Emerging Human Rights Issues

IHRC and Law Society of Ireland
8th Annual Human Rights Conference

Saturday, 20 November 2010

Presentation by Karlin Lillington
Technology Journalist & Columnist, Irish Times

Once upon a time, only select individuals led–or were forced to lead–a public life. A celebrity, a politician, a wealthy businessman or woman, a sports figure, an actor– as soon as an individual became known widely enough to be recognized on the street, to have their achievements, or perhaps their misdeeds or indiscretions, gain public interest, then to some extent, they began to lead a public life.

Now, in the age of digital technologies, all of us lead public lives, often without realizing it, and in some cases, apparently without really caring. We leave a trail of digital footprints across the electronic landscape, whether through phone, mobile or computer use. Much -- most -- of that detail is stored and can be retrieved and viewed by others, sometimes with and sometimes without our knowledge. Either way, for the most part we are unaware of the extent to which this happens.

Some of these footprints are of immediate interest to the State and are -- with dubious reasoning -- now stored for excessively long periods. For several years now, this has been the case with our call data under Irish data retention legislation. Where once we quietly took phone calls in our own homes on a telephone plugged into the wall, now we carry around a mobile phone that, as the Irish Council for Civil Liberties has noted, effectively places a personal tagging device on every citizen. Thanks to an incessant call and response occurring between our handsets and mobile phone masts, our phones record where we are all day long sometimes to within a few meters, and feed this information back to telecommunications companies, which then store this information for several years -- years! -- on the off chance that you might at some point, commit a crime.

Such an approach overturns the most basic legal and human rights tenets of democracies -- that an individual is considered innocent until proven guilty, that evidence is not gathered until a case is made to do so, and citizens should not be monitored and surveyed for one, two or three year tranches just in case he or she might one day be suspected of being guilty.

It also means that we no longer have the basic privacy of daily activity that we once had, to go about our daily business anonymously -- to metaphorically close the curtains to our homes without being suspected of cutting drug deals or laundering money in our sitting rooms. In Ireland, our personal digital information is now held for one of the longest retention periods amongst western democracies, even though in every serious court case

that has used such records as evidence, the details were retrieved from calls made within the 6 month retention period advocated by the Data Protection Commissioner.

Alongside the formal issue of data gathering and retention by commerce and by government and law enforcement, a complicating factor has emerged in recent years that some might argue is proof that Sun Microsystems co-founder and former CEO Scott McNealy was right when he famously quipped in 1999: 'You have zero privacy anyway. Get over it'.

That factor is the emergence of the online social networking universe, in which information is willingly divulged by users of an explosion of social media services (discussion forums, Twitter, blogs, Facebook, Bebo, MySpace, peer-to-peer file sharing networks, etc.) for a perceived benefit – networking, information exchange, casual socialising, setting up meetings, discussing projects, sharing pirated content (music, film, books). Such use has generated an altered view of privacy and, for many users, blurred (or critics might argue, eroded) the division between public and private aspects of one's life and work.

That shift is termed 'Privacy 2.0' by author Jonathan Zittrain, who argues that such use creates fresh challenges as people willingly, and perhaps unthinkingly, divulge information themselves and make it available to others. These others may then use the information in ways not intended by the provider of that information, including making deliberately malicious use of such data. Zittrain observes that:

> the Net enables individuals in many cases to compromise privacy more thoroughly than the government and commercial institutions traditionally targetted for scrutiny and regulation. The standard approaches that have been developed to analyze and limit institutional actors do not work well for this new breed of problem, which goes far beyond the compromise of sensitive information.

He goes on to argue that perhaps a casual attitude about disseminating information is not a recent development – he notes that the general public has always been willing to part with personal data for any range of reasons, and even though polls repeatedly have indicated a public concern about privacy, 'the public's actions frequently belie these claims', to the confusion of researchers and lawmakers.

Web users, with their voluntary proliferation and propagation of data, are perhaps only a logical extension of that ambiguity and, to some extent, steer a 'third way' through privacy issues, particularly in their use of social media. That third way is grounded to some degree in one's age:

> The values animating our concern for privacy are themselves in transition. Many have noted an age-driven gap in attitudes about privacy perhaps rivalled only by the 1960s generation gap on rock and roll...[and yet]...while young people appear eager to share information online, they are more worried than older people about government surveillance.

Younger people seem happy enough to put personal information online, tag it so that it can be easily found, and reveal detail that other generations would have kept within a small circle of friends and family. But Zittrain shrugs off the argument that images of drunken exploits posted to Facebook pages will lose students future jobs when viewed by prospective bosses, for 'soon those making hiring decisions will themselves have had Facebook pages'.

Such developments make for an emergent, highly complex privacy landscape, different to anything that has come before, in which various stakeholders – governments, businesses, individuals – simultaneously desire access to others' data, while wishing to control access to their own, fail to adequately protect stored data against malicious access or casual loss, or willingly share data without much thought about the potential for its long term endurance and availability as archived, easily mined, digital bytes. Society is definitely in transition towards some new way of viewing privacy and stored data. However, that does not remove what lawyer and academic Lawrence Lessig has called 'the burden of... monitored facts' , the pooled random detritus of our monitored digital footprints:

> The burden is on you, the monitored, first to establish your innocence, and second to assure all who might see these ambiguous facts that you are innocent. Both processes, however, are imperfect; say what you want, doubts will remain. There are always some who will not believe your plea of innocence.
>
> Modern monitoring only exacerbates the problem. Your life becomes an ever-increasing record; your actions are forever held in storage, open to being revealed at any time, and therefore at any time demanding a justification.

In the search for an acceptable balance between data generation, data protection and data retention, no easy answer presents itself for societies. Given the yearly proliferation of new technologies that generate an ever larger and longer digital data shadow, it seems highly unlikely that the challenge will become more containable or manageable. With technologies generally racing ahead of our ability to fully understand their implications, and with even their creators finding it difficult to know exactly how they will be used, often the horse has long bolted from the stable before anyone realises the door was open in the first place.

In addition, different societies take different views of where the line stands between a right to data protection and privacy and acceptable – even welcomed – use of personal data. The growing importance of global e-commerce, and the enthusiasm internationally for outsourcing many of the 'back office' tasks that involve personal data processing, means states can struggle to find an acceptable middle ground – witness the long negotiations between the EU and the United States to settle on the Safe Harbor agreement for exchanging the personal data of their citizens.

And one of the greatest obstacles to managing what security expert Bruce Schneier has called **'this tidal wave of data [that] is the pollution problem of the information age'** is that most people fail to realise a problem actually exists. Digital data is not concrete and

obvious, like files of paper or recorded tape. It is invisible to almost all, moves silently through the globe's fibre optic networks and copper cables, and sits quietly within massive servers and small desktop computers.

Bruce Schneier argues that, perhaps because of the internet's generally libertarian origins and operations, the law has shown little appetite to deal with the complexities of privacy and security, leaving the market and the state to decide how to manage personal data. In addition, he notes that individuals fail to perceive that companies like Google, Twitter and Facebook ultimately do not exist to provide them, the consumer, with a service, but to gather personal and collective data that can eventually be sold or monetised in some other way. The system is not set up to protect or benefit the individual or society, but to suck in as much data in ways that companies and governments hope will least be noticed.

Media coverage of hacked corporate computers, Internet fraudsters, missing laptops and stolen storage drives has at least helped more citizens and businesses to understand how worryingly easy it can be to lose digital data, or have it taken. But the broader issues of data retention and data protection get little public airing or engagement and individuals and organisations continue to remain largely ignorant of the ways in which their daily business practices inadvertently may be helping to construct a surveillance society.