1.1 Growing Interest

If privacy is a cornerstone of democracy,¹ then democracy is in trouble. Especially since the advent of the computer, the encroachments on privacy have proliferated. Terrorist attacks in the early 21st century have given governments all the justifications they need to bolster national security by forcing telecom companies to retain telephone records, to justify warrantless eavesdropping on our phone calls, to examine our bank records, to fuse personally identifiable information from multiple sources, to profile citizens to determine who presents a risk to the established order. Many companies have either aided and abetted governmental efforts or engaged in their own surreptitious amassing of the details of our lives. Personal data in real time has become the fuel of today’s economy. The development of new technologies, while indisputably offering many benefits, is the proverbial two-edged sword: it cuts both ways, and if the wielder is not careful, he may suffer more than superficial lacerations. Technologies can be and are employed to discover more about where we are, where we go, what we are doing, what are our interests and proclivities, to manipulate our behaviour and choices in ways of which most people are not aware and, if they are, are powerless against the inexorable lust for personal data. It comes as no surprise that many would-be jeremiahs have already pronounced privacy is dead. Indeed, many of those who would like to preside over the last rites are the very people who stand to profit most from the burial of this fundamental right.

¹ The Supreme Court of Canada has stated that “society has come to realize that privacy is at the heart of liberty in a modern state . . . Grounded in man’s physical and moral autonomy, privacy is essential for the well-being of the individual”. R. v. Dyment (188), 55 D.L.R. (4th) 503 at 513 (S.C.C.). Also: “Without privacy, it is much harder for dissent to flourish or for democracy to remain healthy and robust. Equally, without privacy the individual is always at the mercy of the state, forced to explain why the government should not know something rather than being in the position to demand why questions are being asked in the first place.” Goold, Benjamin J., “Surveillance and the Political Value of Privacy”, Amsterdam Law Forum, Vol. 1, No. 4, 2009.
But privacy is not dead. Opinion polls consistently show unease and distrust of our political leaders and the corporate warlords on matters of privacy. Citizens may choose to forego personal details, at the relentless urging of big business, but they still value what they have left.

One of the instruments for safeguarding privacy is privacy impact assessment (PIA). There is growing interest in PIA and, consequently, it seems timely to publish what we believe is the first book on the subject.

In Europe, the interest in PIA has been sparked by two main events. First was development and publication of a PIA handbook in the UK, the first in Europe, in December 2007. Second was the European Commission’s Recommendation on RFID in May 2009 in which the Commission called upon the Member States to provide inputs to the Article 29 Data Protection Working Party for development of a privacy impact assessment framework for the deployment of radio frequency identification (RFID) tags.

Article 4 of the European Commission’s Recommendation on RFID said, “Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments. This framework should be submitted for endorsement to the Article 29 Data Protection Working Party within 12 months from the publication of this Recommendation in the Official Journal of the European Union.” The RFID PIA Framework, developed by industry, was endorsed by the Art. 29 Working Party in February 2011.

Since these two milestones, there have been frequent calls for PIA in Europe. The European Parliament, in its 5 May 2010 resolution on passenger name records (PNR), said that “any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test”.

European Commission Vice-President Viviane Reding said in July 2010 that “Businesses and public authorities... will need to better assume their responsibilities by putting in place certain mechanisms such as the appointment of Data Protection Officers, the carrying out of Privacy Impact Assessments and applying a ‘Privacy by Design’ approach.”

---


