Data Protection Law & Policy, Volume 4 Issue 11 November 2007

Opinion: The Future of Privacy (part 1) - Privacy 1.0 and the need for change

As information technology continues to evolve, regulators, privacy practitioners and citizens are increasingly questioning the suitability of current privacy frameworks to allow the effective processing of personal data whilst safeguarding individual privacy. In the first part of a two-part article, Christopher Millard, Partner at Linklaters LLP, suggests that current approaches to privacy regulation are fundamentally flawed. In particular, Millard argues that most privacy legislation is incompatible with the architecture of the internet and that the imposition by EU member states of bureaucratic obstacles destroys the usability of pre-approved rules which are supposed to facilitate simplified compliance procedures[1].

Does privacy have a future in an online world?

"You have zero privacy anyway. Get over it!" So declared Scott McNealy, then CEO of Sun Microsystems in 1999[2]. His statement caused quite a stir when it was first reported and it has since been quoted many times in various forms. It seemed to resonate with many internet enthusiasts, who believed that activities conducted in cyberspace were somehow beyond the reach of governments and law enforcement authorities and would, ultimately, prove immune to regulation. Is this assumption correct? I have long considered the view that the internet is 'beyond the law' to be misconceived and, in a 1996 article, characterised it as "cyberspace and the 'no regulation' fallacy"[3]. On the contrary, far from being unregulated, from the early days of Web 1.0 it was clear that nothing in history had ever been subject to as many laws and regulations as activities which took place online. That was not to say that interpretation, application and enforcement of those rules in the internet context was going to be easy, or that there would not be numerous conflicts of laws. Nevertheless, the internet has never been beyond the rule of law.

At the end of 1999, Lawrence Lessig published, to great acclaim, *Code and Other Laws of Cyberspace*[4], since substantially rewritten as *Code Version 2.0*[5]. In this book Lessig argues that cyberspace is not only inherently 'regulable'; it can in fact be regulated to a much greater extent than the offline world. This is because rules can be embedded as code in the 'architecture' of the internet. Businesses, as well as governments, will have an ongoing role to play in this process. Especially powerful are controls that are built in, or hard-wired, into the architecture, or fundamental design, of technology and related business systems and processes. For Lessig, "law as code" is a key concept. I will return, in part 2 of this article, to a related concept of privacy by design and the important role that privacy standards might play in the future. But first, what about privacy regulation today?

Who's unhappy with the status quo?

So, Scott McNealy overstated his case and, to be fair, he was probably aiming to be provocative. However, looking at how the current privacy environment, let's call it 'Privacy 1.0', is working in practice, it is clear that there is something wrong. It is not just that organisations that are subject to privacy regulation are complaining about the burdens of compliance. In addition, there are signs of growing apathy amongst the constituencies that privacy laws are supposed to protect. For example, many members of social networking communities such as Facebook and MySpace appear not merely willing, but almost eager, to disclose and even broadcast vast amounts of personal data. Some of this data is highly sensitive (in every sense of the word); it may be shared with people who are barely known and even with complete strangers, or at least people whose identities cannot be verified. Sometimes this appears to be due to ignorance on the part of users of these sites. Indeed, when alerted to the consequences of the way in which they have configured their privacy settings, some users elect to limit the disclosure of their personal data. Nevertheless, there is perhaps a risk that privacy will increasingly be perceived by many as irrelevant.

Most surprising, however, are the signs of growing discontent amongst privacy regulators. International co-operation on privacy matters has a long history. The work of Expert Groups established by the Organisation for Economic Cooperation and Development (OECD) in 1974 and 1978 led to the adoption by the OECD of *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980. Soon thereafter, in 1981 the Council of Europe adopted its *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*[6]. However, the most integrated and proactive group of specialist privacy regulators is that established under Article 29 of the European Union's Data Protection Directive[7]. This group has made a considerable effort to present a united front and has stated repeatedly that it will act in a co-ordinated fashion. In the past five years, however, reading between the lines of the Working Party's increasingly prolific output, evidence of lively, and sometimes contentious, debate has not been far below the surface. For example, a key paper on Binding Corporate Rules published in 2003 was clearly a compromise document to which some of the national data protection authorities had subscribed only reluctantly[8]. In the last couple of years, it has become clear that a small, but increasingly vocal and growing minority of regulators is not prepared to wait indefinitely for reform of the cumbersome bureaucratic infrastructure that has grown up around privacy regulation in Europe.

In this article I will argue that privacy laws and related regulatory processes in many countries, and in particular the EU Member States, are today badly flawed. However (with apologies to Mark Twain), I still think that rumours of the death of privacy are greatly exaggerated. I remain confident that McNealy will ultimately be proved wrong and Lessig will be proved right. I will review current debates amongst regulators and the business community as to the direction that privacy should take and will look at what

privacy regulation might look like in the future.

So what's wrong with the current approach to privacy regulation?

'Modern' data protection laws first appeared in 1970 (in Germany)[9] as a response to the early use of computers to process information about people. At that time, however, there were relatively few computers, and most were in the public sector or academia, plus a few large corporations. Moreover, these machines tended to be housed in secure locations without direct connections to the outside world. For regulators, the task of tracking and supervising the processing of personal data might have been a realistic objective initially, although not for long. As for processing power, for comparative purposes, the Apollo Guidance Computer which was used to put men on the moon in 1969 was capable of processing up to 9,600 instructions per second. Fast forward to 2007: a Blackberry smartphone can now process over 1,000 million instructions per second and an IBM Blue Gene-L Supercomputer can process 360 trillion instructions per second. Undoubtedly more important than this explosion in raw processing capability, today we have massive, and rapidly expanding, connectivity with a world internet population of 1.25 billion and mobile phone subscriptions predicted to reach 3.25 billion by the end of 2007.

Meanwhile, we are seeing increasingly confident steps towards the 'semantic web' in which computers will 'understand' each other sufficiently to undertake all manner of transactions on our behalf while we, no doubt, immerse ourselves, via our avatars, in virtual environments of various kinds (unappealing though that last part is to many people). Moreover, in developed countries at least, we appear to be moving fairly rapidly towards an environment of ubiquitous computing, as described in fascinating detail by Adam Greenfield in his recent book *Everyware*. Interestingly, Greenfield expresses the concern that "[w]e will have to accept that privacy as we have understood it may become a thing of the past: that we will be presented the option of trading away access to the most intimate details of our lives in return for increased convenience…". Though less dramatic than McNealy's extreme position, this again suggests that a dichotomy remains between technological progress and privacy.

Yet if you look at most privacy legislation, in certain key respects we are stuck with offline mainframe concepts from almost four decades ago and a regulatory environment that is well past its 'use-by' date. Take, for example, the legislation that was enacted by the 27 Member States of the European Union to implement the 1995 Data Protection Directive. By 1995, internet email was already widely used and, thanks largely to the development of Netscape's browser software, use of the web was also becoming popular. Despite the fact that it had been subjected to five years of intense scrutiny and, at times heated, debate, the 1995 Directive contained provisions that were fundamentally incompatible with the architecture of the internet. In particular, the imposition of cumbersome controls on the export of personal data clearly conflicted with pervasive international data communications, especially in the context of unstructured systems such as internet email. It may perhaps have made some sense in 1970 to expect a representative of

a government department, university or major corporation to apply for an export licence before boarding a plane with a briefcase containing a magnetic tape with personal data recorded on it. However, as some of us pointed out at the time, it made no sense in 1995 to adopt a Directive that would lead to analogous controls being imposed on millions of organisations in respect of emails being sent via the internet to any country outside the EU which did not provide an 'adequate' level of protection for personal data. The cumbersome transborder data flow rules have since been rendered even more absurd now that they can apply to the personal data stored in numerous Blackberries, mobile phones, PDAs and laptops that are carried by business travellers on flights out of the EU every day.

To make matters worse, when the European Commission attempted to simplify the compliance process by pre-approving standard contract clauses for organisations to use as a framework for transfers of personal data, some two thirds of the EU member states promptly destroyed the usability of those clauses by imposing bureaucratic obstacles by way of filing or approval requirements. A further attempt to introduce a form of self-regulation via Binding Corporate Rules has also been hampered significantly as a result of the adoption by a number of national regulators of an overly bureaucratic approval process. In addition to these restrictions on international data transfers, most EU countries still require businesses to submit filings (also called notifications or registrations) in relation to their in-country data processing activities. Since it is difficult to see how this bureaucratic obligation either serves to protect the public or assist regulators in their work, in most cases it amounts to nothing more than a data tax by another name. In a number of countries, however, significant resource is focussed by regulators on enforcing such filing requirements as this is the primary means by which their offices are funded! Harsh though it may seem, in most of the EU, complete regulatory paralysis is avoided only due to a combination of widespread non-compliance and the fact that enforcement activity is extremely limited. This is certainly the case in relation to transborder data flows, for which the vast majority of organisations do not yet have in place appropriate arrangements. Even when businesses have attempted to put in place a comprehensive contractual structure to cover data exports, only a very small minority have then gone on to make the requisite filings with all relevant regulators. This is not particularly surprising given how unnecessarily cumbersome and bureaucratic the filing or approval process for international transfers has become in many EU countries.

Is the current EU model sustainable?

Despite widespread criticism of the EU Directive from business organisations and independent commentators, in March 2007 the European Commission informed the European Parliament and the Council of Ministers that it considered that the Directive 'fulfils its original objectives' and announced that it had no plans to amend the Directive[10]. This was a considerable disappointment to many, including a reform-minded group of EU privacy regulators which had made little secret of the fact that it was looking for an overhaul of the Directive at the first available opportunity.

One of the most outspoken, the UK Information Commissioner, Richard Thomas, gave a provocative speech in Washington DC (backed up with a press release) just two days after the European Commission's statement that it had no intention to amend the Directive. Calling for a "greater global consensus on privacy", Thomas suggested that "European laws may need some revision to achieve a closer consensus" and stressed that "the European Union [must] be ready to consider changes."[11] He has since been reported as stating in September 2007 at a meeting of the Data Protection Forum in London that the Directive is "highly confusing and overly prescriptive", that the European Commission's review was "deplorably complacent" and that it is time to start a debate on changing the Directive[12].

Christopher Millard

1. Part 2 of this article will assess the prospects for change from the perspective of privacy regulators as well as reviewing calls from the global business community for a fresh start. It will also address the questions of what Privacy 2.0 might look like and when it might arrive.

2. Wired Magazine, 26 January 1999, http://www.wired.com/politics/law/news/1999/01/17538

3. Millard & Carolina, 'Commercial Transactions on the Global Information Infrastructure: A European Perspective', The John Marshall Journal of Computer & Information Law, Vol XIV, No. 2, Winter 1996, 269-301 at 271.

4. New York, Basic Books

5. New York, Basic Books, 2006

6. European Treaty Series, no. 108.

7. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

8. WP74, 'Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers', available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

9. Hessisches Datenschutzgesetz (HDSG), 30 September 1970, Hess. GVOBL I 1970, P 625. This was a state law in Hessen. The first national law was the 1973 Swedish Data Act, as amended in 1997. Since then, over 50 jurisdictions around the world have enacted omnibus data protection legislation, see Millard & Ford (eds), Data Protection Laws of the World (Sweet & Maxwell, London, 1998).

10. 'Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive', COM(2007) 87 final, Brussels, 7 March 2007

11. 'UK Information Commissioner calls for greater global consensus on privacy', Press Release, 9 March 2007, available at http://www.ico.gov.uk/upload/documents/pressreleases/2007/doing_global_privacy_better_09_03_07.pdf

12. Thomas launches critique of the EU DP Directive, Privacy Laws & Business International Newsletter, October 2007, p 7.

Data Protection Law & Policy, Volume 5 Issue 1 January 2008

Opinion: The Future of Privacy (part 2) - What might Privacy 2.0 look like?

In part one of this two part opinion piece, Christopher Millard looked at the current status of the data protection model that has been evolving since the 1970s, especially in Europe, and concluded that it is seriously flawed. He noted that the European Commission's recent announcement that it has no plans to revise the EU Data Protection Directive provoked a critical response from the UK Information Commissioner. This month he assesses the appetite for change amongst other privacy regulators and in the global business community, before considering what Privacy 2.0 might look like and when it might arrive.

Are international privacy regulators prepared to support change?

In challenging the status quo, the UK Information Commissioner, Richard Thomas, is not a lone voice in the regulatory community, either within the EU or beyond. That he has the backing of a wider group has been evident since the publication in November 2006 of a statement entitled: 'Communicating Data Protection and Making it More Effective'[1]. Also known as The London Initiative, this document was developed from a speech given six months earlier by Alex Turk, President of the French Data Protection Authority (the CNIL). The statement - which was a joint initiative of the CNIL, the European Data Protection Supervisor and the UK Information Commissioner, with the support of the Canadian, German, Spanish, Italian, Dutch, New Zealand and Swiss regulators - called for a realistic review of the effectiveness of the work of each national privacy regulator. Among other things, they acknowledged: 'We must all prioritise, especially by reference to the seriousness and likelihood of harm. We must primarily concentrate on the main risks which individuals are now facing and be careful not to be excessively rigid or purist on issues which do not deserve it. We must be ready for more pragmatism and more flexibility'.

One practical area where privacy regulators as a group internationally are supporting innovation, is in relation to technical standards for privacy. At the 2005 International Conference of Data Protection and Privacy Commissioners, they issued the Montreux Declaration[2] calling on NGOs, such as business and consumer associations, to develop 'standards based on or consistent with the fundamental principles of data protection'. The Declaration also appealed to 'hardware and software manufacturers to develop products and systems integrating privacy enhancing technologies'. Two years later, in September 2007, the Commissioners adopted various resolutions in support of the International Standards Organization's (ISO) privacy-related standards work[3]. In addition, in the key area of identity management, the Ontario Information and Privacy Commissioner, Ann Cavoukian, has been promoting a specific initiative known as the '7 Privacy- Embedded Laws of Identity'[4]. This proactive approach to privacy

by design seems entirely consistent with Lawrence Lessig's prediction that, in the future, privacy law and regulation will increasingly be embedded in the architecture of systems and processes (as discussed in part one of this article)[5].

Is the global business community ready for Privacy 2.0?

More recently, Google has sparked an international debate about privacy standards via a speech by Peter Fleischer, Google's Global Privacy Counsel, at UNESCO on 14 September 2007[6]. This was followed up a few days later with an article by Eric Schmidt, Google's CEO, which was published in the *Financial Times* and elsewhere[7]. Fleischer asked how we might best "update privacy concepts for the Information Age" and called for the creation of "minimum standards of privacy protection that meet the expectations and demands of consumers, businesses and governments". Rejecting the US approach to date as too fragmented and the EU model as too bureaucratic, he suggested that "the most promising foundation" would be the Privacy Framework adopted by the members of the Asia-Pacific Economic Cooperation Forum (APEC)[8]. The Privacy Framework contains Information Privacy Principles which overlap to a large extent with those found in the Organisation for Economic Cooperation and Development (OECD) Guidelines, the Council of Europe Convention and the EU Directive. The APEC Principles cover harm prevention, notice, collection limitation, restrictions on use, choice, integrity, security safeguards, access and correction and, finally, accountability. This last principle includes the concept of consent or due diligence in relation to international transfers. Notably absent from the Framework is the requirement to appoint an independent regulator. Moreover, the APEC Principles are in general perceived as a somewhat weaker framework than that described in the OECD Guidelines. Perhaps not surprisingly, privacy activist groups - such as the Electronic Privacy Information Center - have been quick to criticise Google's initiative as an attempt to promote support for a relatively weak privacy standard which would give consumers less protection than they have in many countries today[9]. It is undoubtedly the case that a global standard based on the APEC Principles would, in certain respects, be less onerous for businesses than, for example, most national laws in the EU. However, as Fleischer rightly observes, the EU model is "too bureaucratic and inflexible". Indeed, that is to put the case diplomatically. For the reasons given earlier, the EU's model for privacy regulation, as implemented currently in most EU member states, has largely failed and is at the very least in need of fundamental reform.

Some of the recent calls for a new approach to privacy regulation have come from unexpected quarters. In the United States there is a long tradition of regulating privacy in an *ad hoc*, piecemeal fashion and this has given rise to a 'patchwork quilt' of state and federal laws covering a range of different issues. In 2006, partly in response to the challenges of dealing with incompatible state laws requiring businesses to publicise security breaches that might put individuals at risk of identity theft (commonly called 'breach notification' laws)[10], the Consumer Privacy Legislative Forum issued a Statement calling for comprehensive harmonised federal

consumer privacy legislation[11]. The Forum was started by eBay, Hewlett-Packard and Microsoft, but by the time of the Statement, had expanded to a dozen major corporations. The Statement was significant for two reasons. First, it was a call for an omnibus federal privacy law. Secondly, it was initiated by businesses, not privacy activists, legislators or regulators.

What might Privacy 2.0 look like?

At the heart of any new model will remain a set of privacy principles designed to protect individuals and to determine what businesses and other organisations can do with the personal data they collect and subsequently use for whatever purpose. While there is clearly a debate to be had at the margins, there is widespread acceptance of the core principles of good information governance in relation to personal data which can be found in broadly similar form in the 1980 OECD Guidelines and the 1981 Council of Europe Convention. A more recent statement of fair information practices on which a broad consensus has been reached can be found in the Global Privacy Standard (GPS)[12]. The GPS was tabled and accepted on 3 November 2006 at the 28th International Data Protection Commissioners' Conference in the UK. Among other things, the GPS is intended to assist in the development of 'information and technology standards, specifications, protocols, and associated conformity assessment practices'. Although criticised by some as a weaker model, the more recent APEC Principles add an important dimension with their focus on harm prevention. This principle has been recognised by a number of influential privacy regulators as a key driver in guiding their enforcement strategies.

Privacy 1.0 went badly off the rails by getting bogged down in bureaucratic processes. As a result, the focus in many jurisdictions shifted away from the individuals that privacy laws were supposed to protect, and onto regulators and their administrative requirements. In Privacy 2.0, the focus should shift back to individuals and the long-established core privacy principles relating to transparency (including meaningful information provision), data quality, choice (where appropriate), data security and remedies (such as correction of mistakes and compensation for actual harm).

It is true that while there has been a high degree of consensus for some forty years now as to what should constitute the basic privacy principles, there have been material disagreements, especially recently, as to the application in practice of some of those key principles. For example, the right of individuals to find out whether information is held about them and to have access to that information is a core principle in the OECD Guidelines, the Council of Europe Convention, the EU Directive and the APEC Privacy Framework. This can be problematic in practice, however. The volume and complexity of information about individuals held by many organisations has exploded. For example, an employer may have an enormous amount of data relating to a long-term current or former employee, including tens or even hundreds of thousands of emails sent by, received by, copied to or containing references to that individual. Software tools are now available

which make it possible for emails to be extracted from systems on that basis. However, the EU Directive's apparently expansive concept of 'personal data' is currently interpreted very differently in various Member States. For example, in the UK following the Court of Appeal judgment in the Durant[13] case, it may be that most of the emails in the scenario just described will not need to be disclosed to the employee or ex-employee because they will not be deemed to contain 'personal data'. In some other Member States, it may be that all of the emails will be deemed to contain personal data simply because they contain the individual's name. Even in the UK, however, responding properly to this kind of 'subject access request' can be extremely burdensome for the organisation concerned. This is because the organisation may need to sift through the emails and other data sources concerned to identify precisely which of them should be disclosed in full or in part. Some may need to be disclosed in full, others may not contain personal data, some may be covered by legal privilege and some may need to be redacted to remove personal data relating to other individuals. For organisations that receive subject access requests with a cross-border element, the current lack of harmonisation can be a nightmare. This may prove to be one of the more difficult areas for the development of next-generation privacy principles, but the *status quo* is not sustainable.

What is absolutely clear from the European experience is that bureaucratic red tape should be eliminated ruthlessly. For example, legislators or regulators that wish to establish or maintain filing or registration systems should be made to demonstrate that the imposition of such burdens on organisations really does benefit individuals. A possible compromise in that regard, perhaps for a transitional period, might be to dispense with filing requirements where organisations can show that they have appropriate internal information governance structures in place. Encouragingly, Sweden has recently followed the example of Germany in providing broad exemptions from such requirements for organisations that appoint a privacy officer. Sadly, some national regulators currently have little choice but to defend the continuation of registration or notification systems that create substantial burdens for organisations yet do little or nothing to protect the public. This is because those regulators depend, directly or indirectly, in whole or in part, on the fees generated by such filings!

In a Privacy 2.0 environment, I would expect to see privacy regulators getting much more involved in addressing harm in three main ways. First, by promoting 'privacy by design'. Secondly, by providing the public with accessible and practical guidance regarding management of privacy risks. Thirdly, by taking targeted and co-ordinated enforcement action with the objective of discouraging future harm. Taking each in turn, a number of privacy regulators are already strong advocates of embedding privacy into systems and processes. One is Peter Hustinx, formerly President of the Netherlands Data Protection Authority and since 2004, European Data Protection Supervisor[14]. Another, mentioned already in relation to identity management, is Ann Cavoukian, Ontario's Information and Privacy Commissioner[15]. A good example of commonsense guidance can be seen in the microsite for teenagers launched recently by the UK Information

Commissioner's Office, which includes practical tips on managing risks associated with posting data on social networking sites[16]. As for targeted enforcement activity, this is an area where the UK Information Commissioner has already started to put into practice the risk-based approach to enforcement agreed as part of the London Initiative, for example by extracting undertakings from financial institutions in relation to alleged security breaches[17].

A difficult challenge for Privacy 2.0 will be ensuring that legislation and regulatory practice are, to the fullest extent possible, both technologically neutral and able to accommodate the very specific technical issues that will continue to arise. With the development of the semantic web (where it is expected that software 'agents' will undertake transactions on our behalf), further deployment of location-based eCommerce services, and widespread adoption of RFID, to give just a few examples, it seems highly likely that technological developments will continue to challenge the ability of legislators and regulators to respond effectively. While the basic principles of privacy regulation have proved robust and flexible, it may continue to be appropriate to add specific overlays, either in the form of legislative rules or regulatory guidance. Ideally, however, this should be done on a multi-lateral basis following informed international debate and not on a specific unilateral basis at a more local level. A recent example of the latter approach, to add to the existing fragmentary legislative patchwork in the US, was the signature into law by Governor Arnold Schwarzenegger on 12 October 2007 of a Californian Bill which, since 1 January 2008, has made it illegal for anyone (e.g. an employer) to force anyone else to have an identification device, such as an RFID chip, implanted under his or her skin[18].

How soon might we expect to see Privacy 2.0?

There are two ways of looking at this. In an ideal scenario, it might be best to start again with all relevant stakeholders around a table to agree a new international convention, supported by the best possible technical standards and Privacy Enhancing Technologies (PETs). As many countries as possible would then be persuaded to sign and ratify that convention and implement it promptly and in a consistent fashion in their national laws. Thereafter, regulators worldwide would collaborate to ensure that they interpreted and enforced the rules in a seamless manner. The technology industry and all relevant service providers would also immediately facilitate the adoption of all approved privacy standards and PETs.

Reality 1.0 (and probably all future versions!) is a great deal messier than that. The emergence of Privacy 2.0, if it happens at all, is more likely to resemble the development of an open-source software product or, perhaps, a wiki or other collaborative Web 2.0 project. There will be ongoing debates, and probably quite a few arguments, over design, scope, enhancements, implementation, and so on. However, the good news is that in this looser sense the development process seems already to be underway with the starting gun having been fired with the recent calls for radical change that have emanated from both regulators and industry.

Moreover, specific work has begun on ISO privacy standards and at least some national privacy regulators have made material changes already to their enforcement practices. There are promising signs that the recent momentum will be sustained.

Christopher Millard

1. Available at http://ico.crl.uk.com/ files/ComE.PDF

2. The protection of personal data and privacy in a globalised world: a universal right respecting diversities, available at http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf

3. Resolution on Development of International Standards, available at http://www.privcom.gc.ca/information/conf2007/res_global_05_e.asp

4. 7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age, available at http://www.ipc.on.ca/images/Resources/ up-7laws_whitepaper.pdf

5. Millard, 'Privacy 1.0': the need for change, Data Protection Law & Policy, Vol 4, No. 11, Nov. 2007, p. 7-9.

6. The Need for Global Privacy Standards, available at http://peterfleischer.blogspot.com/2007/09/need-for-global-privacystandards.html

7. Global Privacy Standards are Needed, available at http://www.ft.com and at http://peterfleischer.blogspot.com/2007/ 09/eric-schmidt-on-global-privacy.html

8. Available from http://www.apec.org/

9. For example, see letter to the editor of the Financial Times by Marc Rotenberg, President of EPIC on 24 September 2007, available at http://www.ft.com

10. Such laws have continued to proliferate. By the beginning of 2008 there were some 40 breach notification laws at state level in the US: http://www.ncsl.org/programs/lis/cip/priv /breachlaws.htm

11. Available at http://www.cdt.org/privacy/20060620cplstatement.pdf

12. Available at http://www.ipc.on.ca/images/Resources/up-gps.pdf

13. Michael John Durant v FSA, CA [2003] EWCA Civ 1746.

14. Peter Hustinx has been promoting 'privacy by design' for many years. For a recent example, see the December 2007 EDPS opinion on RFID: http://euramis.org/rapid/pressReleasesAction.do?reference=EDPS/07/13&format=HTML&aged=0&language=EN&guiLanguage=en

15. A recent lecture on the topic by Ann Cavoukian at the University of Toronto entitled 'Privacy by Design' is available here: http://www.ipc.on.ca/ links/privacy_by_design.asp

16. http://www.ico.gov.uk/youth.aspx

17. See Information Commissioner's Office Press Release, 13 March 2007: http://www.ico.gov.uk/upload/document s/pressreleases/2007/banks_in_unacceptable_data_protection_breach.pdf

18. An act to add Section 52.7 to the Civil Code, relating to identification devices, Senate Bill No. 362 (now Cal. Civ. Code Section 52.7). This makes California the third state, following the lead of Wisconsin and North Dakota, to ban forcible implantation of such devices in humans.