Why *Privacy by Design* is the next crucial step for privacy protection

By Simon Davies
London School of Economics & Privacy International

Sponsored by the Initiative for a Competitive Online Marketplace (ICOMP)

November 2010

Scope of this paper

The purpose of this paper is to enhance the quality of debate on the important topic of Privacy by Design (PbD). The paper is not intended to provide detailed theory or technical data, but instead will describe the general background and potential of PbD.

The importance of effective PbD is increasing with the amount of personal information collected and held about people around the world by private and state-run organisations as they go about their daily lives. The focus on this topic is particularly timely in light of recent high profile developments related to new commercial services on issues such as data collection, retention and mobile privacy.

The paper was developed on a consultation basis, with input from expert meetings in Hong Kong and London. A discussion draft was launched at an ICOMP event at the International Privacy and Data Protection Commissioners meeting in Israel in October 2010.

The evolution of Privacy by Design

Over the past thirty years, as new information and communications systems were being equipped with more aggressive capability to enable surveillance of private data, the attention of researchers and policy makers became increasingly focused on emerging threats to privacy.

Even as far back as the 1970s, the concept of computer assisted "mass surveillance" of large populations had prompted legislative initiatives in several countries and in particular in Europe and the US. These concerns formed the foundations of moves to create harmonised regulation across Europe and throughout Council of Europe and OECD member countries.

By the mid 1990s, research interest was being generated by the notion that surveillance had become an embedded design component of police systems, national security, CCTV[1] and workplaces.[2] Increasingly, "off the shelf" mainstream software, workplace and communications systems allowed enhanced monitoring capability as part of the basic "package". Even the most rudimentary call centre design incorporated capacity to intricately monitor the performance and activities of staff while new urban centres incorporated visual surveillance as a key component of architecture and road development. Attention shifted incrementally from the development of stand-alone surveillance "gadgets" to the nature of design and the default surveillance capability of platforms and large systems.

Privacy by Design as a concept was known to the architecture and building sectors from as early as the 1960s[3], however, within the information realm at least, the expression "Privacy by Design" appears to have emerged only in the late 1990s, but not before another phrase - "Surveillance by Design" - was coined during the debates over the US *Communications Assistance for Law Enforcement Act*" (CALEA) in 1994.[4] This and related legislation globally

---

1 *See the work of Professor Stephen Graham, University of Durham*

2 *See in particular the work of David Metcalf and Sue Fernie, London School of Economics Centre for Economic Performance*

3 *See Alan Hedley (1966) 'Privacy as a factor in residential buildings and site development: an annotated bibliography', in Issue 32 of Bibliography, National Research Council of Canada. Division of Building Research*

4 *See Samarajiva, R. (1996) 'Surveillance by Design: Public Networks and the Control of Consumption', in R. Mansell and R. Silverstone (eds) Communication by Design: The Politics of Information and Communication Technologies, Oxford: Oxford University Press, 129-56.*

was intended to ensure that surveillance capability was embedded into communications design by mandating that systems were designed in such a way that law enforcement agencies were able to access whatever data they lawfully wanted. In some respects PbD was a parallel countermeasure to these developments.

This shift in focus was timely. Along with the drift to surveillance in technology design, legislative gravity was creating a more extensive and universal mandate for population-wide surveillance through systems that were increasingly interoperable. In many cases, through legislation or convention, systems were required to capture data through covert "back door" techniques that were sometimes unknown even to many people involved in developing the technology.

Meanwhile, competitive advantage accrued to developers that could devise systems that conducted surveillance as part of their normal day-to-day functioning. When Privacy International considered in 2002 whether it should conduct a follow-up report to its 1995 analysis of the international surveillance technology trade[5] it determined that the sector had shifted in the space of seven years from sales of specific surveillance technologies to assisting mainstream IT and communications companies to integrate surveillance capability into the core of their general systems in ways similar to those required by CALEA.

In a parallel development, the extent to which personal information has been monetised has also provided strong incentive to developers and platforms to set defaults in privacy settings to maximum information disclosure for tens or even hundreds of millions of users at a time. This trend has been rolled back slightly in recent times, but it is still the case that the vast majority of social networking and other online environments set their "recommended" privacy controls to at least a significant level of disclosure of personal information.

In an effort to counter this trend, researchers and regulators started to pursue countermeasures that might provide a higher standard of privacy protection built from the core rather than as bolt-on measures. Amongst the most important of these is *Privacy by Design,* an emerging approach intended to ensure that privacy protection is maximised by embedding protection seamlessly across every strand of design and deployment of a product or service. As one prominent contributor to the field observed:

How we get there is through *Privacy by Design*. Where PETs [Privacy Enhancing Technologies] focused us on the positive potential of technology, *Privacy by Design* prescribes that we build privacy directly into the design and operation, not only of technology, but also of operational systems, work processes, management structures, physical spaces and networked infrastructure. In this sense, *Privacy by Design* is the next step in the evolution of the privacy dialogue.[6]

In recent years, interest in PbD amongst regulators and companies has been driven in part by increased awareness of the concept behind "Privacy Impact Assessments" (PIAs) which also aim to assist organisations to build privacy into the core of the service or product from the Business Plan stage onward. The nexus between PIAs and PbD is substantial and the migration of support from one approach to the other provides both an insight into the complexity of the challenge facing regulators and organisations, and the pressing need to find immediate and meaningful solutions.

---

5 *"Big Brother Incorporated", Privacy International, 1995*
http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61908

6 *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D*
http://www.springerlink.com/content/d318xq4780lh4801/fulltext.html

It is equally true that organisations appear to be more open to the argument that data minimisation is a sensible approach to risk mitigation and that giving users a degree of data autonomy is central to nurturing trust. In both respects the use of PbD can be an invaluable benefit to seeking practical alternative approaches.

Privacy by Design: controversial?

The theory and practice behind PbD is commonplace, and thus should not be seen as controversial. The concept of embedded protection on the basis of sensitive seamless design has been embraced over the years in numerous environments. In the field of forensics, investigators have for many decades known that the forensic chain of events (collection of material, recording, processing, analysis, reporting etc) is only as reliable as its weakest link and that a “total design” approach should be taken across the entire chain to reduce the risk of failure. According to this rationale, the “spaces” between events and processes are seen as posing as much of a risk of failure as the component parts themselves. With this threat model in mind, a system or infrastructure can be designed or redesigned from ground up to ensure a seamless approach to risk reduction.

The same approach has been pursued to a varying extent for environmental protection, workplace safety, urban planning, product quality assurance, child protection, national security, health planning, infection control and information security.

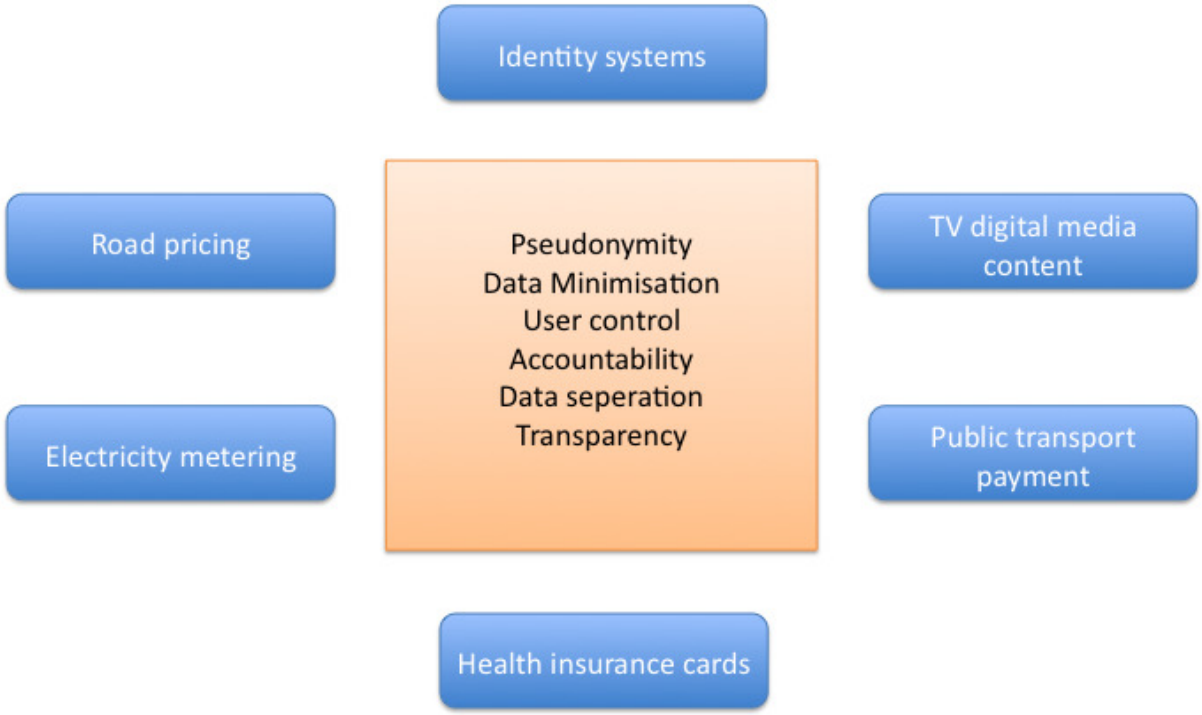
This approach is rooted in a belief that reliable protection in a complex ecosystem can only be achieved through an integrated design approach. It is reasoned that unless a system is developed from “ground up” with protection at its core, failure will emerge through unexpected weaknesses. In the infection control environment, for example, the simple “plastic wall” concept of isolation which depended on sealing off a room with doors or sheeting has evolved into a far more integrated and far sighted plan that extends from procurement oversight to sensitive architectural design.

With this broader use of “protection by design” it is clear that PbD's antecedents go back some decades. By the 1990s the (at the time unnamed) PbD concept was also deeply rooted in cryptographic techniques and – later – with such concepts as “Privacy Enhancing Technologies”.

Possible applications of Privacy by Design

Like PIAs, the Privacy by Design approach offers a means of discovering privacy-friendly solutions in environments that traditionally have exploited large amounts of personal information:

- Establishing permissions without the need for comprehensive and invasive identity checking using such techniques as anonymous authentication or anonymous credentials.
- Developing “pay as you drive” systems that do not require constant tracking of motorists.
- Creating smart electricity metering that involves minimal profiling and data collection.
- Developing verification and ID systems using data that is held and controlled by users rather than organisations.
- Minimising the risk of ID theft through techniques such as data revocation (giving users the ability to delete, suspend or take back data from systems).



Key sectors exploring PbD

PbD models

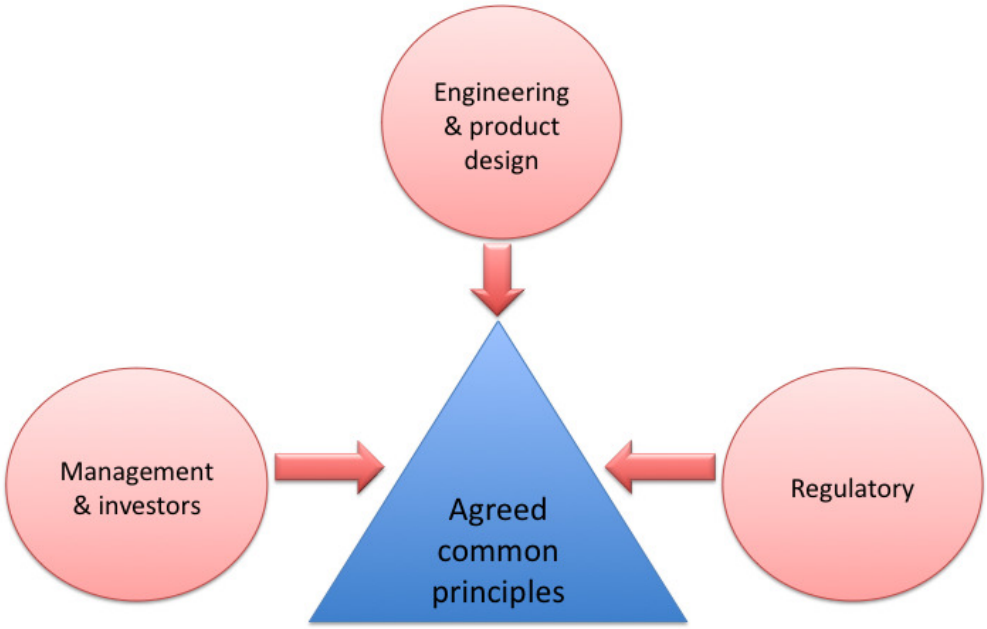
Presently, Privacy by Design is more a concept than a technique. As with risk assessments or Privacy Impact Assessments there are no agreed standards, benchmarks or even concept models. PbD proponents frequently find agreement on the common challenges rather than specific solutions; however, this syndrome has been symptomatic of any complex design evolution, no matter what the sector.

However, it is clear that the drivers behind PbD appear to reside (approximately) in two domains: regulatory and engineering. There is significant overlap between the two.

The regulatory push for PbD is perhaps most notably made by Ontario's Information & Privacy Commissioner, Anne Cavoukian and by her German counterparts, who have led the regulatory community on this concept.[7] While demonstrating a keen awareness of the importance of technology-led privacy solutions, Cavoukian has taken a 'softer' approach to PbD than some engineers in the field. In her model, compliance with privacy, data protection and fair information practices become both the road-map and the principal objective of PbD. The most obvious advantage of this approach is that it lends itself to the potential for a global standard and a set of agreed success benchmarks. The drawback is that the approach risks suffering the same shortcomings as a reliance on legal protections (which can invite the risk of conditional protection affecting only certain circumstances).

The more technical approach, which can be seen emerging from such companies as Microsoft and Mydex, appears to place a stronger emphasis on engineering solutions. This resonates with the cryptographic approaches proposed from the 1980s which mathematically "lock down" privacy to avoid circumvention of the protections. Some privacy advocates argue that the chief drawback of such engineering solutions is that they run the risk of becoming modular by nature, and fail to achieve a harmonious framework that extends beyond the purely technical aspects. In the purist engineering model, solutions are found for particular processes; but, if care is not taken, the whole system, or the organisation as an entity, fails to meet such standards.

Some approaches, notably the 2008 report published by the UK Information Commissioner[8] acknowledge both approaches, but quite pragmatically provide a sharper focus on the organisational reforms that are required prior to adopting PbD. In this approach, substantial recognition at management level is required to pave the way for a comprehensive PbD.



Three appoaches to PbD

The current regulatory system of privacy protection has been described as "soft privacy", and is reliant principally on trust. The engineering model involving "hard privacy" requires a much

7 http://www.privacybydesign.ca/

8 *Privacy by Design, authored by the Enterprise Privacy Group. Published by the UK Information Commissioner's Office, 1998* http://www.ico.gov.uk/upload/documents/pdb_report_html/index.html

smaller degree of trust (or, at least, trust at a more focused level), and establishes concrete protections at a cryptographic level.

It was perhaps always to be expected that there would be a partial "disconnect" between the regulatory, management and engineering worlds in the adoption of PbD. Ontario offers a superb motivational platform, but provides little substantive engineering advice.[9] Meanwhile, papers on privacy engineering tend to focus on specific IT challenges in isolation from an organisation's decision-making processes or business model. Many engineers tend to downplay the substantial role of business managers in any successful PbD approach. Conversely, business managers who are required to pay attention to options for stronger privacy mistakenly believe that added protections must come at a cost to the organisation and fail to understand the core messages from regulators and engineers.

One of the key challenges for organisations is the process of establishing and engaging the entire ecosystem. Defining the scope and nature of that ecosystem can be daunting. Decisions must be made about whether for example suppliers and vendors should be included. A successful PbD approach needs to take into account the complete chain of inputs and outputs.

Bridging the three worlds is proving to be a difficult task. To achieve traction, a PbD system must facilitate a common understanding between engineers, regulators and managers.

The core principles

The high level principles that might underpin Privacy by Design have been articulated in the Ontario model.[10] Most are motivational and aspirational, but they do provide the potential for a common vision for all stakeholders:

1. **Proactive not Reactive; Preventative not Remedial**
   The Privacy by Design approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, PbD comes before-the-fact, not after.

2. **Privacy as the Default**
   Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

3. **Privacy Embedded into Design**
   Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

---

9 *Some high level assessment has however been published by the office including* *http://www.springerlink.com/content/v2265x6u68535712/fulltext.html*

10 *These can be downloaded from* *http://www.privacybydesign.ca/about/principles/*

4. **Full Functionality – Positive-Sum, not Zero-Sum**
   Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. PbD avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. **End-to-End Security – Lifecycle Protection**
   Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, PbD ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. **Visibility and Transparency**
   Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. **Respect for User Privacy**
   Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

These principles play well in the regulatory and advocacy environment because they articulate a set of goals which are largely (to those groups) self evident. Principles articulated in the Ontario model resonate with regulators because of a "common sense" approach that is underpinned by the language and logic of regulatory principles.

However, such models sometimes suffer from a lack of synergy with the majority of business managers. And while the Ontario model argues for a "win win" approach, the statement "No action is required on the part of the individual to protect their privacy — it is built into the system, by default." is controversial in many industry circles because it appears on the face of it to argue for an opt-in approach to the disclosure of personal information – something that is almost genetically opposed by many companies.

At this early stage of development of PbD, and with relatively few management and engineering alternatives, such fears are understandable, though in some circumstances those fears are groundless. A pragmatic engineering solution conducted in concert with business managers can provide innovative approaches to privacy protection which reduce risk for the organisation and the customer without compromising the value of data. Such approaches recognise the importance of the business model but work within those constraints to establish reduced risk through data minimisation.

For engineers, the principles might be substantially different to the regulatory approach. The technological challenges are substantial, and require a more fine-grained approach to PbD. Engineers such as George Danezis, who has worked extensively on privacy related IT problems, have continued the process of peeling back the core elements of the engineering component of PbD and have started to develop principles that cover the following ground:

1. At the functional level, define clearly what you want to do and ensure that this process in itself is not invasive.
2. Rigorously establish the minimum inputs necessary to achieve the required functionality.
3. Build a solution that achieves a balance between integrity of service and that discloses the minimum amount of information.
4. Push the processing of private information to user devices and away from central systems.
5. Use advanced cryptography to facilitate integrity and privacy.

Some emerging areas of PbD implementation are succeeding in bringing together the administrative and engineering strands. For example, the Electronic Proof of Earnings Card in Germany embraces the following design principles[11]:

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

---

11 *Discussed in http://www.springerlink.com/content/f8n9387386r704g7/fulltext.html by Peter Schaar, Germany Federal Data Protection Commissioner*

Each of these areas requires sensitivity to other business needs such as adherence to lawful requirements for data retention (tax or communications data) or revenue issues (such as shunting data to third parties for advertising or commercial sales leads). While engineering principles themselves form the core of a Hard Privacy approach, they would be largely meaningless without a realistic foundation that rests on the *modus operandi* of the organisation.

However, PbD embraces the crucial element of data minimisation and, within such a framework, the requirements for retention of personal data or subsequent disclosure of that data to authorities would be substantially reduced. Without the requirement to act – in effect - as agents of the state, business costs are possibly reduced and a higher level or trust and privacy can be established. As the European Data Protection Supervisor has observed:

It is also clear that the concept of PET is closely related to the principle of "data minimization" that is now widely used, and gradually developed into the principle of "Privacy by Design" that is not only relevant for information technology systems, but also for organizations and methods in general, and thus also for "more effective" data protection authorities. [12]

Some exciting tools are being adopted that might assist a more dependable PbD formula across organisations. The notion of *Differential Privacy* in which a mathematical approach is taken to determining the privacy value of data may, in time, create a common standard which might form the basis of agreement on the common foundation of PbD techniques. The Differential Privacy approach itself is currently little understood in the general business community as it dramatically challenges, in a complex way, more traditional legal and political approaches to privacy protection by instituting a hard ceiling at a mathematical and engineering level on the storage and exploitation of data.[13]

Falling victim to fashion

One of the most striking features of Privacy by Design is the contrast between the popularity of the concept and the actual number of systems and infrastructures that use the technique. PbB has become a fashionable idea, and in the wake of fashion came the pretenders that falsely claim their organisations or products have a genuine commitment to the PbD process.

Many PbD efforts are false, selectively assessing a particular strand of the organisation to lower the risk of criticism, or creating a modular approach that selectively fits the organisation's structure. There are some notable exceptions but the overriding challenge is to identify instances where a PbD effort has been undertaken with the full consent of all stakeholders within an organisation.

PbD appears to be increasingly adopted at the level of principle by large companies and sectors. The mobile phone network provider organisation GSMA for example has announced that it is attempting the development of a set of global privacy principles for mobile based on a PbD process. The need for collaboration to be established with handset manufacturers and apps stores is central to a PbD approach in this instance, but such seismic positioning is fraught with logistical problems that would confront any sector attempting an integrated approach to privacy protection.

However, the key messages embraced by PbD have not been lost on regulators. In Europe, for example, the RFID industry is required by the European Commission to establish a PbD

12 *http://www.springerlink.com/content/8258q1566232h0u4/fulltext.html*

13 *See the work of Cynthia Dwork and others at http://en.wikipedia.org/wiki/Differential_privacy for a general background to Differential Privacy.*

process that will bind the industry to a set of privacy conditions that should provide assurance that privacy is embedded seamlessly throughout the design and deployment aspects of the technology.[14]An industry-led first draft of these principles has been rejected by the Article 29 Working Party of privacy commissioners.[15]

The European Data Protection Supervisor has also signalled a possible embedding of PbD into the basis of data protection law, which might ultimately create a general requirement:

[I]t would be important to include the principle of "Privacy by Design" among the basic principles of data protection, and to extend its scope to other relevant parties, such as producers and developers of ICT products and services. This would be innovative and require some further thinking, but it would be appropriate and only draw the logical consequences of a promising concept.[16]

Facing the challenge

In discussing how Privacy by Design can evolve from a simple concept, popular as it may be, into concrete enhancement of privacy in particular on the Internet, a number of questions need to be addressed:

- As a preventive mechanism PbD needs to be implemented at the earliest possible stage; what should be done to make sure that the relevant expertise is available at that stage?
- What can be done to help smaller organisations deal with this challenge?
- Does the presence of privacy expertise at an early stage risk nipping promising new services and tools in the bud? How can this be avoided?
- Should PbD focus on making products "litigation proof" or is the purpose to raise privacy to the highest possible levels regardless of the existing legal requirements?
- If the previous question is answered in favour of the second option, how can PbD then be promoted? Is market pressure the only realistic tool?
- What needs to be done to make consumers aware of the privacy protection (or lack thereof) offered by certain products and services or their providers?
- Is there a role for third party certification or more generally for third parties?
- How can regulators help? Should there be recognition of the presence or absence of PbD when a product or services is found to be violating privacy laws? Should the application of PbD result in lower fines?

---

14 *COMMISSION RECOMMENDATION of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification http://www.rfidjournal.com/article/view/4890*

15 *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications Report http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm*

16 *http://www.springerlink.com/content/8258q1566232h0u4/fulltext.html*

Conclusions

The emergence of PbD presents a substantial opportunity to raise the bar on privacy protection and to reduce the extent of surveillance of people's data and transactions. However, these are early days and much needs to be accomplished before the idea achieves traction in either the private or the public sector.

The three key perspectives in Pbd – regulatory, engineering and managerial – do involve significant intersection but, while the concept continues to run along divergent paths, there is a substantial risk that the technique will be characterised by difference rather than convergence. More interaction and dialogue is required involving regulators, business managers and engineers.

Currently, the evolution of PbD is being conducted sporadically. This dynamic is true for the early development of all such techniques. If proponents of PbD are arguing for an integrated and seamless adoption of systems, then they must argue with equal vigour for an integrated approach to developing PbD as a practical framework. Without such an approach, investors will remain uneducated and unmotivated and the PbD concept will remain a largely theoretical concept, adopted by a small number of the “good” privacy actors.

About the author

Simon Davies is widely acknowledged as one of the foremost privacy advocates in the world, and is one of the pioneers of the international privacy arena.

His work in the fields of privacy, data protection, consumer rights and technology policy has spanned more than 25 years. Simon is perhaps best known as the founder and Director of the watchdog group Privacy International, but is also an academic, consultant, journalist and author.
Simon has been a Visiting Fellow in Law at both the University of Greenwich and the University of Essex, and for the past ten years has been Visiting Senior Fellow and lecturer in the Department of Information Systems in the London School of Economics, where he teaches the MSc course in "Privacy & Data Protection". He is also co-director of the LSE's *Policy Engagement Network*.

He has also advised a wide range of corporate, government and professional bodies, and has worked on technology, privacy and identity issues in more than forty countries. As MD of the IT development and advisory company 80/20 Thinking Ltd Simon is also working closely with many of the market leaders in Web 2.0 and comms on the development of technical solutions to privacy protection.

Simon's work has put him at the forefront of numerous issues, including the debate over proposals for government identity systems, the ethics of CCTV surveillance, human rights law and the data trade between Europe and the United States.

In April 1999 he received the Electronic Frontier Foundation's "Pioneer" award for his contribution to the development of the Internet. In both 2004 and 2005 Silicon.com voted him as one of the world's 50 most influential people in technology policy. In 2007 he was made a Fellow of the British Computer Society. He has published widely in academic publications and is regularly invited to speak at conferences and functions.

About ICOMP

ICOMP, the Initiative for a Competitive Online Marketplace, is an industry initiative for businesses and organisations involved in Internet commerce. Its overall objective is the sustainable growth of the Internet and key goals are to encourage competition, transparency, data privacy and respect for intellectual property protection as well as the adoption of best practices to promote online creativity, innovation, safety and trust.

As an organisation concerned with the Internet, ICOMP brings together companies operating in the online marketplace across content, infrastructure and services sectors to identify and promote best practices. ICOMP helps to educate and inform stakeholders and decision-makers on how the online marketplace functions and the challenges being faced by those who operate within it.

Over 55 companies, trade associations, consumer organisations and individuals are members of ICOMP and have endorsed ICOMP's principles. These members represent 14 countries across Europe, North America and the Middle East. Microsoft is ICOMP's founding trustee, Burson-Marsteller acts as its Secretariat, and Lord Alan Watson is ICOMP's Chairman.