Has the Era of Privacy Come to an End?

Avner Levin*

Abstract

This keynote address to the 2016 McGill Law Graduate Conference provides a brief history of privacy before discussing contemporary challenges in the form of increasing technological ability to create, store and process personal information, and powerful advocacy against privacy from both government and the private sector. In order for privacy to survive, a new set of personal information protection principles is required and new ways of enforcing these principles must be developed, which will leverage the power of technology to develop hybrid regulatory/technological solutions, such as Google's content removal tool.

INTRODUCTION

A talk such as this is always an opportunity to stand back and reflect on the state of the field, so to speak. As I set about doing that, I was struck by how pessimistic I was about the future of privacy. In fact, and that is the reason for the title of this essay, I believe that unless we take collectively, as a society, and not only in Canada but internationally, urgent steps to protect, or salvage, our privacy, the era of privacy and personal information protection will soon come to an end.

What I hope to take you through in this essay is a (brief) history of privacy, focusing more on the modern era and then a look at the technological and political developments that have been plaguing privacy for a few years now. I will end with a few hopeful suggestions as to how we could counterbalance these developments with a mix of legal, regulatory and technological responses.

I. A (BRIEF) HISTORY OF PRIVACY

We do not often think about it, but privacy is, of course, a very culturally dependent idea. For example, privacy in Japan is based on a societal-normative foundation of customs and traditions[1] (and then of course they have legislative data protection layers as well[2]). So, I apologize, but my "history" of privacy is really a history of a common-law, and to some extent, a civil-law idea of privacy. It certainly is not a comprehensive or comparative review.

---

* Professor, Law & Business Department, Ryerson University. This short essay is based on a keynote address delivered at the 2016 McGill Law Graduate Conference, "Legal Challenges in Cyberspace," 14-15 May 2016.

1 Makoto Nakada & Takanori Tamura, "Japanese Conceptions of Privacy: An Intercultural Perspective" (2005) 7:1 Ethics & Information Technology 27.

2 Hiroshi Miyashita, "The Evolving Concept of Data Privacy in Japanese Law" (2011) 1:4 Intl Data Privacy L 229.

Most legal scholars begin their discussion of privacy with the American paper by Samuel Warren and Louis Brandeis about the right to be "let alone."[3] The paper, written in the late 19th century, was the first attempt by celebrities of that era (the upper class) to limit access to information about them, and to retain for themselves the ability to manage and control their reputation, their image in the eyes of others, their dignity, and their brand. Of course, the paper was not written *exactly* like that, but as a general right to be let alone, and it has been adopted and cited endlessly by privacy scholars in the field.

Interestingly, and we will return to this point later, the Warren and Brandeis article was not concerned about the contemporary American preoccupation with government surveillance. It was about (anti)social interactions. The more significant immediate point I would like to make about the Warren and Brandeis article, vis-à-vis a history of privacy, was that it established a private legal action framework for privacy in the United States (U.S.), or in other words, a tort. That was a very typical "common-law" solution to the issue of privacy as the authors understood it, but the rapid adoption of their article meant that Americans did not really pause to consider other legal solutions, such as legislation and government regulation.

Indeed, the next big development in the U.S. was the paper by Dean William Prosser in 1960 at the University of California, Berkeley School of Law. Prosser, a tort expert, established four privacy torts in his paper "Privacy".[4] That second influential paper cemented the perception in America that private legal action is the preferred mechanism to deal with private sector disputes. Since then, legislation in the U.S. has been a patchwork quilt of special interest accommodations,[5] such as video store records.[6]

But let us leave the private sector for a moment and go back to those concerns about governments. In Europe, post-World War II, and generally in the West throughout and after the Cold War, recognition grew that government surveillance was just as big of a concern, if not more so, because of the state's coercive powers, than any form of private sector invasion of privacy.

In both Europe and in the U.S. we therefore see legislation that aims to curb government power to collect sensitive information about individuals, and to subject it to well-defined protective principles. These are known in the U.S. as Fair Information Practice Principles (FIPPs). The Americans identified five original principles in 1973, which were: notice, choice, access, security, and enforcement.[7] The Europeans and the Organisation for Economic Co-operation

---

3 Samuel D Warren & Louis D Brandeis, "Right to Privacy" (1890) 4:5 Harv L Rev 193.

4 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383.

5 Avner Levin & Mary Jo Nicholson, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground" (2005) 2 University Ottawa L & Technology J 357, s. 2.1.1.

6 *Ibid* at 366.

7 Robert Gellman, *Fair Information Practices: A Basic History*, SSRN Scholarly Paper ID 2415020 (Rochester, NY: Social Science Research Network, 2016).

and Development (OECD) then added more principles in the 1980s and expanded these five principles into eight.[8] Since 2001, in Canada there are now ten principles enshrined in Canada's private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*.[9]

These principles, and equally important, the regulatory framework that developed around their enforcement in the form of independent information and privacy commissions, data protection authorities, or privacy enforcement authorities that now make government departments, agencies and ministries as well as the private sector in Europe and Canada accountable, ushered in the "Golden Age" of privacy. This Golden Age started in the mid-1970s and, I fear, it has just about ended or is in the process of ending. So, let us now talk about this Golden Age, how it came to be, and why it is coming to an end.

II. THE MODERN ERA GOLDEN AGE OF PRIVACY

The Golden Age of privacy came about because these privacy principles (I will refer to them collectively as such for the sake of consistency) had real meaning at the time — following them literally changed information management and provided individuals with real control over their information and who else had it. Control became the essence of personal information protection, and the language of these privacy principles also captured principles of choice, consent and, to a lesser degree, notice. The Germans developed the idea of "informational self-determination" — the ideology that control over your information allowed you to determine and shape your identity, your sense of self, and that this should be an individual right, rather than a government dictate.[10] It is sadly obvious to see how the Germans, learning the lessons from the Second World War, would want to wrest control over the identification of individuals out of the hands of government for good.

Technologically, what allowed members of society to exercise control over their personal information, was the feeble (in modern terms) processing and storage powers of computers at that time. For example, the hard drives sold in the 1970s and 1980s only had between 500MB to 1GB of storage. Manufactured by International Business Machines (IBM), they were the size of a washing machine and weighed over 500lbs. And they cost $35,000.[11]

---

8 OECD ,"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", online: <www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

9 SC 2000, c 5, Schedule 1.

10 Paul Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination" (1989) 37:4 Am J Comp Law 675, s. II.

11 IBM, "IBM Archives: IBM 3370 direct access storage device", online: <www-03.ibm.com/ibm/history/exhibits/storage/storage_3370.html>.

Furthermore, personal information was not collected continuously by governments or by the private sector. Instead, it was collected in a series of discrete interactions. We were able to make separate decisions about whether we wanted to provide information and what information we would provide on a variety of issues, such as when we filled out our income tax returns, or our government census, or applied for a passport or a driver's licence, or, when we shopped, whether we would provide the store with our postal code or telephone number. All of these interactions largely depended exclusively on us to be the source of information about us, and so, we were able to decide whether we wanted to interact, what information we would share in the interaction, and under what conditions. We had, in the language of modern-day principles, a meaningful opportunity both to consent to the collection of our information and to understand the purposes (as in the examples I just mentioned) for which this information would be put to use. Finally, the information collected about us and processed about us was stored in discrete stand-alone proprietary databases both in the private sector as well as in governments. Special effort was required in order to share and transfer (i.e., disclose) information about us between government departments.

The combination of all of these created the Golden Age of privacy. We felt, largely correctly, that we were in control. We felt that if we decided not to provide information to the government or to a business about us then the government or that business would not know or have access to that personal information. We felt that the purposes for which our information was used were well-defined and limited; we felt that we knew, or could know if we wanted to, what information was stored about us. In other words, we felt that the privacy principles were meaningful and real. Then slowly, gradually, incrementally, everything changed. And today, we may well be witnessing the end of the privacy era.

III. THE END OF PRIVACY

There are various estimates on the internet as to how much data is processed in this day and age in order to enable our data-rich lifestyle. Let us pick one estimate, by a company called Domo, which is a snapshot as of 2016.[12] The statistics boggle the mind, demonstrating how far we have come in 35 years in terms of storage and processing power. Almost a million Tinder swipes. *Every minute*. That is pretty personal. Close to two-and-a-half million posts liked on Instagram. *Every minute*. This is a tremendous amount of personal information. And just about seven million Snapchats, again, every minute. All of this personal information created, stored and processed *every minute of every day* in 2016.

You can see, therefore, why privacy protection is collapsing. The principles are no longer up to the task. Let us not forget, as well, that these statistics are

---

[12] Josh James, "Data Never Sleeps 4.0", (28 June 2016) *Domosphere* (blog), online: < www.domo.com/blog/data-never-sleeps-4-0/ > [Domo].

about private sector information processing. Governments around the world have seen a similar rise in their capacity. Most recently, and infamously, that was demonstrated by Edward Snowden through his revelations about the capacity of the National Security Agency (NSA) in the U.S. The NSA's Utah Data Center holds by some estimates 12EB of information.[13] That is *twelve billion* times more information than the IBM 1980 hard drive capacity referenced above. In Canada, we are slowly learning about the capacity of our own Communications Security Establishment, a governmental cryptologic agency, and about the cooperation between like-minded nations such as the Anglo Five Eyes (United States, United Kingdom, Canada, Australia and New Zealand). This form of information sharing is a far distance from those old IBM mainframe databases, those good old-fashioned silos of information.

Our control over information has loosened not only because of the increase in our technological capabilities, but just as much because of the change we have undergone in the way we socialize. Social media is (unfortunately) here to stay which proves that we may be increasingly interested in controlling our information, but also, that we are just as interested in other people's business and lives, in gossip and in information sharing. We are human beings and we do as humans would, whether offline or online. Among the many implications for privacy is this — personal information about us no longer originates exclusively with us. Others can be a rich source of information about us through their activities, and both governments and the private sector can deduce, generate if you will, personal information about us through analysis of so-called meta-data, and by other means.

So, we are now in an era where there is increasing technological ability to process information, and more personal information that is created and available for processing by individuals. This information is proliferated by sensors and devices known as the "internet of things," by other individuals "socializing" online, and by the analyses of this information. Now, to add to this privacy horror story, we must not forget about the advocacy from both governments and the private sector to bring about normative change to diminish the value of privacy, whether in the name of national security or in the name of profit (as Zuckerberg and many others did and will do).[14] All of these erode privacy and erode our control over our personal information and our ability to decide what happens with it. All of this offers clear evidence that the privacy principles of yesteryear are no longer powerful, meaningful or relevant. As a result, I argue

---

[13] Kashmir Hill, "Blueprints of NSA's Ridiculously Expensive Data Center In Utah Suggest It Holds Less Info Than Thought", *Forbes* (24 July 2013), online: < www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/ > .

[14] Bobbie Johnson, "Privacy no longer a social norm, says Facebook founder", *The Guardian* (11 January 2010), online: < www.theguardian.com/technology/2010/jan/11/facebook-privacy > .

that in the absence of corrective action our privacy will soon come, if it has not already, to an end.

IV. A NEW HOPE

So, what if at all can be done? The legal and regulatory answer is clear — we need a new set of personal information protection principles and we can discuss some proposals in this regard. What is perhaps not as clear is that we need new ways of enforcing our privacy principles. The regulatory frameworks within agencies and commissions that once worked for us may perhaps need to evolve and take on new roles.

First, let me talk a bit about the shape that such new principles could take. There have been many initiatives in recent years that could be characterized as either conservative or radical, from the revised OECD principles,[15] to the new European Union's *General Data Protection Regulation* with its intriguing inclusion of new principles such as article 25, "data protection by design and by default" and article 17, the "right to be forgotten."[16] All of these are worthy of their own devoted talks, but I want to focus today on a rogue group of academic and industry leaders that came together a few years ago through collaboration mainly between Microsoft and the University of Oxford's "Oxford's Internet Institute".[17] Their radical proposal was to suggest that it is perhaps time to abandon the principles of notice and consent and to move towards principles that restrict and limit the use and processing of information.[18]

If you go back to the information presented by Domo[19] you will perhaps understand why the Oxford-Microsoft group believes that notifying and asking people to consent to the processing of their data — in the manner it is currently done — does not offer individuals meaningful protection and control over their information. Instead, it offers corporations a fig leaf of legality (also known as a privacy policy, or "terms of use") to cover their continuous data processing activities. Put differently, the act of consent is a discrete, singular act, whereas the processing of data is continuous. What the Oxford-Microsoft group suggests is that meaningful protection in the era of our privacy and personal information will only be found by tightening the constraints over the uses and purposes for

---

[15] OECD, "2013 OECD Privacy Guidelines", online: < www.oecd.org/internet/ieconomy/privacy-guidelines.htm > .

[16] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] O.J., L. 119 [*General Data Protection Regulation*].

[17] Fred H Cate, Peter Cullen & Viktor Mayer-Schonberger, *Data Protection Principles for the 21st Century,* (Redmond, WA, Microsoft Publisher, 2013), online: < www.repository.law.indiana.edu/cgi/viewcontent.cgi?article = 1022&context = facbooks > [Cate, Cullen & Mayer-Schonberger].

[18] *Ibid* at 6–7.

[19] *Supra*, note 12.

which information can be processed, and by focusing on processing that has significant implications for individuals. These include admission decisions to a university, insurance coverage, employment, hiring and disciplinary decisions and healthcare provisions.[20] Many, many other commercial purposes and processing — for example, for advertising and marketing — would be subject to a risk/benefit analysis,[21] which critics have understood to mean that such uses would not be restricted at all.[22]

It is easy to see why the Oxford-Microsoft proposal is both attractive and horrifying at the same time. Does it offer us a brave new hope? Or does it simply surrender the battle over privacy? I think it offers us some hope, but only if we change the way that we currently enforce our principles of privacy protection, which brings me to my second point.

So, second — how do we provide meaningful privacy protection in this day and age, and perhaps, even for tomorrow? We need to find a way to *continuously* offer individuals control, choice and all those other Golden Era privacy principles. And it is no surprise that we will need technology to do that. In fact, we will need to combine regulatory and technological responses and we will need regulatory and legal decisions to directly determine and dictate technological privacy protective measures. In other words, we will need more *Google Spain* decisions,[23] or perhaps, if we cast our net a bit more broadly and earlier in time, we need more *DMCA*s (which is, if you forget, the U.S. *Digital Millennium Copyright Act*).[24]

What the *DMCA* did legally was to establish legal liability for corporations that could be seen to facilitate intellectual property (IP) infringements, unless they could demonstrate their IP protective actions.[25] What the *DMCA* achieved technologically was the creation of an interface, largely automated, through which IP rights could be pursued and protected.[26] As a result, when I look for the latest episode of a popular television show, such as Mr. Robot on YouTube or Google, I cannot easily find it. Note that I did not say I cannot find it at all — but I think it is a fair assumption that most non-tech-savvy folks would conclude that if they cannot find it easily on YouTube or Google then it is nowhere to be found on the internet. And that of course is of vital importance to privacy and is

---

[20] Cate, Cullen & Mayer-Schonberger, *supra* note 17 at 18–19.

[21] *Ibid* at 17—18.

[22] Ann Cavoukian, "So Glad You Didn't Say That! A Response to Viktor Mayer-Sch—nberger" (16 January 2014) *Privacy Perspectives* (blog), online: <iapp.org/news/a/so-glad-you-didnt-say-that-a-response-to-viktor-mayer-schoenberger/>.

[23] *Google Spain v AEPD*, 2014, ECLI:EU:C:2014:317, Case C-131/12 (C.J.E.U.) [*Google Spain*].

[24] *Digital Millennium Copyright Act*, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[25] *Ibid*, Title II.

[26] See e.g., Google, "Legal Removal Requests", Legal Help, online: <www.support.google.com/legal/answer/3110420?visit_id=1-636191549595465825-3132166967&rd=1>.

the beauty of the *Google Spain* decision as well. For the significance of that decision is not only in its confirmation of a right to be forgotten, but also in Google's decision in its aftermath to create a technological interface, similar to the IP interface, that would allow individuals to submit privacy requests easily and efficiently. It is not a perfect process, and there is much to improve, but it is a start.[27]

I can think of a couple other examples, very quickly, in which a regulatory decision could leverage technology, and which could push back against the collection of personal information through the proliferation of sensors and the Internet of Things. Police body-camera video feeds, for example, could be encrypted by default with judicial approval required in order to decrypt the images. Drone manufacturers could be legally required to geo-fence[28] their devices so they could only be flown in open spaces. Manufacturers that do not comply will face legal liability for the resulting illegal processing of personal information. No doubt many more similar examples can come to mind.

We need many more such legal and regulatory decisions, and we need to provide private and public sectors with the right incentives, both positive and punitive that would encourage them, nudge them, and, if necessary, force them to come up with more such solutions. Inescapably, in the Canadian context, this leads to the continued call for greater enforcement and order-making powers for the Privacy Commissioner of Canada that would place the Office of the Privacy Commissioner of Canada (OPCC) on a level plain with other data protection and privacy enforcement authorities worldwide. Such mechanisms should ensure that the private sector views the OPCC as a significant regulator.

V. CONCLUSION

We may be witnessing the end of an era, the era of privacy and personal information protection. Hastened along toward its demise by rapid technological development and new social and political paradigms of information sharing, personal information protection can still be salvaged through a new regulatory approach. This approach should focus on the retention of consent in meaningful instances which have significant implications for individuals — such as in healthcare, employment, and education contexts. In Canada, the Privacy Commissioner of Canada must be equipped with enforcement and order-making powers comparable to other jurisdictions. Globally and locally, further legislation and regulation must protect privacy by leveraging the power of technology to develop hybrid regulatory/technological solutions along the lines of the *Google Spain* decision and the *DMCA*. If we could find a way to protect IP

---

[27] Google, "Search removal request under data protection law in Europe" Legal Help, online: < https://support.google.com/legal/contact/lr_eudpa?product = websearch&-vid = 0-674717288659-1483559549447 > .

[28] Create a virtual "fence" through software around a real-world restricted area.

for strong commercial interests despite technological developments surely we can find a way to do the same for privacy.