SCRIPT-ed

Volume 3, Issue 4, December 2006

Introduction

Lilian Edwards[*]

This Special Issue of SCRIPT-ed grew out of a Workshop on Privacy and Technology which was convened at Edinburgh in September 2005 under the auspices of the AHRC Centre for Research into Intellectual Property and Technology Law. Its aim was to look at the concept of privacy regulation in the widest sense, as it is affected by, and affects, technology and the information society. Participants were drawn from the worlds not just of law and academe, but also from the software industry, from medicine, from sociology and politics, from civil society and digital rights groups, and from regulators and government. Representatives came from far and wide: from *inter alia* the UK, EU, United States, Canada, China, Hong Kong, Australia and South Africa. Discussion, as intended, was fierce and no holds barred, with the editor of this collection herself on the end of several knock-out blows as she attempted to explain her personal version of privacy as a human right. The intention was to generate new, interdisciplinary, bold and imaginative perspectives on various aspects of cyber-privacy law, and my belief is that we not only succeeded but that the proof is in the products of that workshop, namely, this collection of essays.

---

[*] Professor of Internet Law, University of Southampton; Associate Director, AHRC Centre for Research into Intellectual Property and Technology Law. L.Edwards@ed.ac.uk .

Perhaps the key starting issue in any discussion on privacy in the digitised era is whether privacy is fundamentally an inalienable human right, something which constructs a human as a subject in law, or whether it is just another commodity, an item of property which can be packaged and sold. This dichotomy throws into relief the yawning chasm in the classical discourse between the North American attitude towards privacy, especially as developed in the context of digitised databases of personal information, and that in Western Europe and the civilian legal world - with the UK poised precariously between these two poles. In her fascinating and learned contribution, Corien **Prins** attempts to grapple with this debate, taking account of both the philosophical and economic arguments for and against a property right in privacy, as well as recent court cases such as the famous *Douglas v Hello* which arguably veer towards granting such property rights, albeit paradoxically only in the privacy of those whose living it is to be public property: namely, celebrities. Prins' conclusions point towards the idea that it is not enough to simply decide that privacy can or cannot, or should or should not, be propertised: what is truly important is to analyse the *effect* such would have on, for example, limitation of misuse of personal data, and efficiency of re-use of data, especially compared to conventional human rights systems of protection of privacy such as data protection law, which although good on paper, may in reality in the digitised trans-national world of the Internet offer less protection than some property rights systems.

The EC data protection system is itself analysed from a political perspective by **Busch.** One of the key problems that arises from the dichotomy in privacy regimes, mentioned above, is how to deal with the transfer of personal data from European jurisdictions to non-DP law regimes such as the United States. Should European standards of privacy be maintained to protect European citizens, albeit causing severe difficulties for multinational businesses using personal data, or give way to the arguably laxer regime governing commercial bodies handling of personal data in the States? Or, as a "third way", should some halfway house be developed, as with the "safe harbor" agreement negotiated following the passing of the Data Protection Directive in 1998? Busch contrasts the safe harbor result, which he perceives as a "constructive compromise" between European and American norms, with the more recent PNR passenger data records transfer dispute, where the more apt description, he feels, is of a "thinly veiled victory" for the American side; and asks why these outcomes differed so. Such comparisons are valuable if we are to anticipate if increasing globalisation and multi-corporitisation will lead to a "ratchetting up" of privacy standards to a higher standard such as the EU embraces, or a "race to the bottom" as Bennett and Raab have sometimes predicted[1].

One of the key areas of concern in the post 9/11 and 7/7 world is, of course, the interaction between privacy and security. The conventional wisdom that a balance needs to be struck between the privacy of the individual, and the security of society, was much challenged at the Workshop on Privacy and Technology, not least by those delegates who had been involved as part of civil society in the World Summit on the Information Society (WSIS). Such privacy rights proponents would argue that, with some degree of thought and effort, steps can be taken which promote both a secure society and one where privacy is valued and protected. How far these goals can be coexistent and how far they are naturally antipathetic emerged at the Workshop as one of the key areas to be researched in this area.

---

[1] In their influential thesis *The Governance of Privacy* (2nd edn, 2006)

Rauhofer, in her closely-researched and polemic contribution, focuses on an area where it is hard to see any common ground between privacy and security. Data retention has become a key battleground in the ongoing turf war between defenders of human rights and promoters of national security. Knowledge is power, said Orwell, so more knowledge must arguably be more power to stop terrorists, say governments. But hang on, say privacy commissioners: retaining data beyond the purposes for which it was gathered and for indefinite terms is a recipe for misuse. Rauhofer traces the development of EU policy and law on mandatory data retention through the dark days of 2005-2006, finding that the roots of the Data Retention Directive lay in events which began long before 9/11 and exploring murky conspiratorial waters of UK and European politics. Rauhofer's ultimate view on political compromise seems rather more cynical than Busch's – that opposition can be always outflanked by "manoeuvring" where the result is politically desirable, however antipathetic to basic human rights, and that the UK Presidency's success in pushing through the Data Retention Directive was a "master class in diplomacy". It is a shame, perhaps, that these skills were not deployed to such great effect in the PNR wars Busch describes!

Ncube provides a valuable non EU perspective, and companion piece to both Busch and Rauhofer, in her account of recent South African legislation on transborder data flows and interception of communications. South Africa provides a leading example of a developing country which is self-consciously upgrading its privacy legislation to meet "adequacy" standards for the purpose of transfer of personal data from the EU. Yet as Ncube notes, simultaneously South Africa is also responding to international post 9/11 pressures by introducing a system of digital communications interception akin to the UK's Regulation of Investigatory Powers Act; and this legislation has in fact been prioritised over the general privacy legislation. Interestingly, in South Africa, a country where many people have no fixed address and where much communication is via mobile phones, security difficulties arise which have little parallel in the West, e.g. the need to provide a home address which may not exist, so that pay-as-you-go mobile telephone conversations can be tracked. In such circumstances, fundamental conflicts arise not just between privacy and security, but between security and freedom of expression, and rights of digital access. Ncube's contribution thus highlights the need, when elaborating fundamental rights for the digital age, to take account of circumstances not just in the leading technocratic states but throughout the globe.

Finally on this theme, **Bendrath** and **Joergensen** usefully provide an account of how the right to privacy was initially mainly noticeable by its absence in the debates at Geneva and Tunis during the World Summit on the Information Society (WSIS.) As the authors put it, while security was clearly promoted as a strong goal by states, only civil society groups appeared keen to prioritise privacy as anything other than a vague exception to primary rules. Encouragingly though, the later Internet Governance Forum at Athens, while primarily reported in relation to the domain name system and governance thereof, seems to have made positive steps to enshrine privacy as part of the elaboration of "digital identity" as a crucial aspect of the "Web 2.0" world which is emerging from developments such as user generated content, second generation sites, the Semantic Web and identity management systems.

Which brings us, helpfully to the most technical contribution in the collection provided by Miranda **Mowbray** of HP Labs. Mowbray provides perhaps the most

concrete illustration of how privacy might be designed into products, using code at once to protect privacy and enable security. Mowbray gives a simple (well, fairly simple:-) account of how mathematical methods can be used to generate pseudonymous identification, a technique vital to distributed identity management. In layman's terms, such techniques could allow us to have ID Cards which, unlike the current projected UK model, could still protect security by verifying who we were for certain purposes (or "identities") e.g. for access to airports or other types of public transport - without necessarily revealing our other "identities" – e.g., as political dissident, gay man or woman, or of the Muslim race. For politicians and lawyers then, the challenge is to take on board and understand the kind of systems Mowbray and her colleagues are providing, so that "privacy by design" can become the obvious first step to take, instead of the current scenario where state-commissioned computer projects, from ID cards to NHS databases, seem to be designed with privacy as an inadequate bolt-on (if incorporated at all).

Privacy and security are one set of binary opposers, commonly, perhaps misleadingly, contrasted by academics. In the consumer world of e-commerce, a less frequently debated opposition is of privacy and convenience. It is well known from study after study, that although consumers claim to be concerned about their privacy online, in reality when seeking a bargain online or browsing for information they pay very little attention to what personal details they give away while so doing: their focus is on price, brand and speed first, privacy a long way second. As is generic to consumer regulation, the problem is that consumers want jam today without worrying about their sticky fingers tomorrow. Spam, now approaching 80-90 % of all email traffic, is one of the most obvious results of consumer carelessness with their personal data. Spammers historically either gathered email addresses left visible on the Web or harvested them from the membership list of large ISPs such as AOL. Partly because of this, spam has historically been seen as a problem of invasion of privacy, namely, the misuse of personal data. In the US and to a lesser extent in the EU, therefore, its regulation has been seen as a matter of balancing the privacy rights of the individual with the rights to "commercial speech", or as we might call it in the EU, free movement of trade, of direct marketing businesses.

Matwyshyn argues cogently however that this dichotomy is now an illusory foundation for regulation. Spam is no longer simply a problem for the individual user – an invasion of their privacy – but carries wider problems for the whole of society. Furthermore, spam is now part of a larger problem of "malware" spread via "zombies": computers, usually home user machines attached always-on to broadband, which have been taken over by viruses and now respond (unknown to their owner) to commands from remote and usually untraceable "zombie masters". Such "zombie" machines are now used to spread the majority of spam, but are also used to distribute malware, keyloggers, spyware and other viruses, and perpetrate harms such as denial of service and click-fraud. Spam has also become an international problem with spam production being increasingly "outsourced" outside the US to outlaw countries such as some of the Former Soviet Union (FSU) states. Both these points lead, as Matwyshyn argues, to a need to regulate spam as a symptom of a breakdown in international cyber-security, not just as "annoying speech". In other words, spam is

now merely a symptom of the major malaise of critical infrastructure insecurity and should be taken seriously as such[2].

Finally, it is of little use for academics to talk about rights of privacy if they cannot usefully be enforced. One of the best ways to enforce a privacy regime (such as data protection law) is to audit it: to study what statistics reveal about compliance with, and the effectiveness of, the regime. **Leith**, a long time practitioner of the socio-legal critique of law as well as a leading privacy law expert, provides the coda to the collection by questioning how useful the UK system of notification (formerly "registration") of what personal data is collected by data controllers is, through the lens of empirical efforts to extract data from the UK Information Commissioner. Leith's research raises interesting questions about what the function of a public register is, and if disclosures couched in as generic terms as the data protection register notifications are, really provide any effective privacy protection to data subjects (or "the public" as they are colloquially known.) How often do consumers ever consult the notification register to find out what, say, Transport for London are entitled to do with personal information they collect via the ubiquitous London Oyster Card? And is that notification expressible in such wide terms under DP rules, that effectively TFL can do what it likes? If so, one has to question if bringing court actions for non-notification is actually a useful way to spend the very limited resources of the Information Commissioner's office.

We at SCRIPT-ed hope this collection will be as illuminating for you to read as it has been to edit. If nothing else, it should provide interesting alternative festive reading over the holiday season.

December 2006.

DOI: 10.2966/scrip.030406.265

[2] Similar views have been expressed by your editor, who will thus attempt to stop herself cheering too loudly: see L Edwards, "Dawn of the death of Distributed Denial of Service: How to kill zombies" (2006) 24 *Cardozo Journal of Arts and Entertainment Law* 23-62.