Expanding Surveillance
From the Atypical to the Routine

Surveillance is consistently front-page news, and it raises some of the most pressing social, political, and ethical questions of our day. At the same time, surveillance is not new. Interpersonal face-to-face scrutiny is an inherent attribute of human coexistence, and organizations also have a long history of using surveillance for various purposes. However, we are at a historic turning point in terms of the expansion, intensification, and integration of surveillance measures. There is simply more surveillance occurring today, and the surveillance systems we now use have unprecedented abilities to see more, penetrate deeper, and forge more novel connections than has ever been the case in the past. This expansion and intensification is perhaps the most notable and unsettling development in the dynamics of surveillance and monitoring.

Two examples drawn from different institutional settings help to illustrate the scope of contemporary surveillance. The first comes from the business world and concerns the company Acxiom. An international data aggregator, Acxiom collects personal information about people, including Canadians, from different sources, which it then sells to corporations and political groups that use it for marketing and campaigning. The information that Acxiom collects is extremely diverse, including data as familiar as name, address, and telephone number. The company also amasses and sells more sensitive data, such as marital status, family status, age, ethnicity, the
value of your home, what you read, the type of car you drive, what you order over the phone or Internet, where you vacation, your hobbies, any history of mental illness you might have, your patterns of alcohol consumption, and so on. Even before the advent of social media, the quantity of information held by Axiom was immense—roughly equivalent to a stack of King James Bibles fifty thousand miles high. Given the popularity of applications like Facebook, which have revolutionized the amount of personal data available to aggregators and other organizations, that amount now massively under-represents the volume of data that Axiom processes.

The second example pertains to the collection and analysis of intelligence information from electronic sources such as cellphones and the Internet for national security purposes. Since the terrorist attacks of 9/11, Canada and the United States have increased the amount of intelligence sharing between our countries. Although the process remains highly secretive, we get occasional glimpses of the almost unimaginable amount of information that is being collected. James Bamford reports that by 2015, the American National Security Agency expects to be processing information at the astounding level of the yottabyte: ten-to-the-power-of-24 bytes. Translated to the print world, this equals one septillion—that is, one trillion trillion—pages of text. In 2011, the combined space of all computer hard drives in the world did not amount to one yottabyte.

These two illustrations involve surveillance conducted with the aid of computers, often referred to as “dataveillance.” To further round out the surveillance picture, however, one would also have to include technologies such as video cameras, drones, drug testing, automated licence plate readers, smartphones, and biometrics (that is, technologies that identify individuals on the basis of a biological characteristic). The most familiar way to identify someone through biometrics is fingerprinting, but biometric systems can now identify people based on their DNA, facial structure, hand geometry, voice, way of walking, and eye retina or iris patterns. Together, all of these phenomena are producing, and will continue to produce, sweeping transformations in almost every realm of existence, including commerce, warfare, science, international security, health, child care, work, and the formal and informal mechanisms we use to encourage people to conform to societal expectations and follow societal rules (often collectively called “social control”).

Not long ago, we might have believed that surveillance was confined to the world of espionage or directed primarily at criminals. Such assumptions were never particularly accurate given the long-standing use of
surveillance in realms such as work and commerce, but today, it is easier to recognize that surveillance has become an inescapable reality for almost everyone. Being monitored is increasingly the trade-off for reduced prices or improved services. It is also not just a visual phenomenon, since monitoring now involves the massive use of electronic data. In fact, many of us provide some of this data willingly because doing so makes our lives more convenient. The following hypothetical vignette provides a glimpse into how surveillance has become a part of the everyday routine for both Canadians and others in industrialized societies.

A Day in the Life of a Nine-year-old: Farah

Farah crushes the bedcovers around her head, postponing her morning march through breakfast and homework. Her eyes snap open as she remembers today’s plans. Today, she will receive what is perhaps a preadolescent’s most desired technology and will find herself winging her way to another country. Were she attuned to such things, she might also recognize that her day will demonstrate how visible her life and the lives of those around her have become.

She slides out of bed forty minutes before her older brother Kay’s alarm clock is set to pound in the adjacent room. Gazing out the window, Farah catches the eye of her elderly neighbour, Mrs. Krupp, who returns her wave. She and Farah became acquainted at the park, where Mrs. Krupp is one of a handful of adults who watch over the kids as they tear around the play structure.

Farah’s family moved to this Mississauga neighbourhood eighteen months ago. They bought this house because it is on a direct bus route to her mom’s job at a small computer software company. Her father, a physics professor at the University of Toronto, has had to resign himself to battling the traffic several times a week to get downtown.

Today, her dad is already at work, but Farah does not want to wake her mom. By habit, she avoids the creaky floorboards that her parents use to note when she climbs out of bed. Recently, though, they have been less vigilant, because two months ago her mom had a new baby, Bruno. Born prematurely, Bruno had to stay in the hospital for several weeks while physicians ran tests for blood gas analysis, took chest X-rays, and conducted regular cardio-respiratory monitoring. During the pregnancy, Farah’s parents became
accustomed to a high degree of medical scrutiny, given that her mom is over forty, which made her pregnancy more high risk. Consequently, Farah was often left with Mrs. Krupp while her mom went to the hospital for a raft of tests to ensure that there were no genetic anomalies and that the baby was developing according to standard norms.

Shortly before the birth, her mom had come home with a three-dimensional ultrasound image of Bruno. Farah’s parents had immediately posted the picture on her mom’s Facebook page among hundreds of pictures of Farah and her older brother. Everyone calls it Bruno’s “first picture,” but Farah doesn’t think it looks anything like him—or anyone else. She hasn’t spent a lot of time inspecting it, since she finds it kind of creepy.

That was also around the time that her dad set up the baby things, including a crib, right in Farah’s room. Clipped to the side of the crib is a new baby monitor. It allows her parents to hear Bruno, but it also has a camera connected to the Wi-Fi system, which means they can see him on their computer or smartphone from anywhere in the world. The device has night vision and zoom capability, can measure temperature and humidity, and can detect whether the baby is moving around. It even has a speaker that her parents can use to talk to Bruno remotely. Farah has wondered whether her parents use it to see and hear her as well.

Tiptoeing downstairs, she thinks how nice it is not to stumble over the clothes and computer cables that usually litter the floor. Her dad, although exhausted, has made a special effort to keep the house uncharacteristically tidy. Farah thinks he does this because of the community health nurse who has visited their home on a couple of occasions to ensure that Bruno and her mom are doing well, a visit that includes monitoring for signs of postpartum depression or psychosis. Her parents appreciate the concern but are still uncomfortable with how the nurse scans the front room and kitchen for signs that something might be awry. Hence her dad’s out-of-the-ordinary cleaning efforts.

When Farah’s brother Kay wakes up, he will dash off to an early soccer practice, which means that she can play on the computer undisturbed. She enjoys the free online games and does not linger over the implications of their terms of use, which include giving the manufacturers, among other things, permission to collect information on her physical location and phone number and to view the status of the family’s Wi-Fi. She is completely oblivious to the fact that national security agencies use online games to capture personal information. When she logs onto her favourite game the manufacturer also records the minutiae of her online behaviour, which it uses for product development.
and target marketing. The company also sells the data to other corporations eager to learn as much as possible about the consumption patterns of children. The games that Farah plays include personality questionnaires and consumer surveys. By completing the surveys, kids earn extra game points or privileges.

But right now, Farah is hungry. While making breakfast, she notices that the cereal box advertises a contest for tickets to a concert by her favourite boy band. Farah makes a mental note to ask her mom to enter for her. It will require her to go to the company’s website and key in a unique product code from the cereal box. The personal information that she must also provide, when combined with the product code, gives the cereal company precise data about the family’s lifestyle and consumption patterns and contributes
Video Games “See” into Players’ Living Rooms

Video game manufacturers are racing to provide ever more realistic gaming experiences that allow players to perform natural physical movements—for example, dancing or jumping to control a character in a game rather than pressing a series of buttons on a video game controller. The trade-off is that while such games are more immersive because they make natural movements part of play, they are also more invasive since these seeing devices are analyzing gamers’ bodies, behaviours, and environments and thus capitalizing on a rich source of personal information.

One video game system that has used this novel technology is Microsoft’s Xbox 360. Microsoft’s Internet-connected video game system, released in 2005, uses a service known as Xbox LIVE to let users play games with others online, purchase games from a digital marketplace, and keep track of their gaming statistics using digital trophies known as “achievements.”

Although the Xbox 360 has a variety of accessories, including a microphone for voice chat and a webcam for video streaming, its most interesting attachment is the Kinect, a sensor released in 2010 that can “see” a player’s body and distinguish it from furniture and even other people. The Kinect projects infrared light onto the space in front of the device. That light is reflected back by human bodies to an infrared sensitive camera on the Kinect, which tracks movement to a form of target marketing that is becoming more focused because of the greater ability to connect this information with personal data culled from other aspects of customers’ lives.

After brushing her teeth, Farah checks her Facebook account. She is officially too young to have such an account, but she and most of her friends lied about their age when registering and are now regular users. Every bit of information that Farah reveals about herself on Facebook—every event, song, or show that she “likes,” every status update and every picture—becomes part of the enormous data warehouse that the company sells to third parties. In the event of an emergency, police and security officials would also have access to the information on her page. Today, however, not much is happening, except that her friend Josh is bragging about his new toy car. Because he identifies the toy manufacturer by name, his comments will be automatically culled by firms that conduct online “data scrapes,” invisibly amassing and combining the comments of thousands of users about particular topics, products, or services. These firms then sell these data to companies
and translates players’ bodily movements into the game world. The Kinect has proven so vital to Microsoft’s business strategy in video game systems that the device will be included in successor versions of the Xbox.

This seeing capacity of the Kinect is also used to monitor emotional responses to marketing. Should Farah or her brother, or any real-world child, decide to watch a video or television program through the Xbox 360, the Kinect plays an advertisement called a “NUad” prior to the video. During this commercial, the system monitors users’ reactions to see if they are paying attention to the advertisement. Microsoft then sells this data and those from millions of other users—including players’ age, race, and gender gathered by the Kinect and Xbox LIVE, along with information about player behaviour during the commercial—to advertisers for market research. Microsoft has also patented the ability to use the Kinect to prevent people from breaking “terms of use” rules that govern how many people might watch a video or play a video game. For example, if the Kinect senses more people watching a video than are allowed under such rules, it will turn the video off. Does Microsoft have every right to enforce these rules, or is the increasing potential for sensing technologies to enforce digital rights management in physical space blurring the boundaries between Microsoft’s corporate and marketing policies, on the one hand, and the living rooms of its customers, on the other?

eager to read citizens’ candid comments about products or policies. These same firms also collect online comments about people’s views on policies and social issues, which they sell to political strategists.

As her best friend, Ariel, is not yet allowed on Facebook, Farah uses Gmail to send Ariel a funny picture of the family’s dog. Again, although the rules for Gmail say that they are too young to have an account, Farah and all of her friends just lied about their age when registering. What she does not know is that when she communicates by email, her correspondence is subjected to different levels of automated scrutiny by global security agencies that monitor the flow of email. Should she contact suspicious people or use specific words or word combinations, her correspondence could be flagged for still greater scrutiny and follow-up by security officials. Her father often observes that, as a nuclear physicist educated in Iran, it is likely that his and all other family members’ messages are routinely read.

Stepping out the door, Farah contemplates how different things look on this warm spring day compared to the image of their street on Google Street
View, which was taken in January. She only learned about Street View last week when she saw a car driving downtown with a camera sticking out of its roof. Kay then showed her some of the pictures of their neighbourhood streets available on Google’s mapping system. He was particularly eager to find the image of their friend Lani (with his face blocked out) playing with his dog in his front yard.

When Farah arrives at school, her image is captured by one of the video cameras that monitor each entranceway. The cameras were installed a few months ago by the school principal after a spate of graffiti appeared on the school walls.*

Farah hurries to her classroom because today is standardized-test day and she is anxious to do well. Her brother’s poor test scores have restricted his ability to enrol in his preferred high school courses, and she does not want to end up in Kay’s situation. Farah’s test scores will become part of her official educational dossier, which will accompany her at least until adulthood. The standardized-test scores are also used to assess teacher performance, and, in an increasingly competitive schooling environment, they have become a central means by which schools promote themselves and parents assess educational options.

With the tests done, everyone rushes outside for recess, where teachers and a security-screened parent volunteer watch over them. Josh is showing off his new toy, pointing out that what makes the car particularly cool is that it contains a small video camera. When at home, he roars the car around his house and it records what it sees; he has already downloaded the video onto a computer. He has also used it to spy on his brother and to film the car stalking his apprehensive cat (which is implanted with a machine-readable microchip for identification purposes). Josh is disappointed that the girls are not particularly impressed since several own a “Video Barbie,” a doll that also has a working video camera.

* In some American jurisdictions, children are required to wear ID cards equipped with radio frequency identification (RFID) chips that regulate access to parts of the school, produce automated attendance reports, and inform school officials exactly where every child is within the school at all times. Some schools, given concerns about childhood obesity, also require that students have their body mass documented as part of their health program. Cameras in classrooms and halls are common, and more schools are requiring children to pass through metal detectors. Several Canadian school authorities are contemplating introducing some variation of such initiatives.
Farah's brother will buy his lunch in the cafeteria today with cash, but his money may not work here for much longer. A major international trend in schooling is to require students to pay for snacks or meals using electronic vouchers verified by a biometric identifier, such as a fingerprint or an iris scan. These systems eliminate the headache of handling cash and have the added benefit of allowing parents to monitor the purchases made on their child's account. Parents can even specify items, such as candy or fried food, that the system will not let their kids buy.

Farah returns to school and chats briefly with Mrs. Krupp, who is accompanied by Constable Garza, the police officer who works out of the adjacent high school. Constable Garza serves as a role model and provides security, in part by cultivating an informal network of informants among the kids.

In class, Farah works on the school computers. As she visits different websites, her online behaviour is automatically monitored by electronic “cookies,” which track return visits and help to account for the increasingly targeted web advertisements that appear on her screen. Teachers keep a close eye to ensure that the kids do not visit inappropriate sites. Their vigilance is supplemented by the school’s computer software, which tracks students’ surfing behaviour, blocks them from sites deemed inappropriate, and produces automated reports on their online activity.

As the day progresses, Farah can barely contain her excitement about the fact that this evening her family will fly to Tehran to visit her extended family. Farah has often been on airplanes, but this is the first time that she has paid attention to the paperwork involved in international travel. She watched her dad apply for a visa and check the expiration dates on everyone’s passports. She also heard her parents complain about having to rush to get baby Bruno a passport, which involved the comic ordeal of trying to cajole a newborn into meeting Passport Canada’s standardized rules for how people must look on their passport photograph.

Both parents are waiting for her with an early birthday gift when Farah gets home. She already knows that her parents have acquiesced and bought her the smartphone she has been pestering them for. Initially, they were opposed to the idea of a ten-year-old having a cellphone, but they changed their minds as they learned more about the smartphone’s location-tracking abilities. They have already installed software on the phone that will allow them to pinpoint Farah’s physical location and follow her movements. Her parents have also eased their minds about the online risks to kids by installing a popular software program that allows them to access all of Farah’s
email and text messages and to see who she has phoned and which websites she has visited.

Kay arrives home complaining that he was not allowed to have a phone at Farah’s age. An exceptional athlete, Kay trains every day in the hope of making Canada’s youth soccer team. Should he be selected, he will be subjected to random blood and urine tests.*

Everyone makes final preparations for the trip. Since the introduction of new security measures after the 9/11 terrorist attacks, Farah’s dad has become obsessed about arriving at the airport extra early. Given his profession, his Iranian heritage, and the fact that he travels frequently to the Middle East, he worries that the prescreening of passengers might inadvertently place him on a no-fly list. Having the common Iranian last name of Farad compounds the possibilities for mistaken identity, so he leaves plenty of time to sort things out should there be any confusion.

The taxi arrives and Farah’s mom sets the house alarm. Her parents have had an alarm all of Farah’s life, but they recently upgraded to a service that monitors for intruders, fire, carbon monoxide, and flooding. There are also cameras on the entrances that can be watched from a computer or smartphone anywhere on earth provided there is an Internet connection. On a recent trip to Turkey, her dad used his phone to watch the kids leave for school while he himself was in his hotel room overlooking the Bosporus.

As Farah’s family cram into the taxi, they are photographed by a tiny camera near the windshield. Images of the cab driving to the airport are also captured by overhead traffic cameras. To avoid the rush-hour congestion, the driver veers onto the electronic toll road. Elevated sensors connect with the taxi’s transponder, an electronic device that allows the toll company to automatically identify each vehicle as soon as it enters the toll road so the toll fee can be calculated. Farah’s dad never bothered to install a transponder on the family car, so when he drives on this road, an advanced automated number plate recognition system scans his licence plate and processes a bill.

At the terminal, Farah’s dad pays for the taxi using his credit card. That transaction record then becomes one small part of his overall financial profile and also feeds into his credit rating. Everyone unloads the luggage under the gaze of police officers and the security cameras that pervade the airport.

* Some American schools require every child who wants to participate in extracurricular sports to be drug tested.
Some of these cameras are so sophisticated that they can read the text messages on Farah’s new phone from a distance. But they will soon be replaced by cameras that contain microphones, which will enable security officials to surreptitiously listen to and record personal conversations.

Farah’s dad collects their boarding passes from the automated kiosk and surrenders the family’s travel documents to an agent. A sniffer dog ambles past as they heave their luggage onto the conveyor belt. Bruno is fussy in the snaking security line, prompting Farah’s mom and dad to discuss whether this year they should sign up for the Nexus program, which would provide them with an express route through security. This would require a processing fee and the surrendering to border service officials of even more details about themselves—their work history, travel patterns, and any criminal records they might have.

At the front of the line, their documents are checked again as they feed their hand luggage into the X-ray machine. Everyone then strides through the metal detector, Dad carrying baby Bruno, who is not thrilled about being removed from his stroller. Kay’s backpack is swabbed to check for explosives. Each family member then steps into a “stickman” scanner, which will highlight any suspicious areas of their bodies. For this trip, they do not have their fingerprints scanned, but because of an extended visit last year to California while Farah’s father enjoyed a sabbatical at Stanford University, their fingerprint data are already stored on an American border security system. When they catch their connecting flight in London’s Heathrow airport, the family will also be scanned by facial-recognition software. Farah’s mom whispers to her dad that she is glad that this time, no one was selected for even more invasive screening.

Farah’s mom returns her laptop to her briefcase. Her dad snaps Bruno into the stroller, and everyone puts their shoes and belts back on. The family then troops to the executive lounge where Mom shuffles through her deck of customer loyalty cards to find the one that will grant them entry. She has cards for gasoline, groceries, hotels, coffee, cosmetics, and other services. Each membership gives perks and discounts and is part of a new information economy built upon minutely recording the consumption patterns of individual cardholders. Such information has become central to corporate decisions regarding product development, prices, and potential branch locations.

The setting sun illuminates the airplane cabin as they walk to their seats. Unbeknownst to them, an armed undercover RCMP air marshal furtively inspects everyone from his seat near the emergency exit.
Farah and her family will soon be high above Canada, but, in some respects, traces of each of them will remain behind in the form of increasingly large and refined informational profiles of text and image that have become central to how contemporary societies operate. Throughout Farah's full but not particularly remarkable day, she and her family have been monitored by different people and organizations. As a comparatively privileged family, they have a distinctive monitoring profile that is particularly focused on issues of consumption and personal security. Irrespective of one's position in society, however, all individuals can now expect to be subjected to more and different types of scrutiny than in the recent past, a trend that is poised to continue and intensify.

One might suggest that in Farah's case, much of this scrutiny can be explained by the fact that she is a child, and we expect children to be watched. However, as she matures, Farah will actually be increasingly monitored as she engages with new and different organizations. When she drives...
a car and becomes involved in work, finance, travel, sports, and social services, she will be monitored by new organizations. She will be subjected to additional forms of scrutiny if she has medical issues or becomes caught up in the criminal justice system. As she progresses through school, her educational dossier will become larger and more consequential. We might even anticipate that at least some of the futuristic prospects about interactive advertisements and camera-equipped security drones will become a reality in her world. Hers will be a world permeated by surveillance, something that will bring new opportunities but that also threatens to overwhelm existing privacy regimes and will challenge us all to contemplate how we should live our increasingly transparent lives.

**Surveillance Expansion in Context**

This “day in the life” vignette gives a sense of how different forms of surveillance are becoming common and are touching ever more spheres of daily life. However, the story also sidesteps many issues that need to be contemplated in order for us to garner a fuller and more critical appreciation of the issues raised by this expansion and intensification of surveillance. The remainder of this book addresses such issues, some of which are worth flagging at the outset.

To start with, the vignette leaves unanswered whether all of this monitoring actually accomplishes what it is supposed to accomplish. This is a vital question since, too often, the public is asked to take it on faith that surveillance will perform in the ways advertised. Serious questions, however, remain about the effectiveness of such monitoring. To take an obvious example, the global expansion of antiterrorism surveillance might thwart some terrorist attacks, but it does not stand much chance of reducing this overall threat if the social, political, and economic conditions that breed terrorism are not addressed.

More prosaically, it is not clear that the ever expanding network of surveillance cameras actually reduces crime. Evidence regarding their crime-fighting effects is extremely ambiguous, and in many instances it is clear that they do not come close to producing the types of advertised crime reductions. Moreover, even when cameras do manage to catch some
offenders, they do not necessarily represent a wise use of resources. The most in-depth data on the subject come from the United Kingdom, which has installed more cameras than any other Western nation. For example, a report produced by London’s Metropolitan Police, who have been key proponents of surveillance cameras, suggests that it takes one thousand cameras to catch a single criminal. In the face of increasing evidence that surveillance cameras are poor at reducing crime, it is intriguing that security officials are now starting to justify the use of cameras on the grounds that they make people “feel safe”—again, something that is not necessarily true.

Even asking whether surveillance systems actually work can often miss the point since it ignores the factors that motivate the introduction of some surveillance systems. While officials might proclaim that surveillance is being introduced to increase security or efficiency, the greatest appeal for policy makers is often the desire to look modern or to appear to be addressing intractable problems of crime and disorder, irrespective of whether the chosen measures actually work.

The expansion of surveillance also creates increased possibilities for systematic and consequential errors. Although surveillance proponents generally portray systems as working flawlessly, the reality is that all surveillance systems involve routine glitches and errors, and much organizational work can go into trying to identify and reduce these errors. Occasionally, systems contain so many endemic errors in personal data that organizations effectively abandon even the pretense that they are accurate; such is the case with both police databases on criminals and consumer credit reports, each of which tends to be rife with uncorrected, difficult-to-rectify mistakes. This is particularly disconcerting given how consequential those systems can be for shaping people’s life chances.

The increased prevalence of surveillance is important not simply because of how it might track and identify suspicious people but also because it can alter everyone’s behaviours. Even if the camera does not work or the locational abilities on your cellphone are turned off, living in a world permeated by surveillance subtly alters how we all act, what we say, what we post on social media—a form of self-censorship that can have a detrimental and chilling effect on political speech and action.

In addition, the vignette involving Farah and her family does not convey a sense of how surveillance might be resisted. People often find certain surveillance measures objectionable and occasionally take steps to try to eliminate or mitigate those that they see as particularly egregious or
This resistance can involve using legal measures to challenge the legality of an initiative or bringing the situation to the attention of different privacy commissioners. Such formal strategies can occasionally counter specific surveillance measures. For example, Canadian advocacy groups such as the British Columbia Civil Liberties Association and the Canadian Internet Policy and Public Interest Clinic (CIPPIC) have successfully challenged the state or transnational corporations in court and through the offices of the various information and privacy commissioners. Nonetheless, serious questions remain about whether existing privacy laws in Canada can meaningfully check the general expansion of surveillance in almost all segments of society.

Finally, the vignette does not explore the question of how the assorted surveillance systems originated or expanded. With the exception of a small number of high-profile surveillance initiatives, the expansion of most surveillance measures tends not to receive a full public airing. Instead, such expansion occurs through a process of “surveillance creep,” the expansion
Data Breaches and More Data Breaches . . .

The more our information is captured and communicated, the more likely it is that some of it will get lost. Data breaches, now big news in all advanced countries, occur when personal data on customers, patients, clients, or employees are stolen or, more likely, just carelessly mislaid or mistakenly disclosed. Increasingly frequent stories about lost laptops or remote storage devices bring home to ordinary people the practical consequences of living in a surveillance society.

Canadians have experienced many high-profile data breaches in recent years. In 2013, an employee of the federal Department of Human Resources and Skills Development lost an unencrypted USB flash drive containing the personal information of more than half a million Canadians, including Social Insurance Numbers and some health information. According to Public Accounts documents, in addition to USB drives, more than four hundred laptops and BlackBerries were lost or stolen from a wide variety of government departments in fiscal year 2012–13. Since 2002, 3,143 data breaches have occurred within federal agencies, affecting more than seven hundred thousand individuals. Only 13 percent of these breaches were reported to the Office of the Privacy Commissioner of Canada. The ability of our federal watchdog to protect our information has thus been constrained by a lack of transparency on the part of those organizations that are responsible for safeguarding our information. We have also witnessed data breaches from provincial government agencies, hospitals, universities, and from every type of business. No type of institution is immune.

When a data breach occurs, one does not know how the information might be used or to whom it might be leaked or sold. In the hands of identity thieves, isolated pieces of personal data can be combined with others to give fraudsters access to our bank accounts or credit cards. Data of existing practices to cover population groups or regions that they were not originally intended to monitor. Decisions about surveillance creep are typically opaque to the public since they are made behind the closed doors of assorted organizations. The United Kingdom, one of the most heavily surveilled places in the world, provides two iconic examples of surveillance creep. These examples could be instructive as surveillance becomes more heavily integrated in Canadian practices and policies.

The first example involves the expansion of the police DNA database. At the outset of DNA collection, British police and politicians made vociferous promises that they would only collect the DNA of the “worst of the
breaches also harm the interests and reputations of organizations, and many spend significant resources training staff and ensuring that any mobile devices used are properly password protected, and any personal data strongly encrypted. Yet breaches still occur with alarming regularity.

Some countries have strong data-breach laws that impose severe penalties for serious data breaches. Some of these laws require that letters of notification and apology be written to all individuals who might have been affected. Others require strict reporting of breaches to the relevant privacy regulator, who may then require the organization to communicate with all affected individuals if the risks are sufficiently high.

Canada’s data breach–reporting requirements are still largely voluntary. Alberta is the only province that imposes a statutory obligation on private sector organizations to disclose privacy-related data breaches. And under Ontario’s Personal Health Information Act, organizations must provide notice to the Ontario commissioner without reasonable delay. At the federal level, Bill C-12, which would amend PIPEDA and strengthen data breach–reporting requirements, was introduced in 2010. It has yet to be acted upon. Canada desperately needs stronger laws and penalties against data breaches. In the absence of these strong protections, some citizens have taken matters into their own hands and are suing an Ottawa hospital for $40 million for the loss, in 2012, of a memory stick containing data on twenty-five thousand patients.2


worst” criminals—typically, terrorists or pedophiles. Over time, these promises were forgotten as the police and prosecutors recognized the convenience of expanding the database to include the DNA of other categories of offenders, and then to include everyone convicted of a crime, no matter how minor.

Today, the British police are empowered to collect, analyze, and store the DNA of anyone who is simply suspected of being involved in a crime, which, in practice, gives the police a great deal of discretion over who is included in the database and who is not.

The second example of surveillance creep involves the introduction of surveillance cameras in British municipalities. Here, a system designed
and justified for one extraordinary purpose quickly found other more commonplace uses. Originally, the camera system was justified on the basis of antiterrorism legislation, but the authorities soon discovered that few terrorist activities are visibly apparent in Britain’s quiet boroughs. Consequently, local authorities expanded the use of the camera system such that operators were watching for such mundane misdemeanours as urinating in public, underage smoking, garbage dumping, not picking up after your dog, and delivering papers without a licence. While such things can undeniably be daily inconveniences, it is unlikely that the public would have supported an expansive and expensive camera surveillance system as a way to ensure that people were putting their recycling on the curb on the right day.

**Conclusion**

While Canadians might differ on the degree to which they support or oppose any specific surveillance measure, it is worth stressing that monitoring is a form of power—a power that operates over specifically identified individuals or through the ability to manipulate entire populations. The contemporary expansion of surveillance, such that monitoring becomes an ever more routine part of our lives, represents a tremendous shift in the balance of power between citizens and organizations. Perhaps the greatest danger in all of this is therefore not that a specific surveillance measure will be too intrusive, or that mistakes will be made in identifying or processing people, or that data will be lost. Instead, the most significant—but impossible to quantify—danger comes from the simple fact that we are creating, step by step, a society that is hard-wired for surveillance and that such devices can easily be turned to oppressive uses. From this point in history forward, our expanding surveillance infrastructure stands as a resource that will be inherited by future generations of politicians, corporate actors, or even messianic leaders. Given sufficient political will, this surveillance infrastructure can be repurposed to monitor—in remarkable detail—people whom some might see as unpalatable because of their political opinions, religious beliefs, skin colour, gender, migration status, medical history, or any number of an almost limitless list of factors that have been used throughout human history to pit people against one another. Contemplating such a scenario involves the risk of being dismissed as merely engaging in a form of “conspiracy theory,” but one does not have to believe in secret forces operating behind the scenes to
recognize that our ever expanding systems of transparency pose very real and alarming dangers.

Notes

4 Regarding social media and personal data, see Daniel Trottier, Social Media as Surveillance (London: Ashgate, 2012).