It is tempting to conclude that the various trends identified in this report are simply unstoppable. Some people believe that. Sometimes that message comes across loud and clear from individuals and organizations that have vested interests in using the latest technologies to process more and more personal data for profit. The words of Scott McNealy of Sun Microsystems, spoken some ten years ago, continue to echo: “You have zero privacy anyway. Get over it.”

As the nine trends discussed here show, this advice is simplistic and slanted. Personal data are used by all kinds of organizations, with varying results, for better or for worse. But, generally speaking, organizational power over individuals is bolstered by most kinds of surveillance. Following the thrust of this book, we must label as “surveillance” many more practices than just wiretapping or the trailing of suspects by police. McNealy’s dismissal of privacy is simplistic because it fails to note the wide range of surveillance practices, and it is slanted because it deflects attention from the real power of those practices in people’s everyday lives.

So we disagree with McNealy. For all the pressures in favour of surveillance expansion, there exist significant pro-privacy forces that operate in the other direction. Thankfully, we in Canada already have some tools in place to resist the negative impact of these trends and to assert and reassert the simple principle that personal data are not a free resource that public and
Conclusion

private organizations can exploit at will. Our lives have become more transparent as a result of increased surveillance. We thus need initiatives focused on ordinary people in everyday life that aim to bring greater transparency to surveillance practices, especially those embedded within familiar transactions, devices, and environments.

Such initiatives require informed action on several fronts. Surveillance can only be stemmed if a number of approaches are used: law, self-regulation, activism, education, and technological protections as well as old-fashioned political pressure. There is enough evidence to conclude that sometimes, in some contexts, organizations can be forced to halt, and occasionally reverse, the patterns of information accumulation and mishandling documented in this volume.

An obvious place to start is the law.

Privacy does have some constitutional protection. Section 8 of the Canadian Charter of Rights and Freedoms states: “Everyone has the right to be secure against unreasonable search or seizure.” The courts have interpreted section 8 to mean that the police generally need to get a warrant before they can put a citizen under surveillance. Indeed, any time the police conduct a search without a warrant, it is up to the state to prove that the search did not violate the individual’s reasonable expectation of privacy. If the police cannot do that, the courts will generally throw out any evidence obtained through the search.

However, when it comes to applying section 8, the devil is in the details. The Supreme Court tends to divide privacy into discrete but related categories of bodily privacy, territorial privacy, and information privacy. The strongest protections have been given to bodily privacy because it “protects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal.” Less protection is given to territorial privacy, depending on your location. The courts are especially concerned about protecting privacy inside the home. Once you leave your home, however, that protection weakens.

Informational privacy tends to be at the bottom of the hierarchy and attracts the weakest protections. Nonetheless, the Supreme Court has recognized that citizens have a privacy interest in information that “tends to reveal intimate details of the lifestyle and personal choices of the individual.” Privacy protection in this situation is based on “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”
One problem is that new technologies have blurred the lines between bodily, territorial, and informational privacy. When bodies and territories can be turned into information, the level of privacy protection too often drops to the lowest common denominator. For example, although the police cannot conduct invasive physical tests without a warrant, they can analyze the DNA in a used Kleenex discarded by a suspect after an interrogation. Similarly, although the police cannot enter a house and conduct a search for drugs without a warrant, they can check the electricity records for a house and see if the occupants are using enough power to run a grow-op.

Now that information about us leaks from our bodies, our territories, and the electronic devices we carry, it is much harder for courts to discern what constitutes a reasonable expectation of privacy. For instance, in *Tessling v. R.* (2004), the RCMP used forward-looking infrared (FLIR) cameras to take a “picture” of heat leaking out from a house that turned out to contain a marijuana grow-op; the Supreme Court said that this was constitutionally permissible under section 8 of the Charter because informational privacy attracts a lower level of protection than territorial privacy. In contrast, the Supreme Court ruled, in *R. v. A.M.*, that individuals do have a reasonable expectation of privacy with respect to odours that emanate from their clothes or belongings and are detected by a drug-sniffing dog. (Of course, legal actions are not the only way to challenge violations of privacy. For instance, opponents of Smart Metering, which allows for two-way communication between a home electric meter and the utility company, have formed citizens’ coalitions that have been quite vocal in Canada. Other such responses are examined below.)

Challenging surveillance on the basis of section 8 of the Charter can thus produce ambiguous results. It can also be time consuming and expensive. Statutory privacy protections therefore tend to be more relevant for the average citizen. Over the past two decades, an increasingly complex patchwork of statutory laws has arisen to regulate surveillance practices and protect privacy interests. In Canada, unlike other countries, the privacy legal regime is generally divided between laws that regulate government surveillance and those that regulate private sector surveillance. Things are even more complicated by the fact that three levels of government—federal, provincial, and territorial—can pass laws to govern public and private sector privacy in their own jurisdictions.

Federal government information-collection practices are governed by the 1982 Privacy Act, which sets out the rules concerning how government
agencies can collect, use, and disclose personal information. The privacy commissioner of Canada, an independent officer of Parliament, oversees the act and has the capacity to sue, intervene in lawsuits, launch complaints, and conduct investigations. However, because information practices have changed a great deal since 1982, most commentators agree that this legislation is out of date and requires significant reform to confront the kinds of challenges to privacy interests that have been documented in this volume.

All provinces have passed laws governing the treatment of personal information by provincial public bodies. In most provinces, information and privacy commissioners, who are also responsible for the oversight of freedom-of-information laws in their respective provinces, administer these laws.

Private sector information-collection practices are governed at the federal level by the Personal Information Protection and Electronic Documents Act (PIPEDA), which came into full effect in 2004. This act covers all organizations, including foreign companies, that collect, use, or disclose “personal information” in the course of “commercial activity.” PIPEDA was modelled on the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information, which contains ten “fair information principles” that mirror those in other national and international privacy laws and guidelines.7

Under PIPEDA, an organization that wants to collect, use, or disclose personal information about someone must first obtain that person’s consent. When the personal information is particularly sensitive—medical or financial records, for example—the organization must explicitly ask for consent. In many situations, however, consent can be assumed to be implied. The test is whether, under similar circumstances, a “reasonable person” would expect to be asked whether he or she consents to the release of the information.

Because the “reasonable person” consent provisions within PIPEDA depend on the context, the courts have to decide whether consent is or is not implied on a case-by-case basis. For instance, in Englander v. Telus Communications Inc., an individual brought a complaint under PIPEDA against a national telephone company because the company did not disclose that it was selling customer information in electronic form to third-party marketing companies.8 In balancing the customer’s right to privacy against industry needs, the court held that first-time customers must be told before their information becomes publicly available and that they can choose not to be publicly listed and thereby prevent this information from being sold to third parties. In other words, customers must explicitly opt in to the collection, use, and disclosure of this type of personal information.
Under PIPEDA, businesses must also ensure that the personal information they collect is as accurate, complete, and up to date as is necessary for the purposes for which it will be used. The information must also be stored in a secure fashion by, for example, protecting electronic records with encryption and audit trails. In addition, upon written request, companies must provide consumers with access to the personal information stored by the organization so that any errors in the information can be corrected.

Although PIPEDA is a federal statute, it also applies to personal information collected by organizations regulated by the provinces unless the province in question already has “substantially similar” legislation. Québec, British Columbia, and Alberta currently have such laws.

In summary, with few exemptions, all organizations in Canada are covered by one privacy law or another. With few exemptions, the personal data collected on Canadian citizens are subject to basic fair information principles. (See Appendix 1 for a discussion of the major privacy protection laws in Canada.)

Do these laws work? The honest answer is “Sometimes.” They are crammed full of exemptions and qualifications that the average person would find difficult to understand. Our privacy commissioners are typically strapped for resources, which prevents them from engaging in constant and proactive educational and enforcement efforts and from keeping up with rapidly evolving technology. Furthermore, the federal privacy commissioner does not have the power to order organizations to comply with the law. But even those provincial commissioners who do have order-making powers tend to act primarily as ombudspersons, receiving and investigating complaints, quietly and confidentially, from ordinary citizens and working with public and private organizations behind the scenes. Not surprisingly, resolving complaints can be time consuming.

Many of our commissioners have strong international reputations and public profiles and are continually in the national and local media. They have had some high-profile successes. In 2009, for instance, federal Privacy Commissioner Jennifer Stoddart took on Facebook and forced it to change some of its policies. In 2012, BC’s information and privacy commissioner successfully changed the operation of automatic licence plate recognition cameras in Victoria, British Columbia. Sometimes, privacy commissioners try to act collectively, as they did to challenge the government’s “lawful access” proposals (discussed in Trends 3 and 7). They are also beginning to cooperate in enforcement actions on an international scale.
Despite the successes of legal challenges, however, all commentators would agree that law is not enough—or at least that it can only operate if it is embedded within a society that has a fundamental respect for privacy. Privacy laws inherently require that organizations be accountable for the personal data they process and that citizens care about their privacy.

A second important factor, then, is the measures that organizations themselves take to advance the case for privacy. There is much voluntary or self-regulatory activity that organizations can, and do, undertake. Within the private sector, it is now commonplace to assert that privacy is good business practice. The reasoning goes something like this: Businesses need customers to trust them. The appropriate management of personal information is key to gaining and maintaining trust. So when a website states, “Your privacy is important to us,” the business that owns the site is making that commitment so that its customers will see it as trustworthy. Some businesses even place a privacy “Good Housekeeping Seal of Approval” on their websites. But organizations that make commitments about protecting your privacy need to be made to live up to them.

There is now a significant community of “privacy professionals” who help organizations to comply with the various privacy laws and work to enhance the privacy reputation of organizations. The Canadian chapter of the International Association of Privacy Professionals (IAPP), for example, comprises consultants, auditors, lawyers, international compliance officers, and technologists, all of whom have a professional stake in the issue and who create and share best practices about appropriate “privacy management” and “risk assessment.”

Of course, privacy is only important at some times and in some contexts, and, quite often, it comes into headlong conflict with a variety of organizational and technological imperatives that promote surveillance. But lack of attention to privacy can, and does, harm business interests. Huge data breaches, for example, do nothing to help corporate reputations or stock prices. Neither does an adverse finding, or a fine, from a regulator. So private sector organizations have financial incentives to take privacy seriously.

Although the incentives are somewhat different in the public sector, government agencies, too, are keen to avoid the negative publicity associated with data breaches and take steps to avoid such infractions. For instance, many federal and provincial agencies are required to produce privacy impact assessments (PIAs) to try to ensure that privacy is protected when a new policy is implemented. PIAs are meant to provide agencies with a consistent
framework to evaluate departmental policies and procedures in terms of their impact on privacy rights and interests. More often than not, however, they are no more than routine checklists that serve to legitimate new programs rather than to subject them to rigorous scrutiny.

Another way to protect privacy is to build it into the system of information collection and use. From the stories told here, you might assume that technology is the root of the problem—and particularly out-of-control technology that proceeds at its own pace, outstripping social analysis and legal remedies. And that is a big part of the story. But technology can be shaped to be either privacy protective or privacy invasive.

Privacy by Design (PbD) has now become conventional wisdom in the entire community of privacy professionals. Ontario’s information and privacy commissioner, Ann Cavoukian, has promoted the idea most vigorously. PbD relies on seven principles:

1. be proactive rather than reactive
2. make privacy the default
3. embed privacy into the design of information systems
4. create a positive-sum rather than zero-sum solution
5. protect information throughout its life cycle
6. make your information practices visible and transparent
7. show respect for your users.

The starting point of PbD is that many organizations do not actually need personally identifiable data to fulfill some of their basic functions. In other words, we can have security and privacy with proper and proactive design. A good example is a video-surveillance system that encrypts the images by default and only allows those images to be decrypted when a crime has been committed and the police obtain a warrant. Systems like this can be expensive, and their development does conflict with a natural organizational impulse to want as much information as possible. All the same, there is now plenty of evidence that technology can be shaped to be protective rather than invasive and that privacy can be established as the default. Technology can be part of the solution.

Other privacy-enhancing technologies (PETS) are freely available to ordinary citizens. Some are basic and low-tech, and are implemented without a second thought: most of us do not want prying passersby to peer into our homes, so we close our curtains to the outside street. But the equivalent of
“curtains” against prying eyes is now available online: encryption and anonymous remailer programs for our email, privacy buttons installed in most Internet browsers that prevent cookies from being logged, spam filters, and Do Not Track (DNT) systems that prevent third-party advertisers from following your browsing behaviour. You do not have to be particularly tech savvy to use these devices. Over the years, they have become more widespread and user friendly. (See Appendix 3 for a list of commonly available online tools for protecting your privacy.)

These examples illustrate that individual citizens can take steps to protect their own privacy and to hold organizations accountable. We are often asked for excessive and irrelevant personal data by government agencies and by businesses. Canadian privacy laws say that the information collected must be relevant or proportionate to the organization’s needs. The simple act of asking an organization why it requires your personal information can have an important educational effect on that organization and its employees. In 2012, for example, a prospective tenant in Alberta complained when his landlord asked him to provide his Social Insurance Number on a rental application form. The Alberta commissioner forbade the practice on the grounds that the SIN had no connection to determining whether the individual was an appropriate tenant.14

Similarly, in the private sector, Canadians can choose to buy goods and services only from businesses that respect their privacy rights and interests. When consumers believe that a business has violated rights that are protected by law, they can report this alleged violation to their relevant provincial or federal privacy commissioner. And they can also take their business elsewhere.

Research suggests that individuals do resist surveillance. Sociologist Gary Marx has explored the many inventive ways that individuals have found to avoid or thwart surveillance efforts, among them obscuring their identities, distorting their data, and refusing to comply.15 More radical privacy activism takes this resistance one step further when ordinary people watch and record those individuals and organizations that watch us—someone using his or her smartphone to record an abusive police practice, for instance. Mapping out the locations of surveillance cameras in a city and posting them online is a similar example.

Beyond individual resistance, there is always scope for collective action through civil society organizations.16 Privacy advocacy organizations adopt several different strategies: they use online and offline media to publicize
problems and raise issues, they lodge complaints to privacy commissioners, they engage in important research projects, they promote educational efforts, and they file access-to-information requests. They have meagre resources, but they can and do inform, embarrass, educate, and apply appropriate leverage when surveillance measures get out of hand. The Stop Online Spying campaign against the government’s “lawful access” proposals, described in Trends 3 and 7, is a case in point. The success of these efforts points to the important role that public education can and does play in promoting better privacy policy.

Our children also need to be educated about the importance of privacy. The Canadian NGO MediaSmarts has been developing and delivering award-winning privacy education to Canadian young people since 1996. MediaSmarts works with schools and libraries across the country teaching young people to critically evaluate the impact of surveillance in their schools, at the mall, and on social media. The organization also helps young people to understand the important role that privacy plays in democratic citizenship. We can be proud that MediaSmart’s approach has been emulated by digital literacy organizations in Europe and the United States.

Let us not also forget that some surveillance is just plain stupid, self-serving, pointless, futile, and ripe for sarcasm and lampooning. Humour has played, and continues to play, a crucial role in pointing out the oddities of our surveillance culture. In 2003 and 2006, the NGO Privacy International awarded Stupid Security Awards to the most egregious examples of absurd security measures.17 These examples are easy to lampoon because they are visible.

Most surveillance, though, is now routine and embedded, and less and less visible even as it grows more and more commonplace. Surveillance is generally a technique of social power and control that relies on the easy visibility of the one being watched and the relative invisibility of the one doing the watching. It is also designed to enhance the influence of the watcher over the person or group being watched. Regardless of whether the exercise of such power is legitimate or benign, it inevitably challenges liberal democratic norms founded on citizen autonomy.

The conventional way to address such tensions is through openness, public debate, and oversight. The absence of such regulating measures invites abuse and corruption, as those in the privileged watcher position take inappropriate advantage of the less powerful and, consequently, have even more incentive to hide their activities. This poses a special risk when surveillance
is embedded in everyday objects or buildings: such practices are rarely visible from the outside and are usually bundled up with the more legitimate activities on which they depend. Openness and transparency, then, are critical to making those who carry out surveillance democratically accountable.

We have described a variety of approaches and tools: law, self-regulation, privacy-enhancing technologies, consumer education, individual resistance, and collective activism. Each can be made to work in particular contexts. They are all necessary, and none alone is sufficient. But do they all add up to a political strategy? Is there a politics of privacy, or of “antisurveillance”? Canadians undeniably care about their privacy, and politicians who forget this can find themselves up against a wall of criticism. As described in Trend 7, this is exactly what happened when the federal government tried to pass Bill C-30, its online surveillance bill.

Being Canadian in the twenty-first century means experiencing mass surveillance; our lives are transparent to many organizations. This makes a difference, not only because our privacy can be compromised but also because our opportunities and aspirations may be constrained. Profoundly, pervasively, surveillance touches us all: it is not limited to “suspects” or people with “something to hide.” Nine-year-old Farah’s story (in Trend 1) demonstrates that in our ordinary lives with family and friends, surveillance is a constant reality, for better or for worse. The personal is political.

The politics of personal data is focused on making surveillance processes transparent. This happens at many levels and with varied players. Of course, we should be more aware ourselves of the surveillance to which we are subject, whether we deal with data or disclose our own personal information. But to ask ordinary Canadians to discover how they are surveilled and to take appropriate action is laughably inadequate to the current reality. The onus is on those doing surveillance to recognize their responsibilities to those whose data they handle and to make their practices transparent to those affected by them. As the ones manipulating and reconfiguring our personal data, whether it be for profit or policing, they should be accountable to us. Canadian law requires no less, but, in practice, the law is lax and has loopholes.

This book is a wake-up call. We need to be vigilant about the trends we have detailed, aware of our complicity in them, and prepared to speak up for all who are negatively affected by surveillance today—for it is clear that, while we are all affected, some groups and individuals have a particularly raw deal. Large organizations that process personal data must be held to account for
their activities. None of the trends is inevitable. Surveillance is reversible. Privacy is not dead.

Notes

3 Ibid., para. 25.
11 On the efforts of the Global Privacy Enforcement Network, see the organization’s website, https://www.privacyenforcement.net/.
12 On the work of the International Association of Privacy Professionals in Canada, see the IASPP Canada website, https://www.privacyassociation.org/community/iapp_canada.
16 Notable among these organizations are the BC Civil Liberties Association, the BC Freedom of Information and Privacy Association, the Canadian Civil Liberties Association, the Canadian Internet Public Policy Clinic, the International Civil Liberties Monitoring Group, Ligue des