Open Data: Managing the Privacy Challenges


Professor Emeritus, University of Western Ontario; privacy and information policy consultant, Victoria, Canada; David@Flaherty.com

My Background on Privacy and Access to Data

I have been fortunate to have a chequered career. As a Canadian graduate student studying American history at Columbia in 1964, Alan Westin introduced me to the history of privacy, which led to my first book. Using early New England court records for that purpose, turned me into an historian of U.S. law. Ford Foundation money in the 1970s and 1980s turned me into a comparative analyst of the development of data protection laws in North America and Western Europe. In 1993 I became the first Information and Privacy Commissioner for British Columbia. In 1999 I became a full-time privacy consultant, which I still do.

When Emmie Tran, Virginia Scholtes, and Chris Hoofnagel kindly invited me to give this keynote address, they flattered me by referring to my 1979 book, Privacy and Government Data Banks: An International Perspective. It is primarily a study of the collection, use, and disclosure of personal information for research and statistical purposes by national statistical agencies in the United Kingdom, Sweden, the Federal Republic of Germany, the USA, and Canada. I looked closely at the legislative frameworks in place in each country, including the emergence of national and state privacy (data protection) legislation. A central argument of my book was the need to enhance access to personal data for legitimate research purposes under controlled conditions. A favourite example in my memory is interviews with Sir Richard Doll at Oxford about how he used mortality and National Health
Service data for record linkages to definitively study all kinds of health risks, including the famous association between smoking and lung cancer among British doctors.① Professor Richard Peto, and others, continue this linkage work today.

From the perspective of my more than fifty years of experience with issues of privacy and data protection in contemporary societies, and also having been a long-time privacy advocate, I am proud of the fact that I have remained a strong advocate of controlled access to data for legitimate research purposes.② My clients over time have also involved a number of leading Canadian agencies involved in managing health information for research purposes.③

Open Data and Freedom of Information in British Columbia

Thus I strongly favour the Open Data movement because of its potential to increase knowledge, accountability, and transparency. This potential extends beyond health research. As Freedom of Information Commissioner for my province, I was very sympathetic to requesters who wanted access to data in the broader public interest (not just health research), where the privacy risks were de minimis. In 1998 the Vancouver Province newspaper wanted schools to disclose the number of elementary school students taking Ritalin from School District staff.④ The media wanted numbers, grade, and sex of children treated at each school. Vancouver school districts refused to do so. After mediation failed, I held a written hearing and required the Districts to sever the records and disclose them in anonymized form to the

③ www.cihi.ca; www.ices.on.ca; and www.popdata.bc.ca
applicant. I was sensitive to the risks of re-identification and residual disclosure.

Analyzing these data, the journalist published a series of news articles that exposed widespread, high-dose prescription of Ritalin to very young students, and changes were made as a result. This example illustrates the power of open data through access to information, as well as the importance of independent oversight.

In terms of further illustrating the utility of having independent oversight of statutory freedom of information and protection of privacy regimes, I want to draw your attention to an Investigation Report, dated July 25, 2013, from the BC Information and Privacy Commissioner, Elizabeth Denham, Evaluating the Government of British Columbia’s Open Government Initiative. In July 2011, Premier Christy Clark announced an open government initiative for the Province of British Columbia that includes an open information policy, a disclosure log of government’s responses to access requests, and an open data policy. This was reinforced by legislative changes to BC’s Freedom of Information and Protection of Privacy Act (FIPPA) in November 2011 that require public bodies to establish categories of records for proactive disclosure without an FOI request.

This 2013 report evaluates the Open Government initiative and whether it promotes transparency and accountability in practice. On the open government—or open information—side, Commissioner Denham noted that the only information government was disclosing was travel expenses of ministers and deputy ministers. She therefore recommended that the government proactively disclose hospitality expenses, senior public servants’

---

5 Investigation Report F13-03 (50 pp.), at https://www.oipc.bc.ca/investigation-reports/1553
6 See http://www.openinfo.gov.bc.ca/
calendars, government contracts, and audit reports to the Open Information website. Some of that is now happening.

On the open data side, Denham concluded the BC government is on the leading edge of this movement, and that its policy aligns well with the principles of the G8 Open Data Charter issued in June 2013. The DataBC website, BC’s provincial-level open data resource, includes over 3,000 machine-readable datasets on a very wide range of topics, including information on public sector compensation, land use and resource information, statistics from a range of sectors, and the government’s budget. 7 (p. 8) In her report, Denham recommended a series of other records that should be routinely disclosed in the absence of an FOI request, e.g. audit reports.

It is also relevant to the concerns of my presentation, that Commissioner Denham’s open government report addressed protecting privacy in open data that contains personal information without de-identification/anonymization. She called on the BC government to develop “standardized guidance for all ministries to use to de-identify datasets identified for the open data program.” (p. 34) In this regard, the UK’s Information Commissioner’s office has issued detailed code of practice on this problematic issue.8 Other current guidance can be found in the 2015 reports of the Nuffield Council on Bioethics and the Council of Canadian Academies.9 Denham called on the BC government to develop “standardized guidance for all ministries to use to de-identify datasets identified for the open data program.” (p. 34)

7 See http://www.data.gov.bc.ca/
Commissioner Denham has also persuaded the BC government to introduce a new archives and records management law to replace a 1936 law. (pp. 39-41). Those activities are also part of managing the challenges of Open Data.

Troublesome Examples of Open Data

In reviewing the various assigned readings for this symposium, I was very troubled by the findings of the 2014 Federal Trade Commission (FTC) study of the nefarious activities of U.S. data brokers. (I will leave it to you to ferret out the gory details for yourselves.) I was struck, by way of contrast, with the very recent results of an independent investigation by the Privacy Commissioner of Canada into the Relevant Advertising program of Bell Canada, one of Canada’s largest phone companies (April 7, 2015).10

Bell’s 2013 announcement that it would use customers' network usage and account information to enable the serving of targeted ads, on behalf of advertisers, to almost 8 million customers led to an unusual number of privacy complaints (170), because it was using an opt-out model rather than an express, opt-in consent model. After initially disagreeing with the Privacy Commissioner’s finding and being threatened with an enforcement action in the Federal Court of Canada, Bell announced, on the day the decision was announced, that it would indeed comply with the recommendation, including destruction of all of the profiles created to date.11 Bell also kindly suggested that other Canadian

---

phone companies - and Google and Facebook - should also have to follow the same rules!¹²

The Federal Privacy Commissioner’s guidelines issued in 2011 require advertisers to ensure people know they are being tracked, notify them before collecting personal information, and allow them to opt out of being tracked.¹³ In his latest report, the Commissioner noted that “Bell is able to track every website its customers visit, every app they use, every TV show they watch and every call they make using Bell’s network…. When that information is combined with account and demographic information – such as age range, gender, average revenue per user, preferred language and postal code – which the company has long collected, the end result is a rich multidimensional profile that most people are likely to consider highly sensitive.” (para. 73) As it expands its targeted advertising program, Bell intends to use an even greater breadth of personal information to which it has access, including not only websites visited, but also app usage, TV viewing habits, and calling patterns.

Bell also agreed that upon receipt of an opt-out request, it will immediately delete all information from the customer's profile and cease tracking the customer. It also agreed to only use only the first 3 digits of the 6 digit Canadian postal code.¹⁴ Bell further agreed to “exercise greater due diligence, in the form of contractual and other measures, to protect against the possibility that advertisers might, using other available information, link customer profile information to an identifiable individual.”

¹² The actual federal report stated that “If other organizations are engaged in a targeted advertising program which is materially similar to Bell's, then equally, our expectation would be that such a program would be based on express opt-in consent model.” (para. 99)
¹³ Guidelines: Privacy and Online Behavioural Advertising
¹⁴ “According to Statistics Canada, the average number of households served by a postal code is approximately nineteen, but could include as little as one household.” (para. 118)
The Privacy Commissioner reported that in Bell’s compiling of its interest categories for customer profiles, “[a]ny categories that correspond to a list of categories that Bell has predetermined to be sensitive (e.g., "Adult Content", "Special Education", "Diabetes", "Catholicism" or "Gay Life") or likely to be of interest to minors (e.g., "Family Internet", "Society - Teens" or "Animation") are discarded and not added to the Customer Profile.” The Commissioner also determined that Bell could not use credit score information to focus its behavioral advertising.

I present this telephone company story as an example of what a progressive data protection regime, including independent oversight, can accomplish, despite major corporate resistance. As law professor Michael Geist observed earlier this week, “Bell argued that the information it collects is non-sensitive and that opt-out was therefore good enough. If the consumer data is taken piece by piece, Bell might have been right. Yet in an era of ‘big data’, the Privacy Commissioner effectively concluded that the sum of personal information is more than the parts.”

A Brief Diversion: Managing the Privacy Challenges of Big Data
I take considerable satisfaction in the fact that privacy advocates like myself, for the past fifty years in my direct experience, have raised early warnings about the privacy implications of national censuses of population stored in IBM mainframe computers, of the infamous idea of a national data bank in the U.S., of electronic bank transfers and bank machine cards, and now on to drones, national surveillance, and Big Data. These advocates are now substantially reinforced in most advanced industrial countries by official privacy regulators, who are charged with independent oversight of both the public and private sectors. The European Union leads in this regard. The US, of course, is a

notorious exception to this systematic approach to data protection at the national and state levels.

Thus the most problematic aspect of Big Data is its domination by US multi-nationals that are inadequately regulated in the United States and in the developing world.

The Need for a U.S. Federal Data Protection Agency

There was a time, ending in the early 1990s, when almost every presentation I made in the United States argued for the need of the Privacy Protection Commission that was tragically left out of the push for the Privacy Act of 1974.16 That was also the theme of my U.S. case study in Protecting Privacy in Surveillance Societies (1989). So if today’s organizers could persuade me to look again at one of my old books, let me take another look at another one and rehash an old argument that I think still has legs, especially from an international perspective of what other advanced industrial societies expect in terms of national and state data protection regimes. The US is sadly out of step with the rest of the world, despite continued efforts to advance some supposed component of the American way of life, i.e. self-regulation, and/or a hodge podge of specialized regulators and laws that are relatively impenetrable to non-Americans.

I am also motivated in what I am about to argue by the fact that there is so much privacy talent in the United States among public servants, civil society, academics, and privacy advocates. Perusing the assigned readings for this symposium and attending periodic Privacy Law Scholars conferences have further convinced me of that. The amount of analytical writing produced on such matters as Big Data and Open Data is quite staggering. But it lacks

---

an audience that can really make this work effective in a general way, beyond enacting another highly-specialized federal or state law.

I am in a bit of an odd position to try to make the argument for the virtues of a US Privacy Protection Commission, since, at least until I became a privacy regulator in 1993, I was well known as a diligent critic of these national watchdog organizations. I actually expected them to do something! I almost caused a riot at the opening of the International Data Protection Commissioners’ meeting in Quebec City in 1987 when I emphasized the need for privacy watchdogs to do some barking and biting. I take great pleasure in retrospect at having so irritated the French (from France, not Quebec!).

While I admire the recent work of the Federal Trade Commission on consumer privacy, and the skilled presentations by several of its Commissioners at the International Privacy meeting in Mauritius last October, the FTC by itself cannot fill the big boots of an omnibus privacy regulator, enforcing the Privacy Act in particular.

I have already mentioned the important work of some Canadian privacy regulators. I also admire the multiple national and state regulators among the members of the European Union who have made masterful efforts to implement, and then try to update, the European Directive on Data Protection. Thus it is quite encouraging to learn about the administrative order issued on April 8, 2015 by the Hamburg Commissioner for Data Protection and Freedom of Information, Johannes Caspar, to seek to force Google to comply with German data protection law and give users more

---

17 David H. Flaherty, "Towards the year 2000: The Emergence of Surveillance Societies in the Western World," the keynote address to the opening session of the International Data Protections Commissioners' Annual Meeting, Quebec, Quebec, September 22, 1987.
control over their data.\(^{18}\) The French, Dutch, British, and Spanish privacy regulators are also hot on the trail of Google and Facebook in particular. Forgive me for thinking that that is a good thing for global privacy protection.

Although I am not in the habit of re-reading what I have written about anything, I was encouraged by my summary review in my 1989 book about the need for a US Privacy Protection Commission to respond to “privacy and surveillance problems.”\(^{19}\) I was echoing, of course, the findings of the US Privacy Protection Study Commission in 1977 and the Office of Technology Assessment’s 1986 study, *Electronic Records Systems and Individual Privacy*. My own list of eight responsibilities and functions for a Privacy Protection Commission remains credible, even though, in those more innocent days before the Internet, I was primarily worried about the public sector.\(^{20}\)

1. Articulating privacy concerns in every relevant situation, functioning essentially as an alarm system for the protection of personal privacy.
2. Carrying out oversight to protect the privacy interests of individuals in all federal information-handling activities.
3. Implementing statutory duties under a revised *Privacy Act*.
4. Conducting investigations and audits of information systems to monitor compliance with the provisions of a revised *Privacy Act*.
5. Developing and monitoring the implementation of appropriate security guidelines and practices for the protection of personal information in federal hands.
6. Advising and developing regulations appropriate for specific types of personal information systems….


7. Monitoring and evaluating developments in information technology with respect to their implications for personal privacy.

8. Conducting research and reporting on all types of privacy issues in the United States.

I rest my case for a US Privacy Protection Commission in the hands of a very talented younger generation, since my worries about privacy protection will come to an end long before your own.