The Blurring of Sectors
From Public Versus Private
to Public with Private

Throughout our lifetimes, we provide information about ourselves to both the public and private sectors in a variety of different contexts. When we file a tax return or get a driver’s licence, we know that the information we provide will be retained by the government in some file or another. Similarly, when we use a credit card, sign a phone contract, or join a customer loyalty program, we know that the corporation we are doing business with is probably keeping a record of our encounters and what we tell them. If we have concerns about the collection and use of this information, those concerns tend to differ depending on whether we are dealing with the government or a corporation. And, in Canada, different privacy laws apply to personal information depending on whether it is held by a public agency or a private business.

For example, public sector privacy laws are intended to keep Big Brother at bay. Government surveillance can make it difficult for citizens to enjoy democratic freedoms, so we typically expect the state to get a warrant before entering our homes and invading our privacy. And we expect government agencies to collect only the personal data that are necessary to fulfill a statutory purpose and to use and disclose those data only in ways that are consistent with that purpose. Laws restricting the private sector’s collection of information, however, address consumer issues like correcting mistakes in our credit-rating scores or stopping marketers from collecting information about us without our consent. For most of the twentieth century, we safely
assumed that—short of a warrant—the information we gave to the government and the information we gave to corporations would be kept separate.

No more. Although there are technical, organizational, and legal limits on what may travel where, it is clear that data are now flowing freely between public and private agencies. Indeed, data from one sector so often pop up in the other sector, it can be difficult to differentiate between government and corporate surveillance. Since governments and corporations have different rationales and mandates, the implications for accountability are huge.

Let us look at an example. The Canadian Security and Intelligence Service (CSIS), the agency responsible for keeping us safe from international threats, is actively exploring partnerships with private sector owners and operators that would allow CSIS to ask companies to hand over personal information about their customers without customers’ consent. The objective is to develop extensive networks of regional contacts (a surveillance net, in effect) with those who own and run institutions classified as critical infrastructure—everything from pipelines and oil sands to public transit.1

Once those private sector data are turned over to the government, it becomes more difficult for people to track, let alone control, their personal information. How would you know, for instance, whether CSIS had a file on you based on information gleaned from the transit company or electricity business where you work? More importantly, as technologies and security concerns facilitate the blurring of the line between the private and the public, how can you tell who is responsible for any harm you sustain because of this, and to whom do you turn for recourse?

The blurring of the public and private sectors is itself driven by two major factors. First, there is a widespread belief that government and the private sector should work in tandem to maximize efficiency and productivity. Because of this belief, many tasks that were once performed by government are now outsourced to companies. For example, the analysis of Canadian census data has been outsourced to Lockheed Martin, which uses its own software and data-processing equipment, and the BC provincial government has contracted with a US company called Maximus for the delivery of the provincial Medical Services Plan and Pharmacare services. The second crucial factor is that new technologies facilitate the breakdown of traditional institutional distinctions both across and within sectors, allowing data to flow in both directions without the traditional oversight of a judicial warrant. So the breakdown of the barriers between the public and private sectors is both a cause and a consequence of increasing surveillance.
The patterns are complex and multiple. However, to highlight these trends, we focus on three new practices that are breaking down the institutional barriers between public and private agencies: access to communications data by law enforcement; legislative changes that require more and more sharing of personal data from companies to government, and vice versa; and the contracting out of the security function to the “surveillance industry.”

**What Prompted Private-Public Collaboration?**

From the 1980s on, Canada, along with many governments around the world, has been shrinking the public sector, privatizing government services, introducing or permitting the expansion of private security and policing, and cutting back health care, education, and pension programs. As publicly funded services have diminished, those who can afford it have turned to buying such services from the private sector. Thus, we have all become increasingly dependent on businesses and corporations to deliver the community services we rely on.

However, unlike governments, corporations tend to assume that the personal information they collect as they provide these services is a valuable corporate asset that can help generate more profit. There is thus a significant incentive to acquire and retain ever more data about citizens. The legal framework requires that corporations obtain individual consent for the collection of these data. However, as more commercial services become necessary to day-to-day living, we often face a choice between only two options: either we can consent to having our information bought and sold, or we can forego the benefits associated with such conveniences as having a credit card, a mortgage, or access to a physiotherapist. We make a similar deal in the security context: either we consent to having our bags and communications searched, removing our shoes, providing fingerprints, and sometimes enduring personal searches or we are barred from flying.

Once those personal data are harvested, they can flow easily between corporate and government hands. For example, commercial information about us is collected and then resold by (private) “data brokers” to (public) agencies like CSIS and the police. And, of course, a body such as the (public) Canada Border Services Agency routinely has access to passenger details that (private) airlines are obliged to pass on to them before we fly. Conversely, some government information about citizens percolates through to commercial
bodies. Canada Post, for instance, sells personal “change of address” information to (private) marketers. Indeed, the postal code system itself is widely used by marketers to classify consumers.

At the same time that information began to flow more freely between the public and private sectors, the infrastructures that determine organizational practices changed. Manual files stored in physical cabinets and face-to-face and telephone meetings shifted to computer databases and networked communications platforms. The mechanical metaphors that dominated the world of paper documents, storage cabinets, and telephones were replaced by the image of electronic data that move through systems at the speed of light.

Over time, gains in efficiency accredited to new technologies were accompanied by a transformation in organizational practices. Customer relationship management (CRM) and database marketing methods were developed to analyze customers whose preferences and shopping habits were tracked and stored electronically. New software transformed how companies could obtain data directly from customers’ purchases; at the same time, companies using CRM started offering perks and rewards to consumers willing to trade their personal information for the benefits of “membership.”

The information itself became the central item of value; it could be used not only by the company that established the system but also by others interested in the spending patterns of groups and individuals. Among these are the data brokers, mentioned above, who trade in personal data. In this way, enabled by new technologies, the sluices were opened, and personal data began to flow within and between organizations in unprecedented ways. As the following examples demonstrate, it was only a matter of time until the conventional conduits of public and private also broke down, permitting first trickles and then streams of data to flow from governments to corporations and back again.

**Access to Communications Data by Law Enforcement**

One of the most compelling—and controversial—examples of the consequences of this free flow of data between the public and private sectors revolves around proposed “lawful access” provisions designed to make it easier for police to access the data generated by customers through the use of networked communications platforms.

In 2011, an Omnibus Crime Bill package, bundling together three bills, was brought before the Canadian Parliament. The relevant sections of the
bill proposed that Internet service providers (ISPs), which provide access to the Internet, be required to turn over, for “security” reasons, certain subscriber data (such as the identity of a person using a particular IP address) to the state without a warrant.* The proposed law, which in effect made ISPs take on a de facto police function, elicited deeply concerned responses from both federal and provincial privacy commissioners, who combined their concerns in a letter to Canada’s deputy minister of Public Safety. A media campaign on television and the Internet called “Stop Online Spying” sprang into life to raise awareness of the far-reaching negative consequences of passing such legislation, and 145,000 Canadians signed an online petition to voice their concerns. As a result, the provisions were shelved, and a number of months after the debacle the government indicated that it would not be pursuing the matter further. This does not necessarily mean that the matter is over. In fact, it is well established that most carriers already hand over personal data to police informally, without a warrant and without a law in place to mandate that they do so.3

The proposed law remains an excellent example of the consequences of dissolving the line between the public and private sectors and co-opting companies into the business of government. Following the logics of efficiency and privatization, the new law would have required ISPs to modify their systems for real-time surveillance. Moreover, police would have been granted new powers to obtain access to the data generated as people went about their daily lives online—shopping, working, using social media—whether or not the user was acting anonymously. There was little oversight to ensure that these powers would not be abused. One particularly problematic clause would have allowed police to force an ISP to identify an anonymous Internet user, even where there was doubt that it would be useful to any investigation. Categorical secrecy orders would have further obscured how the sweeping powers granted in the bill were being used, making it even more difficult to challenge future abuses of these powers in court.

Critics argued that, should the bill become law, Canadian citizens, ISPs, social networks, and even handsets and cars would be turned into spy tools for the state. Although the bill failed to become law, its introduction shows clearly how the trend toward public-private blurring alters time-honoured expectations about the kind of relationship citizens in a democracy can enjoy with their government.

* An IP address is a number given to each device (computer, printer, etc.) that is part of a computer network connected to the Internet.
These legislative conflicts also reveal the extent to which private companies can be regarded as essential tools for law enforcement. Google, for instance, regularly reports the number of law enforcement requests for information about its users by country. As Google has become more popular, the number of requests has increased significantly. Google complies with such Canadian requests in roughly 24 percent of cases (contrast Twitter’s 7 percent), although there are significant national variations and few details about the types of requests received. A number of online companies have been lobbying hard for clear and consistent legal standards, which would allow them to know the conditions under which these requests should be accepted or refused. Google is reasonably transparent about these processes. Most companies are not. Note, however, that Canadian companies such as Distributel and TekSavvy resist warrantless access to user data. Smaller Internet service providers without extensive legal staff might find it far more difficult to refuse requests for user data.

More worrying is the amount of data that might be shared through this back door access. This issue hit the news in a big way in 2005 when the Electronic Frontier Foundation received whistleblower evidence from the United States that AT&T had allowed the installation of a fibre optic splitter at its facility in San Francisco. The US National Security Agency (NSA) was using the splitter to monitor the email and web browsing of all of AT&T’s customers in real time (see Trends 6 and 7). The revelation was quickly followed by a number of lawsuits against AT&T, but these were effectively brought to a halt when Congress intervened by amending the Foreign Intelligence Security Act (FISA) to shield “electronic communication service providers” like AT&T from liability when they cooperate with intelligence agencies. The FISA amendments also created penalties for companies that fail to comply with a FISA order or that even disclose the existence of the orders served on them. The legislation was renewed in January 2013 and will stay in force until at least 2018. And, of course, in the summer of 2013, the whistleblowing of Edward Snowden reignited debate over the surveillance connections between the NSA, private corporations, and personal information gleaned from ordinary citizens both in the United States and in other countries such as Canada.

The FISA amendments also incorporated “remote computing services” or “cloud computing” into the existing definition of an “electronic communication service provider.” According to a recent report to the European Parliament, this allows US agencies to access customer files and other
information at various US-owned cloud data centres in the United States, Europe, or any other country, including Canada. Moreover, one sweeping provision of the legislation authorizes the targeting of “a foreign-based political organization or foreign territory that relates to the conduct of the foreign affairs of the United States.” These provisions have not been lost on Canadian NGOs that might use the cloud-computing services of companies like Google, Microsoft, Amazon, and Apple for email and data storage facilities. And Canadian privacy law would have no jurisdiction over the intelligence operations of US federal agencies.

The desire for access to communications data by law enforcement is a major factor within the trend toward public-private agency blurring. Governments in many countries other than Canada are moving in this direction, so it is anticipated that the issue will not go away soon or easily. The fact that even without explicit laws in place—and even with clear public displeasure against such data sharing—the likelihood is that these practices will continue anyway, informally and below the radar of democratic oversight. The blurring of public and private agencies with regard to personal data is also an index of increased surveillance that is ever harder to discern and check. This is also seen in the next example, which illustrates how private data are used for public purposes.

**Private Data for Public Purposes, and Vice Versa**

You might imagine that security agencies such as CSIS or the RCMP Security Service are tasked with tracking activities like terrorism or money laundering. You would be correct, but this is also a task entrusted to businesses, such as banks, that employ dedicated personnel in data analytics and related fields to identify suspicious cases and to pass such findings to the conventional authorities. Increasingly, as we have shown, data collected by governments for a public purpose are shared with the private sector, and those collected by corporations in the course of commercial transactions are shared with governments. A good deal of this sharing is authorized by law and is therefore subject to some degree of oversight.

FINTRAC, the Financial Transactions and Reports Analysis Centre of Canada, is an excellent example. FINTRAC is mandated under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act of 2000 to “collect and analyze financial transactions, and disseminate intelligence to assist in the detection, prevention and deterrence of money laundering and terrorist
financing.” Under this legislation, all financial entities—all banks, credit unions, life insurance companies, security dealers, investment counsellors, foreign exchange dealers, property developers, casino operators, and even dealers in precious metals—are legally obliged to report to FINTRAC the details of all financial cash transactions of ten thousand dollars or more. The consent of the person to whom the information “belongs” is not required. Under a Memorandum of Understanding, the information reported to FINTRAC is then shared with the RCMP, the Canadian Police Information Centre, and similar bodies.

The FINTRAC system is possible because computing technologies have transformed the way the private sector conducts finance. Stock exchanges around the world play a pivotal role here by providing the market through which financial (and other) products are traded, and supply and demand (in theory) determine the worth and set the price. But here, too, we see the “innovative” use of masses of data: trading decisions today are “roboticized,”
buy- and sell-orders are made by powerful computers according to the proprietary algorithms that hedge funds and investment banks have programmed into them. Record keeping is computerized and trades are made at any time of the day or night. Because computers can respond more quickly than humans, electronic trading platforms have cut the time required to complete a trade to mere milliseconds, which, in turn, has caused trade volumes to soar.10

Preventing fraud in trades that occur at this speed and volume and with this level of programming sophistication and computer power can only be called a significant challenge to the government watchdogs that regulate the market. Unlike CSIS and the RCMP, these watchdogs do not have the powers, the tools, or the consent of governments to pursue lawbreakers. Instead, they require financial institutions to use real-time surveillance systems to monitor stock market trades and to signal officials when trading patterns appear abnormal. In this way, the job of policing is outsourced to the private sector conducting the business.

The passenger name records (PNRs) that are generated when we book airline tickets also provide a rich store of commercial data that can be used for government surveillance. PNRs are processed through massive global distribution systems; the main one used in Canada is Galileo, based in Colorado. PNRs can reveal a good deal of sensitive information about a traveller’s preferences: meal needs, handicaps, religious practices, and allergies, for instance. Airlines also capture data on refugees or deportees. These data are used to generate no-fly lists by prescreening programs such as Secure Flight, administered by the US Transportation Security Administration, and its Canadian equivalent, Passenger Protect.11 Sharing PNR data between countries has been a matter of continuous tension and negotiation between European data protection agencies and American authorities.

Data about Canadian citizens are also shared widely with our political parties. Under Canada’s Election Act, Elections Canada is allowed to share the basic data from the electoral list. The rules for this sharing are quitestringently laid out in this act. However, each of the main federal parties has used the information they receive from the electoral list as a foundation to construct more extensive “voter management databases” that incorporate a range of other data about voters. These additional data come from a variety of private sector sources: telephone polling, traditional canvassing methods, petitions, letters, commercially available geo-demographic and marketing databases, and the analysis of online behaviour, including social media.
These databases have become increasingly controversial for two reasons. First, they may have a significant impact on the democratic process, and second, they are unregulated by any of our privacy protection laws.12

Public data are also extensively used for private purposes. Most of these data are produced in aggregated and generic form (e.g., 64 percent of Canadians pay their credit card bills in full each month), but some are individually identified. Credit-rating companies, such as Equifax, use public information to assess your credit score in order to ascertain whether you are a “good” or “bad” credit risk. To do this, the company accesses numerous public records to determine whether you have declared bankruptcy, have liens against your property, owe outstanding fines, have a property dispute with an ex-spouse, or have any criminal convictions. Access to public data is regulated by provincial consumer credit laws.

Contracting Out Surveillance

We began by showing how the idea of contracting out public services has become commonplace. In the realm of surveillance, this produces some challenges and some new grey areas. How exactly do the legal requirements to protect personal data work out when there are two sets of rules, one for

Security System Requirements Can Violate Precepts of Dignity and Innocence

Although the logic behind systems like FINTRAC is that better information flow between the private and public sectors will enable the state to identify and prosecute illegal activity like money laundering or terrorism, this kind of surveillance can create real hardships for individuals who are wrongly identified as “suspicious.”

For example, a Canadian student studying in the United Kingdom can trigger an investigation simply by depositing a scholarship in a British bank account. A sudden, large increase in the amount of money in an account, especially a new account, is one of the factors that may flag illegal activity and bring about a criminal investigation. In addition, since British universities with a licence to recruit international students under the points-based immigration system are required to monitor their attendance, just skipping classes can get foreign students into trouble with the law. Should they miss “ten consecutive expected contacts” without permission, the university must report them to the authorities.
The University of East London goes one step further: foreign students who miss 25 percent of their classes are automatically deregistered. Other schools require foreign students to physically check in with staff. At Coventry University, foreign students must present their student identity cards at designated monitoring stations at least three times a week. Both the University of Greenwich and the University of the West of England require foreign students to check in once a month. The UK National Union of Students has taken a stand against this kind of monitoring, arguing that physical checks are discriminatory and violate the dignity of foreign students. The Union of Students also fears that these kinds of practices damage the relationships of trust that are at the heart of the academy.\(^1\)


government and the other for the commercial sector? During 2012–13, for example, the governments of both British Columbia and Ontario considered using “common identifiers” for citizens who obtain government benefits, such as social assistance or employment insurance. Quite apart from the difficulty of handling the large databases involved, there are significant issues around accountability—who will be responsible for the personal data, the corporations supplying the equipment or the relevant government departments delivering the benefits? Will some database management be contracted out to private corporations? Will the common identifiers eventually be used in all government dealings with an individual? What rules will apply, the ones for the public sector or the ones for the private sector?

These questions have become even more difficult to resolve because partnerships between governments and private organizations in the business of surveillance are now a global phenomenon. Indeed, in most cases, the collaboration is so close that it is impossible to determine which party is dominant. In these collaborations, the public sector typically provides the money but delegates the nitty-gritty of decision making—regarding which security products should be purchased, for example—to the private sector as the acknowledged “experts” in the field. But since government contracts are worth millions of dollars to the companies involved, it is in the interests of
technology companies to generate as much business as possible by selling ever more surveillance products (not to mention updates and maintenance). It is also in their interests to reinforce the security concerns that drive governments to make these purchases.

The impact of 9/11 was also economically significant. Although surveillance technologies were important before the World Trade Centre imploded, the opportunities offered by the 9/11 attacks gave a huge boost to a number of security industries. Under the mantra of “connecting the dots,” new systems
Through research and investigation, public campaigning, political engagement, strategic litigation, and naming and shaming, the campaign is having some success. The names of corporations and government agencies implicated in this trade now appear in a “Surveillance Who’s Who.” The list is growing. Are any Canadian companies on that list? Five are mentioned.²


mushroomed, from data sharing and data mining to camera surveillance, full-body scanners, wider use of passenger name records by border agencies, international data-sharing, ID cards and enhanced driver’s licences, behavioural observation, biometric technologies, and drones. These new priorities spread to “urban security,” also reflecting 9/11 priorities with, for example, restricted access and more policing at organized events. The events of 9/11 also expanded how everyday information, such as that gleaned from social media, is appropriated for security-related surveillance.¹⁴
A final example comes from the world of “mega-events.” These globally publicized gatherings of huge numbers of people include major sports or athletic events, high-level political summit meetings, and music and cultural festivals. They attract a massive security operation, and security entrepreneurs typically travel the world, moving from event to event. Because of this, novel liaisons—and thus data sharing—among military, government, and commercial organizations are also created each time a mega-event is held. The Winter Olympics in Vancouver and the G20 meetings in Toronto provided just such occasions for data sharing, whether of video images or intelligence data relating to participants.

Conclusion

This chapter comes to the stark conclusion that, in twenty-first-century Canada, surveillance is expanding steadily as personal data flow, in unprecedented ways, between private and public bodies. The blurring between these agencies may be illustrated in many ways, but the effect of driving more surveillance is common to each case. Public and private bodies have different mandates and different modes of accountability, and personal data become vulnerable to misuse and abuse as the data streams flow in new directions.

Data gathered for one purpose may easily be used for another when public and private organizations share data, which flies in the face of basic fair information practices. Also, accountability for personal-data handling becomes a real challenge when different legal regimes supposedly govern public and private entities. From the viewpoint of the ordinary citizen, it means that you can never know when personal information collected by government or police might become visible to commercial bodies or when data collected from a customer transaction could end up in a dispute over government benefits or could prevent you from boarding a flight. The complex and shifting network of relationships among public agencies, private corporations, and many other institutions in the vast grey area in between complicates the analysis, renders simplistic metaphors about Big Brother meaningless, challenges the ordinary citizen, and taxes our privacy laws.
Notes

1 See Security Intelligence Review Committee, Review of CSIS’s Private Sector Relationships SIRC Study 2010-02 (Ottawa: Canadian Security Intelligence Service, 14 February 2011).


7 Ibid., 34.


10 High-speed trading platforms have cut the time it takes to complete a trading order down to 300 microseconds. In other words, the machines can process 100,000 orders per second, or 500 million per day. In this technological arms race, predatory traders labour constantly to discover and “game” the algorithms of opposing firms. (The shelf life of an algorithm is now down to fourteen days.) See Laureen Snider, “The Technological Advantages of Stock Market Traders,” in How They Got Away with It: White-Collar Crime and the Financial Meltdown, ed. Susan Will, Stephen Handelman, and David C. Brotherton (New York: Columbia University Press, 2013), 151–70.


13 See, for example, Robert O’Harrow, No Place to Hide (Toronto: Free Press, 2005).
