David Young Law
Compliance Bulletin
January 2016

Deconstructing Privacy – What it tells us about the future[1]

David Young

If we look back to the origin of our current privacy laws – the *1980 OECD Privacy Principles* – we may note a bit of irony, if not self-fulfilling prophecy. The OECD Principles were developed, in a forward looking perspective, to respond to the challenges to personal privacy envisaged by the oncoming digital era. Viewing the privacy world today, one is struck by the fact that that digital idiom, in its early 21st century form, is posing the very real question of whether privacy can or should continue to exist, or whether privacy laws need to be adjusted to reflect whatever this reality may be.

The most significant of the *OECD Principles* is the "collection limitation principle" – that collection of personal data should be made only by lawful and fair means and, with certain exceptions, and that the *knowledge and consent* of the data subject is required. However, we know that today this *knowledge and consent* requirement is under serious scrutiny.

More broadly, we may be asking: firstly, in the context of the digital idiom – and what may be called the *"Sharing Society*" – does privacy still exist, and secondly, if it does still exist, where do we end up when interfacing privacy with surveillance and security?

In trying to find answers, I propose to draw on an analysis by Frank Work, former Information and Privacy Commissioner of Alberta, delivered to the recent IAPP Canada Privacy Symposium, entitled "*Deconstructing Privacy*"[2]. What follows draws significantly on Frank's model, with some thoughts of mine – in which he sets forth what he sees as the social forces that are shaping our current view of privacy.

Security overtook privacy

I recall many discussions in the early days of the last decade highlighting the security rule as a significant aspect of the privacy law because, for the first time in a law of general application, a duty to protect and secure information was articulated. It is instructive to note that prior to the privacy laws, protection of

[1] Comments to the Privacy and Access Law Section of the Ontario Bar Association at the presentation of the 2015 Karen Spector Memorial Award for Excellence in Privacy, June 24, 2015.
[2] "Deconstructing Privacy", Frank Work, QC, Address to the IAPP 2015 Canada Privacy Symposium, Toronto, May 28, 2015.

information was almost exclusively addressed by way of private party legal relationships. No overarching obligation not to disclose information existed.

Frank points out that among the eight *OECD Privacy Principles* and the ten principles of the CSA's *Model Code for the Protection of Personal Information* (which are based on the *OECD Principles* and which form the substantive rules for PIPEDA, the federal privacy law) - security is only one. He notes how much the world has changed since 1980 and asks whether it is good that there's so much concern about security. He posits that it leads many people to believe that ***security IS privacy*** – that data collectors may collect whatever they want and do whatever they want with it as long as they don't lose it.

Governments found that privacy was inconvenient

Frank notes that governments found that keeping personal information within the silos of separate government agencies made it challenging to administer social programs, including finding fraudsters. Furthermore, they wanted their security agencies to have extensive powers of investigation and surveillance and be able to identify real "bad guys" – as they are from time to time defined.

The Web overtook us all and then social media overtook the Web

This is the "*sharing society*". Frank suggests that just because we all like to share and over-share does not mean that there should be a free-for-all with our personal information. However social media sites and search engines do lots with our personal information and most of us do not care enough to set the privacy settings that we're allowed.

Fear

Frank suggests that since 9/11, the prevailing attitude has been that sacrificing privacy for national security is a good trade-off. With every subsequent event which our political leaders or law enforcement tell us is an "act of terror" there must be new initiatives to enable more surveillance. Polls say most of us accept this. Bill C-51 is the latest iteration.

Employers

Frank highlights the ever-increasing demands by employers to have personal information about their employees. We know that, stretching back at least to the 1990s, employers sought new avenues to not only learn more about *whom* they are hiring but also about *what* their employees do at work. And as we now know from recent experience, what an employee does outside of their workplace may be cause for termination. It is clear that surveillance and even simple collection of publicly available information (such as on the web), which is not surveillance, may be acceptable.

Businesses

Frank mentions that "customer relationship management" has been a key priority for businesses for two decades. However, today, we don't hear as much about the term, "customer relationship management" as we do about "targeted advertising". In my view, this is because businesses, while they value information about existing customers and want to leverage that, are very focused on new customers, or customers with whom they have not yet had any close relationship, but about whom they can learn a lot - through online tracking, geo-location marketing and "Big Data" databases.

Another facet of industry desires for information can be found in the context of "The Internet of Things" – companies interested in knowing their customers' lifestyles – including their bad habits and risky behaviours – generated by data sent from wirelessly connected devices.

Schools

Frank mentions other more innocuous yet still potentially invasive forms of information collection – including schools interested in the lives of their students (identifying students facing personal challenges or to prevent bullying) and parents who not only seek this information but demand it.

The surveillance society

I suggest that all of this increasingly pervasive collection of intimate personal information could be characterized as part of a broader societal shift toward embracing surveillance.

New notions of social relations and human nature: accountability and inquisitiveness

Frank suggests that there is a new notion of social relations that impacts privacy - *accountability*. He refers to an article by Anita Allen[3] in which the author suggests that that privacy and accountability in their own way render us more fit for valued forms of social participation – that we all have "accountability mandates". He cites examples of public figures who had extra-marital affairs and for whom the public not only demanded a confession but also an explanation of the facts and circumstances.

Perhaps the most broadly philosophical theme that Frank identifies is that of our human nature - *to be inquisitive*. It is a variation of the "sharing society" idiom. We are an inquisitive species, especially where fellow human beings are concerned. We are good at collaboration and cooperation; we love to share information. We care what others think even if we say we don't. Our brains try to make sense of things: to rationalize discrepancies and to seek explanations. But, Frank suggests, massively shared

[3] Anita Allen, "Privacy Isn't Everything: Accountability as a Personal and Social Good", from Information Ethics: Privacy, Property and Power, ed Adam. D. Moore, Seattle: University of Washington Press, 2005.

social media does not foster these things. Understanding an issue, analyzing it and forming an opinion on it which is consistent with our subjective self is reduced to "*like*"-ing a posting.

Frank posits that in this sense, the threat to privacy is not that everyone gets to see what you think; the threat is that, living in the glass house, we lose our subjectivity and our individuality. There is no worry about people seeing inside our brains if all our brains are thinking pretty much the same things. When that happens, there is no innovation, no criticism and no dissent. We need privacy to become individuals. We need privacy to firm out our ideas and values so that we can innovate and criticize.

Where do we end up on the philosophical issues?

The interface of security and privacy has benefited from a healthy and vigorous debate, resulting in, for the most part a constructive dialogue, including that relating to Bill C-51. I believe that this dichotomy must continue to be debated vigorously and constructively in the public forum with the goal of achieving a consensus that reflects social values.

However, in Frank Work's view, the real enemy of privacy may NOT be surveillance, but the dumbing down and flattening out of our individual *intellects, individualities and creativities* by moving our self-development increasingly and exclusively into the public arena of electronic media.

I would argue that privacy does still exist and should exist – the self versus public idioms mentioned by Frank are testament to this. However the bounds of what is private versus public will continue to be explored and defined. We are in an evolving, rapidly changing privacy world and, of course, that presents on-going new challenges for those of us involved in how the law responds to the changes.

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.