

Event date: 23 March 2010, 5.30pm



Post comments on this paper by clicking [this link](#)

Privacy and Identity in a Digital Age



Identity

The ownership, maintenance and security of one’s own identity is at the heart of an individual being able to exist in a Connected World. Public concern over identity theft and privacy is already high, and can only grow as we become more engaged online.

Naturally, the problem of identity theft is most closely associated with the growth in use of the Internet. Media coverage of the theft of thousands of credit card account holder details from a single database, or the loss of CDs containing social security numbers and claimant details for the whole country, while they have helped to illustrate some of the dangers, have erroneously portrayed the problem as a uniquely online issue. In fact, most identity theft cases in the past have been much more mundane – a credit card taken behind a counter in a shop or restaurant; the loss of a bank statement in the post.

Swedish authorities reported an increase of 30% in identity theft-related fraud in 2008, and in the same year, 9.9 million Americans apparently fell victim to identity-related fraud. But this statistic includes even a single fraudulent transaction on a credit card, and the same report noted that in well over half the cases, thieves “came into direct contact with personal information through mailed documents, trash or the handling of credit cards”. Similarly in the UK, “forwarding address fraud”, where the fraudster redirects the victim’s post to an address where he or she can then collect it, accounts for 36% of all identity fraud (source: Experian).

Nevertheless, the problem is a rapidly growing one, and driven almost entirely by the exploding digitisation of the world’s information. In the past, we had two practical defences: we had relatively little online in terms of our real identity, and the databases that contain information about us were rarely connected or correlated to each other. In other words, we were protected by the difficulty of (or our inefficiency at) retrieving and accessing even computerised data. This effect – known as ‘practical obscurity’ – has been de facto for the whole of human history; it is this effect that is being challenged and rapidly overcome by a Connected World.

The sheer ease of replicating, stealing, editing, or deleting digital information in large quantities is the problem. Coupled with the reality of increasingly connected and correlated databases, it is clear that a well-funded and knowledgeable criminal can steal more value, and create more practical difficulties for victims, more simply than ever before. The reality is illustrated in the economics – in summer 2009, it was reported that the black market cost of a complete financial identity in the UK had fallen to just £80, indicating a market rapidly flooding with information.

Privacy

In addition to the serious problem of identity control is the less financially worrying but equally invasive issue of privacy. We are used to the regular and media-driven invasion of privacy of celebrities and other public figures; there are well-worn arguments that weigh an intentionally-famous individual's right to privacy against a public right to know. But none of those arguments hold when considering the rights (or otherwise) to privacy of a 'normal' person.

Where does knowledge about an individual or his/her activities cross the line between transactional data and personal information? What should the rules be about availability and use of private records? What should be covered by privacy laws and what is fair game to be sold on and used for (say) marketing? What is privacy anyway, and are we entitled to it? If we put information about ourselves online (for example on facebook, or even on an email), can we reasonably expect it to stay private? If we look at Google Earth's Street View and see a picture of child riding a bicycle, or someone sunbathing in their garden or breaking into a car, has their privacy been infringed? Is the act of taking the photograph the infringement, or is it making it available online? Do all your holiday snaps infringe the privacy of other people on the beach? What if you put them on flickr for the world to see?

More pertinently perhaps, what happens as we move forward and make more of our information, such as medical records, fully electronic? How should governments plan to provide public services securely? Even if we cut out the regular loss of electronic records from laptops left on trains or CDs lost in transit, how will governments keep our records safe? Should we link tax, driving, medical, benefits, and other personal records to be accessible in one place for ease of citizen use, or does that introduce an unacceptable systemic weakness?

What to do?

It is clear that the computerised data genie is well and truly out of the bottle. And it is clear that both government agencies and commercial entities will store and cross-relate information more aggressively as we the world becomes more connected – whether for tax or policing purposes, or for more effective sales and marketing approaches.

Although today we see millions of people willingly handing over large quantities of personal and behavioural information to companies such as Google and facebook, it is highly unlikely that many have thought the consequences through. How do we know that information about us kept by commercial organisations is safe and not available to be abused? Today we have the Data Protection Act to protect us, but is it adequate? Can IT security keep pace with both technological change and the best efforts of increasingly sophisticated online criminals? Where is the data anyway? In a world of cloud computing, can we even know where (and in what jurisdiction) our data resides?

Perhaps we should move to a situation in which each individual controls his/her own online identity and specifies where it is and who can access it? Is this in any way realistic? Government agencies are unlikely to agree that individuals should be in control of their tax records for example. What happens when that individual is incapacitated for any reason? How will we handle the significant minority of people who have none of the requisite skills, desire or money to participate? Can we coordinate such a system on a global basis, so that we can use our credit cards or get medical treatment in America or Armenia as well as in the UK? Do we need to? And what of the immense practical difficulties, not least in changing millions of databases across public and private sectors to relate to a central identity system?

Finally, will future legal and regulatory systems prove any better at targeting problems than they are today, when the burden and costs of everyday proof so often falls on the law-abiding while having little effect on criminal activity?

Whatever the challenges and whatever the pros and cons of potential solutions, a solution must be found. The ability to combine and correlate data relating to individuals is a defining feature of a Connected World. If we are to live and interact safely and securely in it, the ability to protect who we are, and to know with whom we are interacting, is fundamental.

