diminishment of privacy or the serious threats to privacy posed by the inertia of technological development run rampant is probably an issue just too big for PBD or any single legal or technical solution alone. But, taking no action is not an option either, as society is faced with increasing threats to privacy posed by the evermore advancement and deployment of PITs. The realistic objective of PBD is to separate the problem into achievable legal, policy and technical options for addressing the threats posed by the latest technologies now and in the future. However, with the evermore advancement of privacy-threatening technologies, in any case, probably the best we can hope for and strive to achieve for now is at least to defend privacy and liberty for the foreseeable part of the 21st Century.