Today, our lives are transparent to others in unprecedented ways. In Canada, as elsewhere, many kinds of organizations watch what we do, keep tabs on us, check our details, and track our movements. Almost everything we do generates an electronic record: we cannot go online, walk downtown, attend a university class, pay with a credit card, hop on an airplane, or make a phone call without data being captured. Personal information is picked up, processed, stored, retrieved, bought, sold, exchanged. Our lives—or rather, those traces and trails of data, those fragments of reality to which our lives can be reduced—are visible as never before, to other individuals, to public and private organizations, to machines.

Do we care? Some shrug off this loss of privacy as an inevitable consequence of living in a digital world. Some say, “So what? In the days when people lived in villages and small towns, their lives were forever open to personal scrutiny. What we have today is just a new electronic form of the same kind of public knowledge of private lives.” Others—in particular, those who use personal data to make money—dismiss any worries as misplaced. For example, as early as 1999, Scott McNealy of the giant computer company Sun Microsystems claimed, “You have zero privacy anyway. Get over it.”1 In 2010, Facebook’s Mark Zuckerberg memorably declared: “People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.”2
In what follows, we will see that such responses range from inadequate to wrong. Surveillance does matter. It confronts us with questions that will not go away and that cannot simply be shrugged off. Yes, surveillance has exploded in a digital world, but what are its actual effects? Do we know? Yes, people in villages knew that details of their lives were open to public scrutiny, but now it is large government and business organizations, not only our neighbours, that probe our lives, and they do so on a massive scale. Yes, systems like Sun Microsystems work to diminish privacy in some settings, but “zero privacy”? This assumes that systems are all-knowing and that people cannot resist, which is clearly not the case. Yes, social media help to push the privacy envelope, but the “social norm” is much more complex and consequential than Zuckerberg cares to think. These simplistic (not to mention self-serving) responses to a complex situation fail to grasp the personal, social, and political consequences of surveillance. As Canadian Internet guru Don Tapscott says, “With radical transparency, all of our identities and behaviours become flattened and observable by others—and we lose control.”

“The New Transparency,” the title of the seven-year research project that prompted this book, was chosen to drive home the point that we are visible to others as never before. The extent to which personal information is gathered, processed, and retained is unparalleled in human history—a fact that may produce feelings of discomfort or uncertainty about our own lives. I did not intend that photo to be seen by a potential employer, we may realize in hindsight. Why is this store asking for my phone number yet again? But the subtitle of the research project is “Surveillance and Social Sorting.” This phrase is meant to spotlight not only our discomfort at being exposed—surveilled—but also a second issue: What happens to us when our personal information is collected and used by others? Having a sense of control over our public persona is vitally important, as are the ways in which we are profiled and categorized, because such processes have an impact on our life chances and choices. We are treated differently depending on our profiles, and such treatment, in turn, changes our present and our future. This is social sorting.

The “we” here refers to Canadians. Surveillance, of course, knows no national boundaries. But while similar processes occur in other countries, this book spotlights how surveillance is being augmented and intensified in Canada. And Canadians do care. For instance, more than half (55 percent) of Canadians polled in 2012 said that they object to police and intelligence services, even with a court order, obtaining information from content posted on social media sites. Two-thirds of Canadians polled in the same
year disagreed with the statement that the “police and intelligence agencies should have more powers to ensure security even if it means Canadians have to give up some personal privacy safeguards.” And 90 percent object to companies like Google selling their information to others. As surveillance spreads, Canadians need to know not just about specific and spectacular cases of privacy invasion or security breaches but also about the key trends in surveillance. We badly need a way to put our experiences, our anxieties, and our hopes about the treatment of personal data in context. And we need to communicate these trends to policy makers, technical experts, information officers, educators, and the like so that we all have a voice in shaping the future of digitally dependent Canada.

**What Is Surveillance?**

Not long ago, the word *surveillance* conjured up a mental image of agents in trench coats with raised collars shadowing suspects through dingy streets or placing hidden bugs in the homes of their targets. Today, all that has changed. Not that such things no longer happen; they do. But surveillance is much, much broader than that. Bureaucracies have always, for the sake of efficiency and enlarged capacity, kept files and stored information on individuals. Now, computer and communication technologies take this much further. For instance, whereas yesterday’s filing cabinets for paper documents created single silos of information that only a few could access, with today’s searchable networked databases, information now grows and flows in ways that would have been unimaginable to the office clerks of yesteryear. And, today, information is easy to access: a few keywords and clicks, and—voilà!—entire biographies can be made to appear.

It does not stop there. It is not just that more personal information is circulating and is being used in new ways to promote today’s political and economic priorities and to manage risk. In Canada, for example, novel ways of thinking about our border with the United States as a “security perimeter” have had concrete consequences: personal information now flows more freely south, the security of international trade is now a key purpose of security efforts, and risk-management criteria help to determine who is—and who is not—allowed to travel freely based on the radio frequency identification (RFID) tags embedded in passports or on the images collected from full-body scanners.
What happens to personal information is crucial, then. People with certain kinds of profiles “pass” with greater ease than others. And this is true not only at the border but also in the marketplace. Your frequent flyer card at the airport and your loyalty card in the supermarket are the visible tip of a hidden iceberg. If that iceberg were exposed, it would show a series of systems constantly busy collecting and sorting troves of data. At the airport, some Canadians discover that they are on a no-fly list (called “Passenger Protect” in Canada), while others can daydream their way through security checks. On the phone to a customer service agent, some consumers discover that they are unexpectedly rewarded, while others cannot get past the “Your call is important to us . . .” holding position. Surveillance underlies all of these processes.

Surveillance today is not just a matter of tracking “bad” or “dangerous” people. Statistics and software together turn surveillance into a way of classifying people based on whatever personal data are available. Yesterday’s target was a person; today’s target is a profile. Yet, as we have seen, that profile packs a punch. You soon know if the profile associated with you is categorized as risky or reliable, one to be rewarded or rebuffed. But how did it happen? What information pushes your profile in one direction, not another? Surveillance was once literally “watching”; now, it is also “seeing with data.” How those data are collected, manipulated, and acted on is pivotal.

So what exactly is surveillance? We define it as any systematic focus on personal information in order to influence, manage, entitle, or control those whose information is collected. Put this way, it is clear that surveillance can be good or bad, acceptable or not. But it is also clear that surveillance is more than peeping at, snooping, or eavesdropping on others. Surveillance is a dominant organizational practice that often results in people being categorized in ways that facilitate different forms of treatment for different individuals. From Google to Homeland Security, from Revenue Canada to the RCMP, this sort of surveillance is central. Perhaps we should say, this sorting of surveillance, because the big question is how we are socially sorted by surveillance today.

At the same time, the rapid expansion of many kinds of surveillance has prompted or facilitated its further growth in new directions. Most of this volume is about surveillance by organizations that gather data on individuals and populations, profiling them for various purposes. However, ordinary individuals are engaging in an increasing amount of small-scale surveillance. They may set up home security systems, or install nanny cams (video cameras hidden in such things as teddy bears or clocks), or track others using social media (see Trend 9). Still others may try to “return the gaze” of
organizations as they watch for abusive or illegal organizational practices. The decisive difference between individuals and organizations is the kind of power available to each. Even though ordinary Facebook users have access to the largest facial-recognition system in the world (Facebook’s “tag suggestion”), they do not control the algorithms that classify people into groups for differential treatment. This is why the social sorting dimension, available primarily to large organizations, is vital for understanding contemporary surveillance.

Surveillance is now a ubiquitous and complex phenomenon. On the one hand, it is the routine way in which many organizations work, often with benign consequences. On the other hand, surveillance is a form of power that affects everyone, sometimes as identifiable individuals and sometimes as whole populations. Some groups are touched by surveillance more than others, but in all cases the balance of power between individuals and organizations shifts with the growth of new surveillance practices and processes. So while surveillance may produce good or bad outcomes, it is never neutral. And the issues are far too important to leave to bureaucrats, politicians, or technical experts. In what follows, much of the focus is on the questionable aspects of surveillance, and we conclude with how we might rise to the new challenges before us.

**Surveillance in Canada: The Context**

As in any country in the world, surveillance is vital to government and commerce in Canada. Indeed, with its early commitment in the 1960s to high technology and to the growth of an information infrastructure, as seen in the country’s use of mainframe computers and its pan-Canadian telephone grid, Canada was a leader in processing personal information. Operational efficiency was seen as a key goal. From the beginning, however, it was also clear that socio-political values influenced how computerization occurred and thus how different groups were affected. As early as 1940, the Dominion Bureau of Statistics (predecessor to Statistics Canada) used punch cards and sorting and tabulating machines for the National Registration process to determine who was “available” for conscription into the armed forces. Germans, Italians, Japanese, and Doukhobors were “ineligible,” as were Chinese and Indian residents. Social sorting has increased and intensified since that time. Today, information technology (IT) enables more precise classification of groups,
increases reliance on private sector companies, and facilitates and fosters the sharing of information within and between organizations.11

It must be said, too, that the need for regulation—for legal limits on data processing—was acknowledged from the start. Indeed, for many around the world, Canada is seen as a beacon when considering how personal data are protected and privacy is upheld. The Canadian network of privacy commissioners, who can receive and act on complaints, is the envy of many countries. Canadians have much to be grateful for in the commitment of government to protecting ordinary citizens from the risks and hazards of circulating personal data. Much progress has been made over several decades.

For example, data-protection provisions were introduced into the Canadian Human Rights Act in 1977; the Canadian Charter of Rights and Freedoms (1982) includes freedom from “unreasonable search and seizure,” which has been interpreted to include protection for privacy; and the Québec Charter of Human Rights and Freedoms (section 5, 1976) says that “every person has a right to respect for his private life.” The first Canadian Privacy Act was passed in 1983, regulating how the federal government uses, collects, and discloses personal information. In 2000, another federal law, the Personal Information Protection and Electronic Documents Act (PIPEDA) was passed, regulating the use of personal data in commercial contexts. It was fully in effect by 2004.

Other countries have been slower to act or have enacted weaker protections. For example, although the United States passed its Privacy Act in 1974, earlier than Canada did, it did not establish a specific body similar to the Office of the Privacy Commissioner of Canada, which was created in 1977 to monitor and oversee compliance with privacy legislation. Americans are directed to the courts with any complaints or charges arising from their privacy laws. Ontario also scored a first, establishing in 1988 the Ontario Information Privacy Commission (IPC), a body that oversees both privacy and freedom of information. Admittedly, some believe that this apparently contradictory dual mandate dilutes the impact of the IPC. At the federal level, another important provision requiring consent appeared in the 2000 PIPEDA legislation. This provision requires organizations to obtain consent of an individual when they collect, use, or disclose his or her personal information.

Canada, however, cannot rest on its laurels. Technology changes fast, but so do commercial and government practices. If one thinks of national security or, for that matter, of social media, challenges to personal-data handling have mushroomed beyond recognition since the year 2000. Airport
security currently involves data gathering and profiling procedures—fingerprinting, camera surveillance, electronic devices in passports—that would have been unthinkable in the late 1990s. And as for social media, who would have guessed that personal data would be so freely—some say recklessly—shared online, or that a company such as Facebook that makes its profits from selling the personal data of its users would produce the world’s youngest billionaire in just a few short years?

If we look at what ordinary Canadians say, there is cause for concern. A survey conducted by the Globalization of Personal Data (GPD) Project in 2006 showed that a majority of Canadians not only care about their personal data but also take steps to protect themselves by, for example, reading privacy policies when making a purchase from a private company (49.4%) or refusing to give information to businesses when they do not believe it is necessary (77.1%)—and, in follow-up survey by Vision Critical in 2012, these figures had risen to 60 percent and 79 percent, respectively. Canadians clearly know that privacy issues affect them.

More than half of Canadians simply trust government to look after their personal data properly. However, the GPD Project’s landmark 2006 survey reported that less than half of the population is aware that there are laws to protect personal information (and this fell by a further 8 percent in the 2012 follow-up survey). Only about a third of Canadians think that they have any control over what happens to their data. And almost all Canadians are apprehensive regarding the security of government-held data, sensing the potential for it to end up in private sector hands (slightly under one-half of Canadians surveyed trust companies to protect their data) or with foreign governments—as will happen, for instance, under new “perimeter security” border provisions that increase personal-data sharing with the United States. Canadians are also leery about national security. More than half of the 2006 survey respondents said that national security measures are intrusive (this remained steady in 2012), with many believing that the government should not share personal information with law enforcement unless people are suspected of wrongdoing. About 37 percent of Canadians are certain that visible minorities ought not to have extra security checks (although this proportion shrank somewhat in 2012).

There are, of course, subtle—and at times not so subtle—differences between Québec and the rest of Canada. According to the 2006 survey cited above, Québécois are, by and large, more optimistic about the benefits of surveillance and show less concern about the collection and use of their
personal information than residents of other Canadian provinces. Fewer worry about the possibility of a national ID card, for example, and a smaller proportion think that national-security surveillance measures are intrusive. In this, they sometimes have more in common with their counterparts in European countries, many of whom tend to be comparatively unalarmed by the rise in surveillance.

However, if polling results about surveillance and privacy are in any way indicative, Canadians do care about issues such as profiling. More than half of Canadians polled in 2006 and 2012 oppose targeting visible minorities at airports, for example. But when it comes to rewards from loyalty programs or selling marketing profiles of individuals, more than half of Canadians think that these kinds of social sorting practices are acceptable. The difficulty here is that it is hard for pollsters to get at the issue of how people might be negatively affected by profiling done by marketers. Few citizens understand how some people may be marginalized in multiple ways as disadvantages stack up disproportionately for those rejected by advertisers, marketers, and service providers.

Surveillance in Canada: The Drivers

Part of the problem is that governments and corporations continue to build surveillance infrastructures faster than the public can learn about and debate the consequences. Why is surveillance growing so quickly? What pushes it forward and enables surveillance to seep into every imaginable space of our lives (and even into some we had not imagined)? Technology, law, politics, economy, culture, and our own perceptions and practices each play a part. There is no one dominant driving force behind the rapid expansion of surveillance in Canada. The combined pressures, however, originating at many levels and from many sources, propel the quest for more and more personal information. Some of this expansion seems relatively innocuous, while other aspects are downright egregious. Some is part of deliberate policy, whereas some is an unintended consequence of a legitimate or even desirable process. We discuss these matters later, but here we provide an overview of some of the causes behind the growth of surveillance in Canada.

The first driver is technological potential. Many tools have been developed over the past few decades that make systemic surveillance much easier. Because of the strong cultural belief, especially in North America,
that technology is a key to solving social and political problems, adopting new high-tech management tools frequently prompts surveillance-based solutions. This faith in technology is demonstrable: even though nontechnological solutions may exist, and even though technological solutions do not necessarily work in the ways claimed for them, the rate at which new technologies are embraced and deployed continues unabated.

This ties in tightly with the second driver, the personal-information economy. Personal information is a commercial gold mine (Facebook went public in 2012, valued at $104 billion) and is also highly valued in government departments and in policing, intelligence, and security services. Personal information is often called the “oil” of the twenty-first century—and it may be salutary to think of the risks associated with that! More than twenty years ago, consumers rebelled when Lotus Corporation launched Household Marketplace, a system that would have tracked names, addresses, income levels, and number of children for every household in the United States. Today, parallel activities are commonplace. A 2006 Canadian Internet Policy and Public Interest Clinic (CIPPC) report on Canadian “data brokers” illustrates “how detailed information about you gets into the hands of organizations with whom you have no relationship,” because those same brokers are able to sell that information to commercial organizations and governments alike. The authors conclude that “the increasing accumulation of personal data and consolidation of databases leaves individuals vulnerable to abuses by those with access to that data.”

The third driver is the turn toward neoliberalism, that is, governmental policies that stress free trade and deregulated markets. In its current form, neoliberalism emphasizes the economic role of the private as opposed to the public sector. From this perspective, the market may be relied on to ensure prosperity for all, thus reducing the primary task of the state to military and policing functions: law and order and security. The example of Lockheed Martin’s contract with the Canadian government to provide IT support and armaments, illustrates this trend well. Free-trade agreements between the United States and Canada encourage such economic interaction, but, at the same time, support for the security function spells profit for Canadian companies. However, the neoliberal state is sometimes less than liberal in how it works to reshape people’s outlooks, expectations, and choices through surveillance. For example, legitimate protest may be redefined as subversive or even terrorist activity, as the actions of environmental groups are portrayed by the Canadian Integrated Terrorism Assessment Centre.
Closely related to neoliberalism is a widespread emphasis on risk management, the fourth driver. For decades, and especially since the 1980s, Canada has relied heavily on statistical analyses of risk to guide public policy. Because so much uncertainty surrounds normal life, from accidents and disasters to financial failure or project collapse, government and related businesses need tools to mitigate or minimize risk while maximizing opportunity. But information is required to find out what the risks are, which is where surveillance comes in. A landmark study of Canadian police, for example, shows that policing was transformed in the late twentieth century by new technologies designed to identify and track risk. To perform this function, police use surveillance to watch people and then categorize them according to the level of risk they might pose. Once again, social sorting is the other side of the surveillance coin here. Proving one’s “innocence” becomes less easy for individuals falling into the wrong category, because the default position is suspicion of guilt until the system proves otherwise.

Such emphases also show up in the fifth driver, national security. Although organizations responsible for this task were already expanding in the twentieth century, responses to the attacks of 9/11 gave them a tremendous boost. The logic of risk management holds here, too. Travellers, in particular, have become acutely aware that the demands of national security require us to remove shoes, discard liquids, and display laptops. Increasingly, however, this involves surveillance of bodies as well as baggage. Have you ever noticed the sheer number of ceiling cameras above you as you pass through the security check at the airport? The Canadian Air Transport Security Authority operates these cameras as well as the now familiar body scanners. More importantly, well before departure, passenger data are used to track our movements. But the national security driver is both more and less than “national.” It relies on a network of participating countries that increasingly functions beyond the control of the Canadian government (see Trend 6). And it also justifies watchful eyes in many other areas—such as urban space, sports arenas, and schools—now deemed to have “security” dimensions.

The sixth driver is public perceptions that permit or proscribe new developments in surveillance. While it is clear, as noted earlier, that a large proportion of Canadians are cautious, if not negative, about the extensive reach of surveillance—recall that a steady 60 percent think that security surveillance is intrusive—others reluctantly or resignedly accept more and more monitoring. This is significant. It is easier to introduce new surveillance measures if people are inclined to accept them. The climate of fear
that characterizes Canadian life, especially since 9/11, inclines many to accept more surveillance. But equally important, acclimatizing ourselves to commercial surveillance online seems to make many more sanguine about surveillance in other areas. Clearly, though, if citizens dislike new measures—as was shown when an unprecedented 145,000-plus signed an online petition against “lawful access” provisions in Bill C-30 that would require Internet service providers and others to pass subscriber data to police without a warrant—the powers-that-be take notice.

The seventh driver is new laws that allow or require surveillance or relax legal limits to surveillance. Privacy laws are increasingly put under pressure to provide exemptions for law enforcement. The “lawful access” provisions that were proposed for Bill C-30, as mentioned above, are a glaring example. Ann Cavoukian, Ontario’s information and privacy commissioner, called the bill “one of the most invasive threats to our privacy and freedom that I have ever encountered.” But similar threats arise even within the current laws. For example, if an organization can demonstrate basic compliance with privacy principles, it can legally pursue surveillance practices with impunity. For instance, since 1997, the so-called Business Transformation Project has been used to reduce “welfare fraud” in Ontario, using several surveillance tools, such as “consolidated verification procedures,” that check eligibility for social assistance every twelve months. This reduces the time that case-workers can spend with their low-income clients and increases the demands on those clients to justify their daily activities. No one suggests that Ontario welfare agencies are contravening privacy laws when they share information with other government agencies, but the negative discrimination produced through their activities—especially against single mothers—is well documented.

**Surveillance in Canada: The Trends**

The best way to grasp the magnitude of surveillance changes affecting Canadians is to look at the general trends. This book examines nine key trends of surveillance—all of them large-scale changes that are accelerating faster than ever. In fact, under current conditions, it is difficult to recall just how things used to be before 9/11 or social media. The surveillance story can be told largely as a before-and-after tale. Once, Lotus Corporation—the major corporation that attempted to launch the tracking system of names,
addresses, income levels, and numbers of children in individual US households—was forced to reverse policy when consumers objected to its “Orwellian” data-collection project. Now, social media users disclose far more revealing details to a broad array of corporations with every click of the mouse. Once, you could cross the Canada-US border with no more than a driver’s licence. Now, your scrutinized personal data make the trip ahead of you, and you need an “enhanced” licence or a passport to make it past immigration control. And so on. Each of the trends discussed in this book explains how different influences interact to magnify surveillance. Each of the trends examined has profound impacts on social life, freedom, and justice in twenty-first-century Canada.

The discussion of the first trend, surveillance expansion, details some dimensions of the spread of surveillance, demonstrating that practices once considered one-time novelties are now routine and taken for granted. The second trend, securitization and surveillance, relates to the “security” driver: more areas of life are labelled risky and thus require surveillance for security. What is less and less clear, as illustrated by the third trend, the blurring of sectors, is who conducts this surveillance, because public and private agencies each play a role in often complementary or interacting ways. Such blurring is also characteristic of the fourth trend, the growing ambiguity of personal information. But while what counts as personally identifiable data becomes less clear, what is increasingly clear is that surveillance grows despite the ambiguities.

While personal data may be more ambiguous, there is nothing uncertain about the fact that surveillance is no longer just about who you are and what you are doing but also about where you are. Expanding mobile and location-based surveillance is the fifth trend. Moreover, you will be likely to encounter similar kinds of surveillance in different parts of the world: the sixth trend is the globalization of surveillance. But it, too, is complex because local cultures and conditions mean that people experience surveillance differently. Surveillance in Canada is deeply affected by global trends, but it is filtered through Canadian law, traditions, and cultures. The seventh trend, the embedding of surveillance in everyday environments, indicates that surveillance is increasingly ubiquitous and embedded in objects such as cars, buildings, and homes. But this ubiquity is not limited to objects; there is now increasing surveillance in the body, the eighth trend, because of the daily ways in which our bodies are treated as data sources, from our fingerprints or DNA to the way we walk.
The ninth trend, *growing social surveillance*, is in some ways the most recent, but it is undeniably proving highly significant. Although people watching people is nothing new, it is now tremendously enhanced by social media. As a trend, it is extraordinary. From postwar worries about Big Brother, the overbearingly vigilant tyrant, through the domestication of surveillance in the consumer scrutiny of database marketing, we have come full circle and now monitor each other. Of course, in surveillance terms, this is small potatoes compared with the power of what Google or the Canadian Security Intelligence Service (CSIS) can do. Nevertheless, could carrying out such small-scale surveillance ourselves foster the further acceptance of all kinds of surveillance as “normal”?

**Where Do We Go from Here?**

The trends described in *Transparent Lives: Surveillance in Canada* paint a striking picture. Together, they show that even though much surveillance has positive outcomes, overall, as surveillance increases, the balance of power between individuals and organizations tilts perilously toward organizations. So how much can we trust these authorities, government or commercial, as they watch us constantly? How accountable are they with our personal data? Beyond simply analyzing these trends, then, we set out some conclusions, together with policy responses and specific recommendations. We hope that, most importantly, this book will stimulate urgent public debate at many levels.

**Notes**

4. For more about The New Transparency research project, see http://www.ssequeens.org/projects/the-new-transparency.


7 On Public Safety Canada’s Passenger Protect program, see http://www.passengerprotect.gc.ca/home.html.


9 See, for example, Michael Adler and Paul Henman, “Computerizing the Welfare State,” Information, Communication and Society 8, no. 3 (2005): 315–42.


14 “The Globalization of Personal Data Project,” 13, 26, and 33; Angus Reid Global, “Privacy and Surveillance,” tables 33 and 44.


17 Regarding the belief in the efficacy of technology, see, for example, Vincent Mosco, The Technological Sublime (Cambridge, MA: MIT Press, 2004); and Arthur Kroker, Technology and the Canadian Mind (Montréal: New World Perspectives, 1984).
It's not clear who coined this phrase, but it is used, for example, by Perri 6, “The Personal Information Economy: Trends and Prospects for Consumers,” in The Glass Consumer: Life in a Surveillance Society, ed. Susanne Lace (Bristol, UK: Policy Press, 2005); and by Greg Elmer, Profiling Machines; Mapping the Personal Information Economy (Cambridge, MA: MIT Press, 2004).


Ibid., ii.


See, for example, David Lyon, Surveillance After September 11 (Cambridge, UK: Polity Press, 2003).

The 2012 Vision Critical survey shows that about 50 percent of those polled, whether social media users or not, agreed that employers should be able to use social media to check on employees (Angus Reid Global, “Privacy and Surveillance,” table 38). Does such broad acceptance of surveillance suggest that similar attitudes would prevail in other areas, such as national security surveillance?

