SURVEILLANCE, THEN AND NOW: Securing Privacy in Public Spaces

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

June 2013

Acknowledgements

I would like to express my deepest appreciation to Stephen McCammon for all his hard work and dedication! His invaluable contributions were vital in giving this paper life.

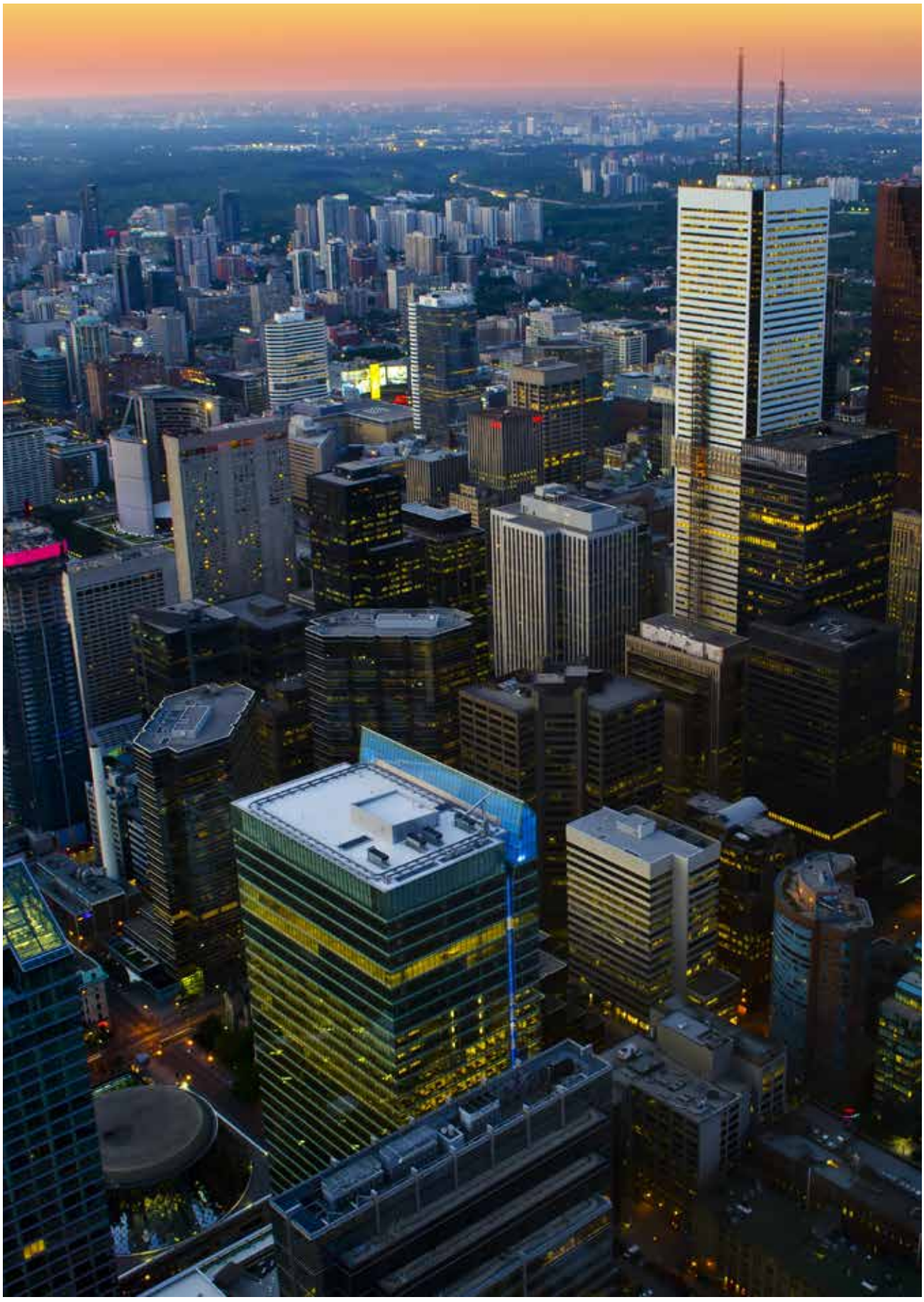
I would also like to recognize Hannah Draper for her tireless efforts and Jenny Ryu for her support in preparing this paper.

Information and Privacy Commissioner, Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Table of Contents



Executive Summary

Surveillance is growing, as are the technologies that extend its reach. But surveillance that facilitates the sustained monitoring of people engaged in everyday activities in public is, in Justice Gérard La Forest's unforgettable words, "an unthinkable prospect in a free and open society such as ours."[1]

Unthinkable as it may be, the prospect of close and continuous surveillance is no longer simply the stuff of science fiction. Governments now have access to precise and affordable technologies capable of facilitating broad programs of indiscriminate monitoring. The unfettered use of these technologies raises the spectre of a true surveillance state. To freedom-loving people, that is an unacceptable prospect.

The purpose of this paper is to assist law enforcement, lawmakers, and the broader public in understanding and protecting our fundamental right to privacy with respect to surveillance by the state of our activities in public spaces through the use of ever-growing new technologies.

Of course, our expectation of privacy in public spaces is lower than in private places. However, it is not entirely eliminated. Let us remember that the right to privacy protects people, not places. In addition, as governments consider the implications of recent terrorism-related developments in Canada and the United States, we must consider that new technologies may be able to provide increased efficiencies for law enforcement and their performance of vital public safety functions.

How can free and democratic societies ensure that the public receives the benefits associated with these new technologies, while continuing to provide strong privacy protections? To secure our right to privacy in public, in an era of explosive new technologies, requires a proactive approach that emphasizes the right to informational privacy owed to all citizens. The true value of privacy must be recognized, and ideally enhanced, not diminished, in any effort to modernize law enforcement powers.

A proactive *Privacy by Design* approach is central to designing and implementing the regulatory framework needed to properly supervise state surveillance. It is our experience that, where the use of a particular surveillance technology is justified, proportionate, and effective at delivering public safety, a proactive *positive-sum* approach is available that will ensure that privacy, accountability, and transparency are embedded into the legal and technical design specifications of any proposed surveillance system.

In an effort to encourage a proactive approach to the use and supervision of the next generation of surveillance technologies, this paper examines the following:

- The vital importance of privacy to freedom and liberty (Part I);
- How we came to secure privacy in government's information-handling practices, as well as in our private communications and activities (Part II); and
- A range of the current challenges to securing privacy in the online and digital world (Part III).

What emerges from this study is a set of 10 principles that we apply to law enforcement's use of four emerging surveillance technologies: video surveillance cameras and closed circuit television (CCTV), automatic licence plate recognition systems, geolocational tracking, and drone-based surveillance (Part IV).

One of the crucial principles is that the police power to deploy any form of intrusive surveillance technology must be supervised under a system of prior judicial authorization. The importance of this point cannot be overemphasized. Unfettered law enforcement access to surveillance technologies that are capable of facilitating indiscriminate monitoring threatens our right to a reasonable expectation of privacy, particularly where that monitoring may be continuous and persistent.

At the same time, not all surveillance programs are equally intrusive. For example, it is possible that surveillance may be effective without being persistent or penetrating. Nonetheless, with respect to the deployment of *any* surveillance technology, what will be required is the right mix of legal, administrative and technical controls to *ensure* that their use is appropriate and accountable.

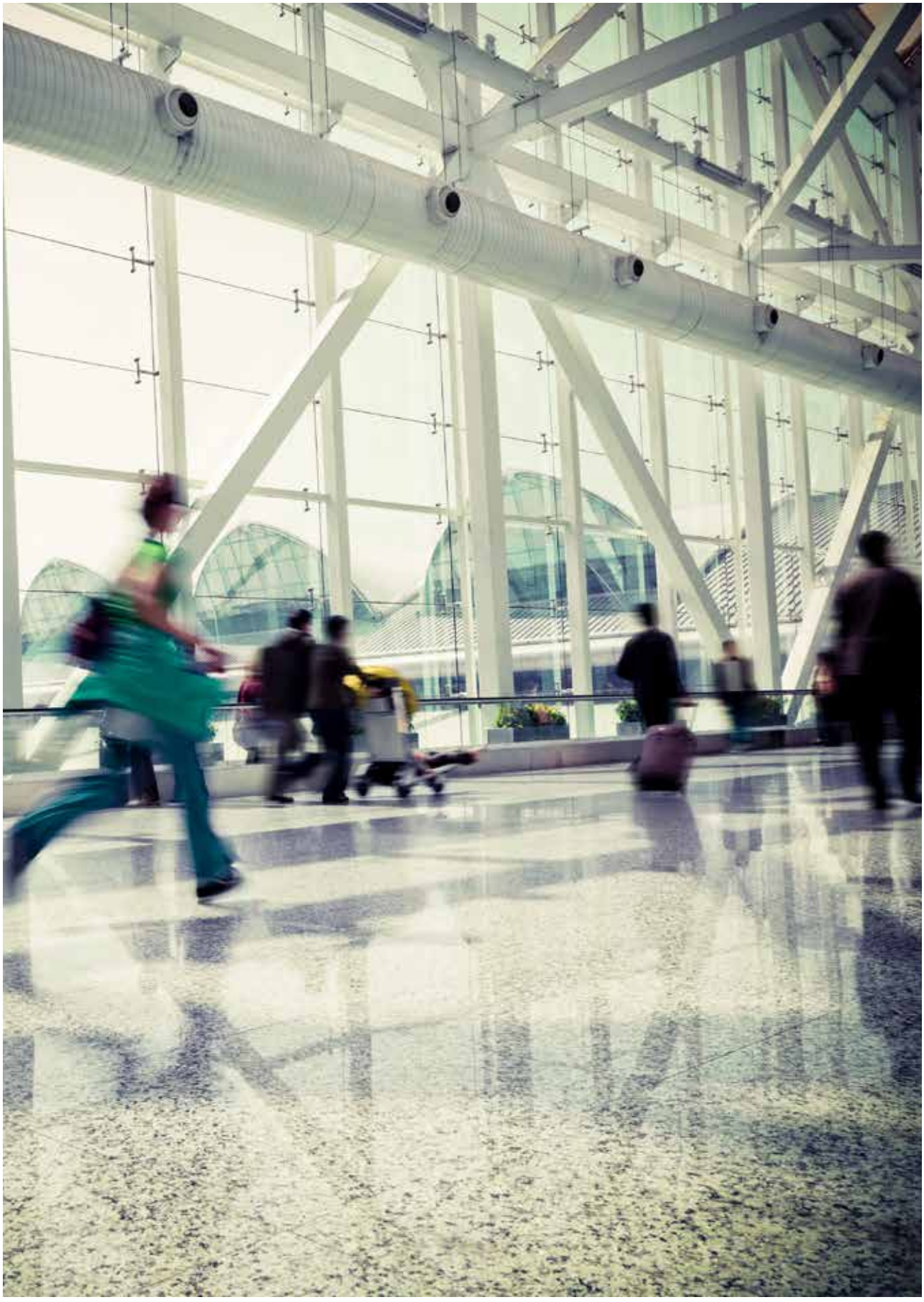
This paper sets out what we believe to be the controls necessary to ensure the appropriate and accountable use of CCTV video surveillance cameras, automatic licence plate recognition systems, geolocational tracking, and drone-based surveillance. Those controls include open, accountable and proportionate information-handling practices that are subject to independent scrutiny, including through notification and reporting requirements.

Whatever the future holds, we know that, in addition to privacy and freedom, people will require safety and security. We believe that now, and for the foreseeable future, it is essential that we strive to have both, in tandem. Freedom must be preserved from both terrorism and tyranny. While eternal vigilance will be required to secure our fundamental rights, including our right to privacy, we remain confident that we can have both public safety and personal privacy in public spaces. There is neither reason, nor need, to settle for anything less.

In summary, our approach to the proper supervision of law enforcement's use of new and emerging surveillance technologies is based upon the following key principles:

Privacy Principles in Public Spaces

1. *Data-gathering by the state should be restricted to that which is reasonably necessary to meet legitimate social objectives, and subjected to controls over its retention, subsequent use, and disclosure.*
2. *The state should be open and accountable for its information-handling practices.*
3. *Compliance with privacy rules and restrictions should be subject to independent scrutiny.*
4. *The authority to employ intrusive surveillance powers should generally be restricted to limited classes of individuals such as police officers.*
5. *The police power to deploy any form of intrusive surveillance must be supervised under a system of prior judicial authorization.*
6. *Even where genuine emergencies make it impracticable for the police to obtain judicial authorization before they employ surveillance measures, the state must remain transparent and accountable for its use of intrusive powers through subsequent, timely, and independent scrutiny of their use.*
7. *A positive-sum approach to designing a regulatory framework governing state surveillance can avoid false dichotomies and unnecessary trade-offs, demonstrating that it is indeed possible to have both public safety and personal privacy. We can and must have both effective law enforcement and rigorous privacy protections.*
8. *Close attention must be paid to the privacy impact of new technologies, business practices, and police tactics if we are to continue to ensure strong, principle-based privacy protections.*
9. *Surveillance practices that intrude upon privacy by leveraging new technological platforms or transmission processes must be scrutinized to ensure that they are accompanied by sufficiently rigorous privacy and accountability protections.*
10. *Eternal vigilance will be required to secure our fundamental rights, including the right to personal privacy in relation to all public spaces, including those found online and in other virtual spaces.*



Commissioner's Foreword

As we all adjust to the tragic bombings at the Boston Marathon, followed by the thwarted plot to derail a VIA Rail passenger train travelling between Toronto and New York, and the flurry of terrorism-related charges that ensued, it is critical that citizens of free and democratic societies raise their voices in support of those committed to achieving both security and privacy.

In this climate, the authorities in multiple jurisdictions, including the United States, will be under enormous pressure to overreact. Some officials are already arguing that they need "an enhanced ability to monitor public places."[2] Others have even suggested that, post-Boston, "privacy is overrated."[3] Of course, reasonable proposals to achieve real improvements in public safety should be welcomed, but the notion that we should somehow dispense with privacy protections is clearly excessive.

Proposals to obtain security at any cost must be resisted. In the drive for unattainably perfect security, we will invariably experience the real loss of privacy and freedom. As Benjamin Franklin, one of the founding fathers of the United States, wisely observed, "They that can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."[4]

I believe we must continue to seek measures designed to provide both security and privacy, in an accountable and transparent manner. Whether the issue is one relating to cybersecurity legislation or surveillance technologies ranging from CCTV cameras to biometrics, to automatic licence plate recognition to drones, we must reject the dated zero-sum, either/or, win/lose approach. By shifting to a positive-sum mindset focused on win-win solutions, we will be able to accommodate multiple legitimate interests, thereby avoiding unnecessary trade-offs and false dichotomies.

Introduction

> [I]n this era of explosive technology, can it be long before a device is developed that will be able to track our every movement for indefinite periods even without visual surveillance? … This is the time to begin regulating the use of electronic tracking devices while they are still in their infancy and before the law enforcement authorities begin routinely using them as part of their work habits.
>
> (*R. v. Wise*, 1992, Supreme Court of Canada Justice Gérard La Forest)

Governments around the world have long used technology to help prevent serious harm and prosecute wrongdoing. Periodically, however, in order to protect our fundamental right to privacy, lawmakers have had to respond by imposing controls on the use of intrusive new surveillance techniques. The purpose of this paper is to assist lawmakers, law enforcement, and the broader public in understanding and protecting our fundamental right to privacy, particularly with respect to state surveillance of our activities in public spaces using new technologies.

By state surveillance, we mean surveillance carried out by the law enforcement agencies responsible for investigating, prosecuting, and preventing serious harm. In the discussion that follows, we will be referring to these agencies using the terms law enforcement, the police, and the state interchangeably. As a regulator with oversight over law enforcement institutions, we have the greatest respect for the important work they do. At the same time, as Justice Jackson of the United States Supreme Court "pointed out in [a case dating back to 1948], law enforcement is a competitive enterprise in which government agents will naturally seek any strategic advantage available to them. Pursuit of that advantage naturally impels government agents, acting with the best of intentions, toward broader and more intrusive forms of surveillance."[5]

Twenty years have passed since the Supreme Court of Canada first grappled with the police use of a primitive "beeper" to track a suspect's car in *R. v. Wise*;[6] nearly 10 years since the Court looked at police surveillance from an airplane using an unsophisticated infrared radar camera in *R. v. Tessling*.[7] In the meantime, we have seen a significant increase in the state's capacity for intrusive surveillance. One emerging issue that raises substantial privacy concerns is the state's use of drones for domestic surveillance. Others include law enforcement's use of geolocational tracking and

Internet-based surveillance. Left unchecked, such surveillance will have considerable implications for the future of freedom and liberty.

Now, more than ever, it is critical that we revisit the way we supervise the state's use of new surveillance technologies. Neither a "wait and see" nor an individual "case by case" approach will suffice. Legislative rules, independent oversight, policy guidance, and administrative and technical controls can all contribute to the protection of privacy. To secure our right to privacy in an era of explosive new technologies, however, requires a proactive approach that emphasizes the right to informational privacy owed to all citizens.

The right to informational privacy or data protection includes the individual's right to exercise a significant measure of control over the collection, use, and disclosure of one's own personal information. In the context of state surveillance, individuals frequently do not have sufficient knowledge and power to effectively control the collection, use, and disclosure of their own personal information by law enforcement. Instead, the right to informational privacy must be protected by both: (i) the implementation of *Privacy by Design*[8] principles in the design and operation of legitimate state-deployed surveillance; and (ii) the insistence on legal rules and norms as found in systems of prior judicial authorization and other systems of independent oversight and accountability. The latter rules and norms are the primary focus of this paper. While special attention will be given to the Canadian context, we also look farther afield at developments in the United States (U.S.) and beyond.

Before considering some of the current challenges and emerging technologies, let us first recall the important role privacy plays in a free and democratic society, and look back at the emergence of FIPs-based[9] public sector privacy legislation and how we came to regulate some of the early and still-evolving surveillance techniques.

Part I – The Importance of Privacy

The protection of privacy is essential to safeguard the "type of society which Canadians, by the adoption of the Charter, have elected to live in." The constitutional restraints imposed on government limit its power to "pry into the lives of the citizen [and] go to the essence of a democratic state." Privacy rights and the legal rules supporting them are designed to increase government accountability while leaving individuals secure in the knowledge that "information collected by government institutions is relevant to their legitimate programs and operations."[10]

The right to privacy, which has its origins in the recognition of the inherent worth of the individual, plays a central role in the promotion of "respect for individual dignity and autonomy" and the "preservation of a free and democratic society."[11]

Privacy includes the right to exercise control over one's own person, personal spaces, and personal information. It preserves an "essential space for the development of ethically grounded citizens capable of engaging in the critical functions of public citizenship."[12] In shielding dissidents and human rights advocates, it supports and facilitates freedom of speech and freedom of association. It also helps to ensure freedom from interference and repression.

What of the right to privacy in public? "While the expectation of privacy in public spaces may be lower than in private spaces, it is not entirely eliminated."[13] We must remember that the right to privacy "protects people, not places."[14] In a 2012 case discussing the right to "public privacy" — a privacy right closely associated with our right to informational privacy — the Ontario Court of Appeal stated that "personal privacy protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society."[15] Indeed, in the information and technology era we live in, the protection of our right to informational privacy is increasingly critical to the preservation of our rights to life, liberty, and security of the person — in essence, our freedom.

Properly understood, informational privacy protects our ability to live as both private and social beings, secure in the knowledge that the state will not access our personal information or seek to identify us, let alone record and retain our conversations, communications, movements, or activities, without just cause. These rights are guaranteed under section 8 of the *Charter of Rights and Freedoms* (the *Charter*), which provides that "Everyone has the right to be *secure* against unreasonable search or seizure."[16] This right to be secure is not the security or safety interest frequently invoked as a value weighing against or overriding privacy rights. Like its antecedent in the Fourth Amendment to the U.S. *Bill of Rights*, the constitutional concept of security that animates section 8 of the *Charter* was born of "the conviction that certain kinds of searches and seizures [are] intolerable."[17]

Today, both section 8 of the *Charter* and the Fourth Amendment recognize that everyone has a right to be secure against the use of unreasonable state powers in the form of unjustifiable and intrusive searches or seizures. As a general rule, this constitutionally mandated security can only be provided by ensuring that intrusive powers are subject to timely, exacting, and independent scrutiny.

In addition, privacy legislation such as Ontario's *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)[18] ensure that people "have a right to expect the following: that their personal information will only be collected for legitimate, limited and specific purposes; that the collection of their personal information will be limited to the minimum necessary for the specified purposes; and that their personal information will only be used and disclosed for the specified purposes."[19] In our view, these general principles apply to all public space surveillance systems.

Of course, in addition to privacy and freedom, people require safety and security. Benjamin Franklin's resounding cry from 1775 bears repeating: "They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety." This declaration is as relevant today as it was then; we believe it is essential that we strive to have both together. We recognize that freedom must be preserved from both terrorism and tyranny.

And the public clearly recognizes this too. In the *aftermath* of the Boston Marathon bombings, a Time Magazine poll shows that 61 per cent of Americans are more concerned about the government enacting new antiterrorism policies that will excessively restrict civil liberties than they are about government going soft on security. Not surprisingly, at a time when private security cameras and personal cellphone cameras are always rolling (and considering their role in the quick identification and capture of the suspected bombers), Americans' tolerance for video surveillance in public places has spiked to a post-9/11 high (81 per cent are now in favour of increased cameras, up from 63 per cent). However, there are also indications that there is wariness about *enhanced* video surveillance. Two weeks *after* the bombings, support for use of facial recognition technology to scan public events has *declined* from a September 2001 high of 86 per cent to 79 per cent. More telling is the fact that "Americans are warier than ever about government monitoring of their cell phone and email communications, with 59 per cent opposed to such actions." In fact, only 38 per cent of Americans favour increased powers with respect to the monitoring of these communications, *down* from 54 per cent.[20]

Fortunately, we are not faced with the unpalatable and impractical choice of trying to prohibit the state from using emerging technologies for public safety purposes. By adopting a *Privacy by Design* framework and imposing legal, administrative, and technical controls to ensure that the use of such technologies is appropriate and accountable, we can accommodate all legitimate interests and objectives in a positive-sum, *win-win* manner, not the dated *zero-sum* model of *win/lose, either/or*. In this context, it is critical to recall that our approach to wiretapping, video surveillance and other forms of surreptitious electronic surveillance has allowed for necessary and effective law enforcement while securing the public interest in a reasonable expectation of privacy. Success in achieving a constitutionally appropriate regulatory framework has taken considerable time and debate, but the lessons learned point to the continuing need for a principled approach in order to sustain not only "peace, order and good government,"[21] but freedom and liberty.

Part II – Looking Back

Securing Privacy in Government's Information-Handling Practices

> [A] privacy protection policy intended to preserve informational privacy would therefore attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives and would attempt to maximize the control that individuals are able to exert over subsequent use and dissemination of information surrendered to institutional records keepers.[22]

In the years following the adoption of the *Charter* in 1982, comprehensive FIPs-based public sector privacy legislation was enacted across Canada. In one jurisdiction after another, federal and provincial Parliaments established rules restricting the collection, retention, use, and disclosure of personal information by institutions at all levels of government. These privacy rules also provided for rights of access and correction, complaint mechanisms, and other means of ensuring government compliance with and accountability for privacy requirements. The institutions bound by these rules include police services and a range of other institutions that carry out law enforcement functions. Independent Privacy Commissioners and ombudsmen were established to oversee compliance with privacy requirements.

The public concerns that motivated this wave of legislative activity focused on the fact that, in many circumstances, individuals were unlikely to have an effective choice to refuse to supply their personal information to the state, information holdings were becoming increasingly extensive, and there was public anxiety about government agencies sharing their holdings of personal information and building comprehensive files on individuals.

As with criminal law safeguards provided for by prior judicial authorization, FIPs-based privacy legislation was drafted with the intention of preventing privacy harms before they occur. Data minimization forms a critical component of privacy harm prevention. This principle instructs government not to collect, retain, use, or disclose any more personal information than is reasonably necessary to meet well-defined, legitimate social objectives.

Like the *Criminal Code of Canada* (*"Criminal Code"*)[23] rules providing for public reporting and after-the-fact notice with respect to wiretapping, compliance with FIPs-based privacy legislation ensures a commitment to openness and accountability. For example, government is generally required to be open about its data-handling practices, ensure the accuracy of its information holdings, and provide individuals the right to access and request a correction of their personal information. In addition, Privacy Commissioners have a role to play in recommending improved information-handling practices to ensure compliance with privacy requirements. Many may also order an institution to comply with privacy requirements.

The resulting framework of privacy statutes is not based on a confidentiality analysis in which privacy is only protected with respect to information that has been kept secret. Privacy statutes generally apply to all personal information collected by government, whether captured on the street or the Internet.[24] Moreover, a government institution's authority to collect personal information for one purpose does not entitle it to use that same information for a secondary purpose. In addition, while law enforcement officials have been granted exemptions from certain privacy rules,[25] their authority to collect, use, and disclose personal information must nonetheless fall within the scope of their law enforcement duties and powers as circumscribed in legislation, under the common law, and by the *Charter*.

The crucial principles to emerge with the rise of privacy legislation: *Data-gathering by the state should be restricted to that which is reasonably necessary to meet legitimate societal objectives, and subjected to controls over its retention, subsequent use, and disclosure. The state should be open and accountable for its information-handling practices. Compliance with privacy rules and restrictions should be subject to independent scrutiny.*

Further consideration will be given to the role of FIPs-based privacy legislation, as well as *Privacy by Design*, in Part IV of this paper. In the meantime, let us turn to consider how we came to regulate some of the early and evolving surveillance techniques.

Securing Privacy in Private Communications and Activities

> The right to privacy implies not just freedom from unreasonable search and seizure, but also the ability to identify and challenge such invasions, and to seek a meaningful remedy.
>
> (*R. v. Tse*, 2012, Supreme Court of Canada Justice Rosalie Abella)

There is a longstanding relationship between emerging technologies, police surveillance tactics, and the means by which we secure our right to privacy. Throughout this relationship, privacy has shown itself to be resilient, yet not to be taken for granted, even with respect to privacy in activities such as speaking on the telephone at home. Periodically, we face the challenge of law enforcement wanting a free hand in the use of new or evolving surveillance technologies. In response, we must ensure the proper supervision of their use of powerful new, evolving, and often undetectable surveillance technologies.

Consider, for example, that in Ontario in 1972, the decision to authorize audio surveillance of telephone conversations was made, not by a court, but by the police. At the same time, wiretapping technology had "advanced so rapidly" that the Ontario High Court of Justice recognized that:

> The apparatus used in snooping devices have been developed in such miniature and deceptive form that it has become difficult to detect that one is being subjected to its secretive observation or attention. Such listening is not now confined to apparatus directly connected with the telephone or with wires leading to one's residence. Devices have been developed that permit listening in to conversations in a room without any apparatus being installed in the premises whatsoever.[26]

While the High Court of Justice identified "a pressing need for legislation in Canada providing protection to the individual … and regulating the area within which such devices may be lawfully used," it nonetheless found that, at that time, a person had "no legally enforceable right to the privacy of his conversation even if held on the telephone." In this context, the Court was reluctant to "interfere with the judgment of the … Police [authority] as to the methods which it feels essential to meet the task of retaining law and order and suppressing crime."

Since this ruling, the public, governments, and Parliament, as well as the Courts, have given careful consideration to the police use of electronic surveillance in the course of their duties, and to the individual's right to privacy. Beginning in 1974 and with periodic updates over the ensuing decades, Parliament has laid down a detailed set of rules to both protect privacy in private communications and allow for necessary surveillance by the police. Now found in Part VI of the *Criminal Code*, these rules signal Parliament's appreciation that "as a general proposition, surreptitious electronic surveillance of the individual by an agency of the state constitutes an unreasonable search or seizure under [section] 8 of the *Canadian Charter of Rights and Freedoms*."[27]

In Canada, this means the "presumed constitutional standard for searches or seizures in the criminal sphere" is judicial authorization: "a prior determination by a neutral and impartial arbiter, acting judicially, that the search or seizure is supported by reasonable grounds, established on oath[.]"[28]

In the early 1990s, this principle-based approach to protecting privacy was extended to video surveillance as well as to "all existing means by which the agencies of the state can electronically intrude on the privacy of the individual, and any means which technology places at the disposal of law enforcement authorities in the future." In concluding that all such surveillance must be carefully regulated, the Supreme Court of Canada emphasized that:

> [T]here is an important difference between the risk that our activities may be observed by other persons, and the risk that agents of the state, in the absence of prior authorization, will permanently record those activities on videotape … To fail to recognize this distinction is to blind oneself to the fact that the threat to privacy inherent in subjecting ourselves to the ordinary observations of others pales by comparison with the threat to privacy posed by allowing the state to make permanent electronic records of our words or activities.[29]

As a result, in Canada, the police use of any device or investigative technique, including a television camera or similar electronic device, generally requires prior judicial authorization wherever its use would intrude upon a person's reasonable expectation of privacy.[30]

The crucial principle to emerge over the two decades spanning 1972 – 1992: *the police power to deploy any form of intrusive surveillance must be supervised under a system of prior judicial authorization.*

The importance of this point cannot be overemphasized. Are there exceptions to this principle? What about in "genuine emergencies?"[31] If there must be an exception to the warrant requirement in emergencies, how can we ensure that the state remains accountable for the use of such an extraordinary power?

In an April 2012 case called *R. v. Tse*, the Supreme Court of Canada ruled that the state's statutory power to engage in warrantless wiretapping in an emergency was unconstitutional. The Court gave Parliament one year to amend the relevant provision in the *Criminal Code* (section 184.4). The fact that the nearly 20-year-old power includes strict statutory conditions to help ensure that warrantless interceptions are only available in exigent circumstances to prevent serious harm was found to be insufficient. What was missing was an effective means for ensuring accountability. In this context, the Court understood that:

> Unless a criminal prosecution results, the targets of the wiretapping may never learn of the interceptions and will be unable to challenge police use of this power. There is no other measure in the *Code* to ensure specific oversight of the use of s. 184.4. For s. 8 purposes, bearing in mind that s. 184.4 allows for the highly intrusive interception of private communications without prior judicial authorization, we see that as a fatal defect.[32]

In recognizing after-the-fact accountability as a critical privacy protection required under the *Charter*, the Court emphasized that its ruling would protect privacy rights without impairing important police functions:

> The obligation to give notice to intercepted parties would not impact in any way the ability of the police to act in emergencies. It would, however, enhance the ability of targeted individuals to identify and challenge invasions to their privacy and seek meaningful remedies.[33]

As the deadline for complying with the Court's order to ensure notice loomed, Parliament passed Bill C-55, the *Response to the Supreme Court of Canada Decision in R. v. Tse Act*.[34] Not only did the bill amend the *Criminal Code* to provide that a person who has been the object of an emergency wiretap must be notified of the interception within a specified period, it went further. The federal Minister of Public Safety and provincial Attorneys General are now required to issue annual public reports on the number of interceptions made under section 184.4. In addition, the wide range of officials previously permitted to conduct electronic surveillance under Part VI of the *Criminal Code* has been restricted to police officers. Mayors, bailiffs, prison guards, and other officials no longer have access to this extraordinary power.[35]

The Court's analysis in *Tse* and Parliament's legislative response provide an excellent example of the power of positive-sum thinking. The resulting regulatory framework achieves the goal of both enabling law enforcement functions and protecting privacy, demonstrating that it is as possible as it is desirable to have both.

The key principles to emerge from Tse: *Even where genuine emergencies make it impracticable for the police to obtain judicial authorization before they employ surveillance measures, the state must remain transparent and accountable for its use of intrusive powers through subsequent timely, exacting, and independent scrutiny of their use. The authority to employ intrusive surveillance powers should generally be restricted to limited classes of individuals such as police officers. A positive-sum approach to designing a regulatory framework governing state surveillance can avoid false dichotomies and*

unnecessary trade-offs, demonstrating that it is indeed possible to have both effective public safety and rigorous privacy protections.

Given the bewildering rate at which new, complex technologies and services continue to emerge, how can we continue to ensure the preservation of our right to privacy?

The Supreme Court of Canada decided a case raising these kinds of issues in March 2013. *TELUS v. The Queen* was initiated by a communications service provider determined to protect the privacy of its texting customers. Canadians communicate with one another through millions of text messages sent every day. As part of its standard business practices, TELUS briefly preserves records of such conversations, solely for the purpose of "troubleshooting customer problems."[36]

In the course of conducting a criminal investigation, the police may need to see a suspect's text message conversations. TELUS was faced with production orders requiring it to provide the police with access to anticipated *future* strings of text messaging conversations shortly after they are created and recorded. These court orders are easier to obtain and come with fewer safeguards than Part VI wiretap warrants. Protections provided under Part VI — but missing from a production order — include limits on: which officers can apply to conduct intrusive surveillance; when they can apply (only as a "last resort"); and whose privacy will be invaded, where, and in what manner. The protections also include accountability controls in the form of requirements that the authorities provide: notice to the surveillance target(s) within certain timeframes; and annual reports to Parliament concerning the number of applications made for authorizations under Part VI and the details thereof.

TELUS successfully questioned whether the police should have too-ready access to the ongoing conversations of Canadians simply because of the technical and customer service arrangements facilitating their effective delivery. We applaud TELUS for challenging the routine collection of such information by the police.

Faced with an emerging pattern of police applying for and obtaining hundreds of less onerous production orders requiring TELUS to provide police with future access to strings of such conversations, the Supreme Court of Canada observed that "technical differences inherent in new technology should not determine the scope of protection afforded to private communications."[37] The Court held that when the police seek to seize an anticipated stream of text messages, they must observe the same rigorous privacy and accountability protections governing the interception of other live or ongoing electronic communications, such as voice calls. In so ruling, the Court recommitted itself to the proposition that "the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 [of the *Charter*] is meant to keep pace with technological development … to ensure that we are ever protected against unauthorized intrusions upon our privacy by the agents of the state, whatever technical form the means of invasion may take."[38]

The key principles to emerge from TELUS: *Close attention must be paid to the privacy impact of new technologies, business practices, and police tactics if we are to continue to ensure strong principle-based privacy protections. Surveillance practices that intrude upon privacy by leveraging new technological platforms or transmission processes must be scrutinized to ensure that they are accompanied by sufficiently rigorous privacy and accountability protections.*

Part III – Current Challenges

Securing Privacy in the Online and Digital World

> [I]n Canadian society people can reasonably expect that they can move about on public highways [or while "participating in activities on the Internet"] without being identified and continually monitored by the state. If the state chooses to engage in that kind of invasive conduct, it must be able to meet the constitutional requirements of s. 8. … [W]hile the public nature of the forum in which an activity occurs will affect the degree of privacy reasonably expected, the public nature of the forum does not eliminate all privacy claims.
>
> (*R. v. Ward*, 2012, Ontario Court of Appeal Justice David Doherty)

In 2012, in a case concerning the ability of the police to pierce online anonymity by obtaining information linking an Internet Service Provider (ISP) customer to an Internet Protocol (IP) address associated with a criminal offence conducted online,[39] the Ontario Court of Appeal held that: "Anonymity 'to some degree at least' is a feature of much Internet activity ... Depending on the totality of the circumstances, [a person's] anonymity may enjoy constitutional protection under s. 8 [of the *Charter*]."[40] In this context, the Court affirmed that the right to privacy includes the concept of "public privacy." In particular, the Court's reasoning clarified that public privacy is the right to seek and find freedom from identification and surveillance with respect to activities engaged in within public spaces, including on the street and on the Internet.[41] In coming to this conclusion, the Court held that:

> Personal privacy is about more than secrecy and confidentiality. Privacy is about being left alone by the state and not being liable to be called to account for anything and everything one does, says or thinks.[42]

In reaching this conclusion, the Court gave careful attention to the implications of new technologies and business practices, as well as the relationship between the police, ISPs, and ISP customers.

While the Court rejected the notion that law enforcement should be able to "unilaterally, and without restraint, gather information [from third parties] to identify individuals engaged in public activities of interest to the state," it recognized that ISPs can, in the appropriate circumstances, exercise their discretion to disclose the personal information of a customer to the police for the purpose of assisting an active criminal investigation.[43] In this further example of the power of positive-sum thinking, the Court's reasoning allows for the maintenance of law and order and the protection of fundamental rights.

Contemporaneously, in Canada, the U.S., and the United Kingdom (U.K.), Legislators have been asked to authorize very significant changes to the relationship between ISPs and other communications service providers and the state. With these kinds of changes, communications service providers would be much more tightly controlled by the state, particularly through legislative proposals that would require the retention and warrantless disclosure of personal information to law enforcement and security agencies. If adopted, such proposals threaten our right to digital privacy and the related right to move about and participate in activities in social spaces without the risk of being identified and monitored by the state. Fortunately, the latest developments suggest that elected officials are becoming increasingly sensitive to the concerns their constituents have about state surveillance and the right to personal privacy. Consider the fate of three such bills: the U.K. *Communications Data Bill*; the U.S. *Cyber Intelligence Sharing and Protection Act*, and Canada's Bill C-30, the *Protecting Children from Internet Predators Act*.

In the United Kingdom

The U.K. government's July 2012 draft *Communications Data Bill* seeks to extend the range of information that communications service providers will have to store for up to 12 months. It would include — for the first time — communications traffic data related to messages sent on social media, by webmail, text, tweet, and instant messaging, in voice calls over the Internet and while gaming, in addition to emails and telephone calls. This data is capable of showing who was involved in what digital activity, and when and where. Pursuant to current U.K. law, a number of investigative bodies would have warrantless access to this data, namely the police, intelligence agencies, and revenue and customs authorities. They would not need the permission of a judge to see details of the time and place of digital messages, provided that they were investigating an offence or protecting national security. The bill would, however, place restrictions on warrantless access to the data by other public bodies, including local authorities.

The draft *Communications Data Bill* was subject to substantial scrutiny by a joint committee of the House of Commons and the House of Lords, which made its final report to Parliament in December 2012. The report was highly critical of the draft bill. In response to this criticism, the British government indicated that it will rewrite the legislation. As hinted at in the Queen's May 8th, 2013 Speech to the Throne, the new draft is expected shortly. However, many remain concerned about the risks associated with mandatory data retention. In this challenging context, many key questions remain. For example, will the retention requirements and access powers be clearly spelled out in the bill? Will they be justified and proportionate? Will the data be stored securely? Will law enforcement access be properly supervised? Under what circumstances, if any, should the state be allowed to have direct access to communications network traffic, for example, by way of automated inspection tools capable of sifting through all network traffic? Answers to these questions may dictate the state of digital privacy in the U.K. for years to come.

Meanwhile, the European Union Data Directive that requires European governments like that in the U.K. to enact data retention legislation is being reviewed. And, in the background, European Courts continue to declare provisions of some of the transposing national laws unconstitutional. As observed in rulings from countries such as Romania and Germany, sweeping communications data retention requirements expose people to the potential for arbitrary state action and generate a perception of surveillance which — on its own — may impair the free exercise of fundamental rights. In addition, those Courts have indicated that such laws may not be necessary, efficacious, or appropriate given that criminals may be able to sidestep a data retention regime through the use of offshore service providers and anonymous SIM cards. Sooner or later, the European Court of Justice will likely have to determine whether the broad mandatory retention of communications data comports with the "right to a private life" guaranteed in the European Convention on Human Rights.[44]

In the United States

In February 2013, the proposed *Cyber Intelligence Sharing and Protection Act* (*CISPA*) was reintroduced before the U.S. Congress. It passed the House of Representatives in mid-April, 2013. If such a bill were enacted, it would authorize broad information-sharing between government agencies and private sector companies (including of the content of communications) and provide the private sector with substantial immunity from civil and criminal proceedings. At the same time, *CISPA* provides for a degree of post-disclosure oversight by the Inspector General and Congress.

Supporters of *CISPA* see it as a means of helping companies and government share information to catch "bad actors" who breach networks to steal information or sabotage systems. Critics worry it will trump existing privacy laws, and

allow information about the mobile activities and Internet communications of Americans to go directly to law enforcement and intelligence agencies without effective checks and balances. Given that companies are already permitted to disclose personal information to the authorities in a range of related circumstances,[45] it appears that *CISPA* sets the stage for unjustified and overbroad information-sharing.

Meanwhile, President Barack Obama's February 2013 Executive Order, "Improving Critical Infrastructure Cybersecurity," has been praised for focusing on cybersecurity solutions that do not negatively impact civil liberties. That Order directs federal departments and agencies to use their existing authorities to provide better cybersecurity, with an emphasis on increased information-sharing by government and the private sector, while adhering to "Fair Information Practice Principles, and other applicable privacy and civil liberties frameworks and polices."[46]

In this context, it is expected that cybersecurity proposals will face close scrutiny in the Senate in the months ahead, particularly in view of President Obama's April 16th, 2013 statement that he will veto an insufficiently privacy-protective *CISPA*. Indeed, at the end of April, the Senate signalled that protecting privacy will be critical to its efforts to strengthen cybersecurity. Media reports also indicate that while the Senate may yet introduce a different information-sharing bill at some point, the House version will not be advanced any further.[47] Coming up with a good plan to protect cybersecurity is, of course, essential, as is respect for privacy.

Meanwhile, on May 15th, 2013, U.S. Attorney General Eric Holder signalled that the U.S. Justice Department supports privacy protections requiring the government to obtain a probable cause warrant in order to access emails and other content stored in the Cloud. This provides further reason to be hopeful for a comparable privacy-protective approach to cybersecurity legislation.

In Canada

In Canada, proposed legislative changes introduced before Parliament in February 2012 represented the most significant attempt to rewrite the rules governing electronic surveillance since the 1970s. Unfortunately, the bill's drafters appeared to misconceive how Canadians interact with new communications technologies and significantly underestimated the sensitivity of the personal information involved. As a result, Bill C-30 amounted to a sweeping proposal for new surveillance powers without adequate attention to necessary privacy protections.

In particular, the bill would have significantly increased the state's surveillance capacity by: (i) allowing for warrantless access to subscriber information identifying and linking customers to both their online and offline, mobile and desktop activities; (ii) expanding, simplifying, and accelerating court-supervised avenues for law enforcement access to and monitoring of other sensitive digital information and activity; and (iii) giving the state significant control over the design of communications systems and software. Privacy Commissioners, civil society groups, and a wide variety of citizens spoke out forcefully against the privacy-invasive bill. While acknowledging that it contained some positive elements, we warned that it "represented a looming system of 'surveillance by design.'"[48]

An engaged public recognized the risks the bill posed to privacy in digital communications and joined together to call on their elected representatives to reject the proposed surveillance powers. To their credit, Members of Parliament and the government listened to the enormous public outcry against overbroad and warrantless access and withdrew the bill in February 2013. Together we demonstrated that the true value of privacy must be recognized — and ideally enhanced, not diminished — in any effort to modernize law enforcement powers.

With citizens calling on government to withdraw or at least rewrite controversial privacy-intrusive legislative proposals, now more than ever, it is crucial that we deepen our commitment to work together to help ensure that: (i) first and foremost, *Privacy by Design* is built into new communications systems and other technologies; and (ii) new surveillance and information-sharing regimes do not undermine the independently-supervised rules and procedures which secure our shared rights to privacy, freedom, and security of the person. Intrusive surveillance tools without adequate safeguards are a recipe for disaster.

Even if such disasters appear remote or hypothetical, history teaches us that injustice and tyranny are preceded by a rising tide of intrusions on the privacy and dignity of ordinary citizens. In the meantime, even in free and democratic societies, sophisticated and readily available technologies add a whole new dimension to the state's power to subject its citizens to surveillance. In the words of U.S. Supreme Court Justice Brennan, "[t]hey make [surveillance] more penetrating, more indiscriminate, more truly obnoxious to a free society. Electronic surveillance, in fact, makes the police omniscient, and police omniscience is one of the most effective tools of tyranny."[49] The time to maintain and strengthen democratic safeguards is now, while we enjoy a strong consensus about respect for human rights and the rule of law.

People everywhere expect and deserve privacy in their online and digital activities. The protection of both public safety and fundamental rights requires careful attention to the implications of the relationship between law enforcement agencies and communications service providers. Law enforcement's power to gather information from third parties to identify individuals engaged in activities of interest to the state must be subject to timely, exacting, and independent scrutiny in the form of the appropriate combination of prior judicial authorization and/or subsequent notice, reporting, and accountability requirements.

The preceding three principles may be particularly relevant to the emerging debate about Big Data, Data Analytics, and online privacy. ***The key principles that have emerged from recent legislative controversies and related criminal cases which we will consider in this paper are that:*** *We can and must have both effective law enforcement and rigorous privacy protections. Eternal vigilance will be required to secure our fundamental rights, including the right to privacy in relation to all public spaces, including those found online and in other virtual spaces.*

Part IV – Meeting the Future Head On

Securing the Right to Privacy in Public Spaces

> … a moment's reflection will confirm that as we go about our daily business many, if not the majority, of our activities are inevitably carried out in the plain view of other persons. The prospect that the agents of the state should be free, on account of this fact alone, to make it their business to electronically track all our comings and goings is simply an unthinkable prospect in a free and open society such as ours.
>
> (*R. v. Wise*, 1992, Supreme Court of Canada Justice Gérard La Forest)

It is one thing to be *seen* in public. It is another to be *tracked* by the state. Public spaces facilitate a range of vital, everyday activities in a democratic society: transportation, recreation, shopping, socializing, and artistic performance. "They are places in which political movements … make themselves visible" and in which the individual is able to merge into the "situational landscape."[50] Similar things can be said about tracking people in open fields and woods — spaces which facilitate solitary walks, intimacy and romance, as well as group worship.[51] Warrantless surveillance that facilitates the sustained tracking or monitoring of people engaging in everyday activities in public and open spaces is, in Supreme Court Justice La Forest's words, "an unthinkable prospect in a free and open society such as ours."

Unthinkable as it may be, the prospect of close and continuous surveillance is no longer simply the stuff of science fiction. Increasingly sophisticated surveillance technologies are being deployed by the state. Miniature surveillance drones, unseen digital recognition systems, and surreptitious geolocational monitoring are readily available, making long-term surveillance relatively "easy and cheap."[52] Unfettered law enforcement access to surveillance technologies that are capable of facilitating indiscriminate monitoring risks intruding upon our right to a reasonable expectation of privacy, particularly where that monitoring may be close and continuous.[53] After all, the right to privacy is of concern, not only to accused persons, "but to the general … public who have every right to go about their law-abiding business without being the subject of random police

searches …"[54] As previously indicated, we are not faced with the unpalatable and impractical choice of trying to prohibit the state from using emerging technologies altogether, but simply of imposing legal, administrative, and technical controls to ensure that their use is appropriate and accountable.

The Supreme Court of Canada faced the issue of the right to personal privacy in public spaces in 1992, in a case concerning the warrantless and non-consensual use of an unsophisticated tracking device — a "beeper" — installed under a car by the police. In *R. v. Wise*, the Court determined that police monitoring or tracking of a person's movements on public roads intrudes on the reasonable expectation of privacy, even if that expectation is a reduced or diminished one. Since this decision, in Canada, the use of a tracking device has required a warrant.

The U.S. Supreme Court only faced this issue head on 20 years later, in 2012, in a case involving GPS (or global positioning system) tracking.[55] In *U.S. v. Jones*, the entire Court held that the government's warrantless use of a GPS tracking device violated an individual's Fourth Amendment right to be free from unreasonable searches and seizures by the state. While the Court was divided on whether the violation resulted from the government's physical intrusion on the individual's vehicle in installing the device to monitor his movements on public streets (the view of five justices), or from a violation of the individual's reasonable expectation of privacy from long-term GPS monitoring of his movements (the view of four justices), both views recognize society's privacy interests in public places as a factor in any future Fourth Amendment analyses. This is significant given future cases will likely involve new technologies like remote location tracking technologies that do not require a physical trespass for their activation.

While both Canadians and Americans can take some comfort that they have a constitutional right to a degree of privacy in public spaces, it is critical that lawmakers and the public begin to think more proactively about the relationship between emerging technologies, police practices, and our right to privacy in public. As indicated at the outset, we live in the era of explosive new technologies.

Governments now have access to technologies capable of facilitating broad programs of continuous and indiscriminate monitoring — technologies that are increasingly precise, scalable, affordable, and widely available. Unfettered use of these technologies by law enforcement and security agencies raises the spectre of a true surveillance state.

At the same time, new technologies can provide increased efficiencies for law enforcement and safety. How can democracies ensure that the public receives the benefits associated with these new technologies, while continuing to provide strong privacy protections?

The answer to this critical question lies in the key principles and lessons that have emerged during the course of our look back, from past to present. These are summarized here as follows:

In the remainder of this paper, we will consider the application of these principles to the way we supervise law enforcement's use of a number of surveillance technologies: automatic licence plate

Privacy Principles in Public Spaces

1. *Data-gathering by the state should be restricted to that which is reasonably necessary to meet legitimate social objectives, and subjected to controls over its retention, subsequent use, and disclosure.*
2. *The state should be open and accountable for its information-handling practices.*
3. *Compliance with privacy rules and restrictions should be subject to independent scrutiny.*
4. *The authority to employ intrusive surveillance powers should generally be restricted to limited classes of individuals such as police officers.*
5. *The police power to deploy any form of intrusive surveillance must be supervised under a system of prior judicial authorization.*
6. *Even where genuine emergencies make it impracticable for the police to obtain judicial authorization before they employ surveillance measures, the state must remain transparent and accountable for its use of intrusive powers through subsequent, timely, and independent scrutiny of their use.*
7. *A positive-sum approach to designing a regulatory framework governing state surveillance can avoid false dichotomies and unnecessary trade-offs, demonstrating that it is indeed possible to have both public safety and personal privacy. We can and must have both effective law enforcement and rigorous privacy protections.*
8. *Close attention must be paid to the privacy impact of new technologies, business practices, and police tactics if we are to continue to ensure strong, principle-based privacy protections.*
9. *Surveillance practices that intrude upon privacy by leveraging new technological platforms or transmission processes must be scrutinized to ensure that they are accompanied by sufficiently rigorous privacy and accountability protections.*
10. *Eternal vigilance will be required to secure our fundamental rights, including the right to personal privacy in relation to all public spaces, including those found online and in other virtual spaces.*

recognition systems, video surveillance cameras and CCTV, geolocational tracking, and drone-based surveillance. The approach outlined here builds on the constitutionally appropriate regulatory framework required to secure our right to privacy and provide for effective law enforcement. It does so by combining a *Privacy by Design* approach with a modern appreciation of our right to informational privacy.

Automatic Licence Plate Recognition Systems

Automatic Licence Plate Recognition ("ALPR") technology is used to take digital pictures of vehicle licence plates in order to recognize and record vehicle licence plate numbers. It employs optical licence plate detection software to seek out and recognize the presence of licence plates in view of an ALPR camera. Once an ALPR system recognizes the presence of a licence plate, the plate number is automatically extracted, at which point it can be recorded. ALPR systems can also leverage GPS technology to record the date and time, as well as relative location of all recorded images.

While ALPR systems generally do not film vehicle occupants — their focus is on the licence plates of vehicles — associated cameras could be configured to capture images of all drivers and passengers, as well as vehicle licence plates. ALPR systems — whether they are focused on licence plates or enhanced to create a more detailed record of a vehicle and its occupants — may be deployed openly from a stationary platform such as a pole, or mounted on a vehicle such as a marked police cruiser. Nonetheless, in many circumstances, they may operate in an opaque manner that may go unnoticed by much of the affected public.[56]

In Ontario, basic ALPR systems are currently being used for valid law enforcement purposes — in particular, those related to road safety. However, the use of enhanced ALPR systems to maintain a detailed accounting of every licensed vehicle that passes along a stretch of road, clears a check-point or enters into a park, town or city, 24 hours a day, seven days a week, would obviously have grave implications for privacy. So too could their use to track and monitor the comings and goings of political activists or anyone on a vaguely-defined "person of interest" watch list. Such surveillance could intrude upon a reasonable expectation of privacy — even if it were not conducted surreptitiously.

At the same time, a proactive, positive-sum approach allows for the accountable, limited, and justifiable deployment of an ALPR system. In taking this approach, we can avoid unnecessary trade-offs and demonstrate that it is indeed possible to have both public safety and personal privacy on public roads.

In this context, it is significant to note that driving is a regulated activity and some surveillance and supervision of vehicles and their drivers is expected. Surveillance of drivers, however, must be reasonable. As discussed above, Canadians have a legally-recognized "privacy interest in automobile travel" and the use of surveillance technologies in public spaces may violate section 8 of the *Charter*.[57] In this regard, police roadside and highway operations may interfere with

the "fundamental right to move about in the community."[58] As such, they must be designed and operated in a manner consistent with legislation, the common law, and the *Charter*.

Even if ALPR surveillance only results in roadside stops in a small percentage of cases, the system effects a digital identity check of drivers and their vehicles, typically for the purpose of identifying whom to stop or subject to further surveillance. *FIPPA*, which sets out rules governing the collection, use, and disclosure of *personal information* by government institutions in Ontario, permits the police to collect personal information where it is to be "used for the purposes of law enforcement."[59] Section 2 of *FIPPA* defines *personal information* as "recorded information about an identifiable individual" and "law enforcement" to include "policing."[60] Consistent with the overarching legal framework, our office has determined that the words *used for the purposes of law enforcement* require a policing institution to demonstrate that a collection of *personal information* is to be used by police acting within the scope of their law enforcement powers.[61] And, as indicated, in Ontario, ALPR systems are currently being used for valid law enforcement purposes.

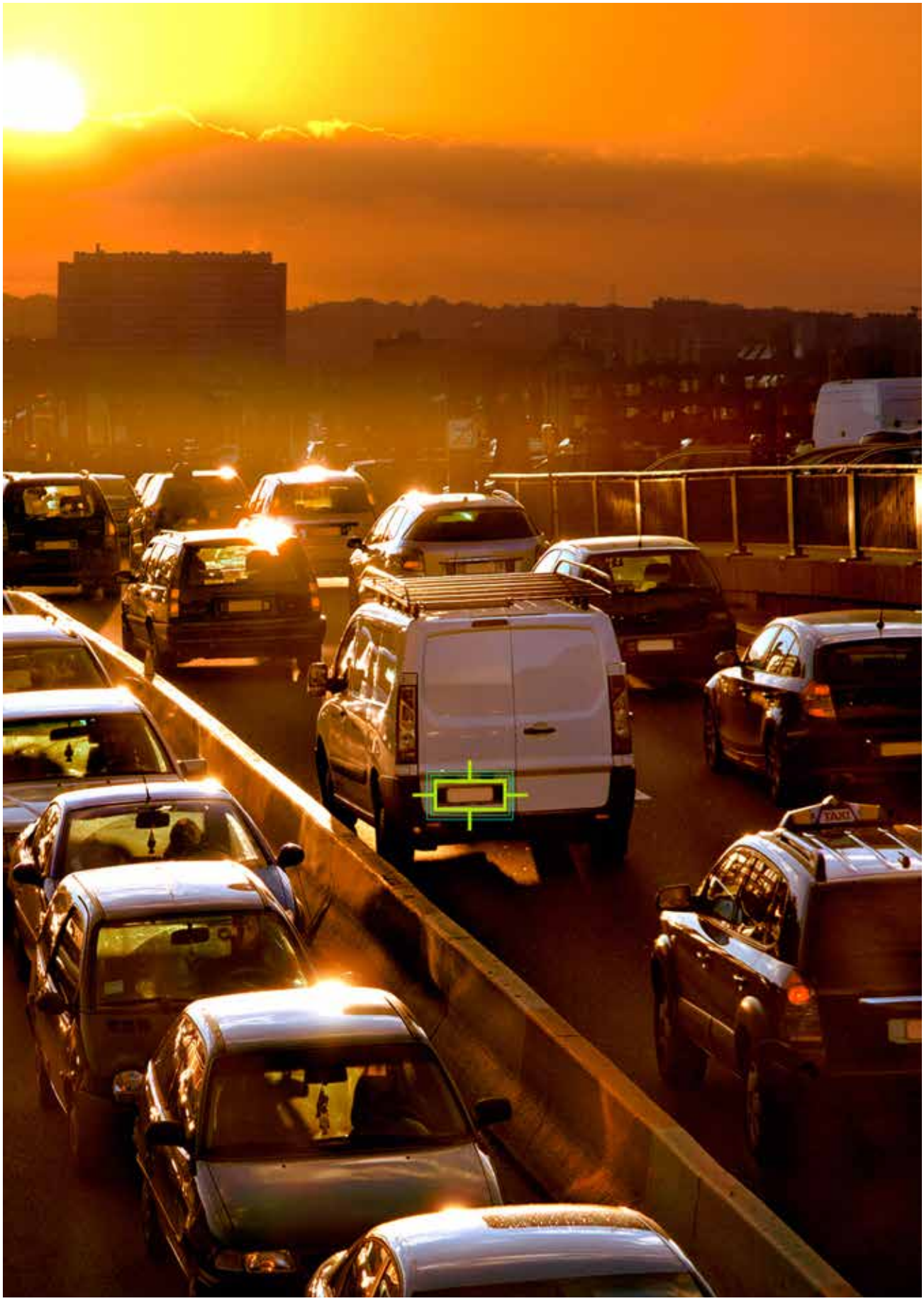
In this context, we note that, in considering the scope of law enforcement powers at the roadside and in highway operations, the Courts have consistently determined that the powers granted to the police for the purpose of enforcing the highway traffic laws, while significant, are nonetheless limited. For example, in 1992, the Supreme Court of Canada held that:

> [Highway safety] programs are justified as a means aimed at reducing the terrible toll of death and injury so often occasioned by impaired drivers or by dangerous vehicles. The primary aim of the [roadside stop] program is thus to check for sobriety, licences, ownership, insurance and the mechanical fitness of cars. The police use of check stops should not be extended beyond those aims. Random stop programs must not be turned into a means of conducting either an unfounded general inquisition or an unreasonable search.[62]

While a legitimate police interest beyond highway safety concerns need not taint the lawfulness of an otherwise valid exercise of a police power, road and highway safety concerns do "not provide the police with a means to pursue objects which are themselves an abuse of the police power or otherwise improper."[63] In this context, the Supreme Court of Canada has observed that a random stop program "designed as a 'comprehensive check for criminal activity' … was … fatally flawed from the outset."[64]

To date, ALPR surveillance systems have been used by Canadian police for purposes such as recovering stolen vehicles and licence plates, enforcing rules prohibiting driving under a suspended licence, and identifying "persons of interest" to law enforcement. Licence plate information collected by police-operated ALPR systems is recorded and compared against other information retained in police databases.

Concerned Privacy Commissioners have conducted investigations and reviews and engaged in consultations with police about their use of ALPR systems. To their credit, the police have responded by indicating their commitment to comply with Commissioner recommendations. As a result, we understand that ALPR systems are now generally only being used by police to vet vehicles against defined and appropriate *hit-lists* without retaining any data on law-abiding, *non-hit* vehicles or their occupants.


TAXI

Getting to this point has taken a positive, collaborative, but vigilant approach. Over the course of the last 10 years, the Privacy Commissioner of Canada, as well as the Information and Privacy Commissioners of British Columbia and Ontario have cautioned that, without significant controls, ALPR systems are capable of subjecting law-abiding Canadians to excessive and improper surveillance.

Beginning in 2003, our office accepted the use of mobile ALPR systems for valid law enforcement purposes (such as the location and retrieval of stolen vehicles), but cautioned against their use to continuously track and record the movements of law abiding citizens. In the intervening years, we have worked with the Ontario Provincial Police (OPP) to ensure that the personal information of law-abiding drivers — *non-hit* data — is deleted immediately after the ALPR system determines that there is no match with data on a properly-controlled highway safety-related *hit-list*. Similarly, the Privacy Commissioner of Canada has vigorously engaged the Royal Canadian Mounted Police (RCMP) over their retention of *non-hit* information, describing their initial practices as "ubiquitous surveillance of law-abiding Canadians who had committed no infraction." In 2012, she reported that "the RCMP agreed to stop retaining the *no-hit* information for the present."[65]

At the end of 2012, the Information and Privacy Commissioner of British Columbia wisely determined that "collecting personal information for law enforcement purposes does not extend to retaining information on the suspicionless activities of citizens, just in case it may be useful in the future."[66] In addition to recommending that police delete *non-hit* data immediately after the system determines that it is not a match to licence plates linked to an RCMP alert list, she recommended that the police limit their collection to reducing auto theft and motor vehicle violations. She also recommended that the municipal police work with the RCMP to amend their alert list to restrict it to addressing unlicensed drivers, driver-related court orders, and stolen vehicles.[67]

Bearing in mind the restrictions and recommendations described above, and applying our principled framework to law enforcement's use of ALPR systems, leads us to the following conclusions about the deployment of ALPR systems.

ALPR surveillance practices that intrude on privacy by leveraging new technologies must come with rigorous privacy and accountability protections. With those privacy requirements built into the technological, administrative, and legal controls, the public can be satisfied that the fair and efficient enforcement of highway safety is accomplished in a positive-sum manner.

In this regard, the deployment of ALPR systems should be restricted to circumstances where its use is necessary to meet legitimate social objectives, such as the identification of stolen vehicles or suspended drivers on a properly controlled *hit-list*. The resulting data collection should be subject to strict controls to limit the retention and subsequent use and disclosure of any personal information of law-abiding Canadians. *Non-hit* data should be deleted and destroyed immediately after the system has determined that it does not match the data on the *hit-list*.

Recalling that ALPR systems may operate in a manner that may frequently go unnoticed by much of the affected public, police services should provide the public with annual reports on their use of ALPR surveillance. In order to ensure that law enforcement remains transparent and accountable for its use of ALPR systems, such reports could, for example, provide:

- A detailed description of the times and locations at which ALPR surveillance is used;
- The purposes for which it is used;
- Whether it is deployed in a covert, overt, or opaque manner;
- How the applicable highway safety-related *hit-lists* are defined;
- How many *hits* are recorded; and
- The number of *non-hits* that are observed.

Each report could also:

- Include a declaration confirming that all *non-hits* were purged, deleted, or destroyed immediately after the system determined that they did not match data on the applicable *hit-list*(*s*) and that they were purged, deleted, or destroyed in such a manner that the *non-hit* data cannot be reconstructed;
- Indicate how many ALPR deployments have occurred that, for operational reasons associated with the need to protect the integrity of ongoing police investigations, cannot be described in detail in the report; and
- In the event that any *non-hit* data has been preserved, list the number of instances where such data has been retained, and the length, purpose, and justification for its retention.

Finally, we must not lose sight of the issue of ALPR systems being used surreptitiously or covertly. In our view, the authority to employ a covert ALPR surveillance system should be restricted to the police. In addition, the police power to deploy ALPR surveillance surreptitiously or for purposes other than those related to highway safety — such as to monitor the comings and goings of a suspect or person of interest — should be carefully supervised under a system of prior judicial authorization. Even where a genuine emergency makes it impracticable for the police to obtain judicial authorization before they employ such surveillance, the state can and must remain transparent and accountable for its use of such powers through subsequent timely, exacting, and independent scrutiny of their use — facilitated, for example, by notification and reporting requirements.

Video Surveillance and CCTV Cameras

Historically, pervasive video surveillance has posed a threat to privacy and our constitutional rights. When controlled by government departments, video surveillance can provide the government with massive amounts of personal information about the activities of law-abiding citizens, simply going about their daily lives. When individuals know they are being watched, this may have a chilling effect on their freedom to speak, act, and associate with others. Since individuals may censor their own activities when they are aware of being watched, video surveillance may also be perceived as a means of enforcing social conformity.

Privacy and the right of individuals to go about their daily activities in an anonymous fashion not only protects freedom of expression and association, but also protects individuals from intrusions into their daily lives by the government. Accordingly, when government organizations wish to use surveillance technology in a manner that will impact the privacy of all citizens, there must be clear justification for doing so. Specifically, the benefits of the technology should justify any invasion of privacy.[68]

The appropriate deployment of video surveillance can also provide significant benefits. In the aftermath of the April 2013 acts of terrorism in Boston and the alleged terrorist plot to bomb a VIA Rail passenger train travelling between Toronto and New York, it is not surprising that many have urged the deployment of increased video surveillance, including in public spaces, with CCTV cameras controlled by the police. As stated at the outset, however, the need for security must not come at the expense of privacy. Instead, we must consider achieving both goals — privacy **and** security.

With respect to surreptitious video surveillance, recall that, in Canada, the police use of any device or investigative technique, including a television camera or similar electronic device, generally

requires prior judicial authorization wherever its use would intrude upon a person's reasonable expectation of privacy.

As Justice La Forest observed in an opinion he provided to the Privacy Commissioner of Canada regarding public space video surveillance in 2002:

> [S]ome may be tempted to conclude that there can be no reasonable expectation of privacy in what is by definition public space.
>
> Such a conclusion, however, would be far too facile. Section 8 protects personal privacy in a host of situations. It does not demarcate rigid, formalistic borders between private and public spatial domains. As I stated for the Court in *R. v. Dyment*, "the spirit of s. 8 must not be constrained by narrow legalistic classifications." Determining whether individuals have a reasonable expectation of privacy in a given context is a nuanced, contextual, and fundamentally normative enterprise. As Justice Dickson held in *Hunter*, in each case "an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement." This assessment must be made in the light of all the circumstances.[69]

Decisions dealing with public space video surveillance illustrate that we have a reasonable expectation of privacy in the confines of a public washroom cubicle. As one Ontario Court judge expressed it in 1995, "it would be difficult ... to find many 'public' places where there is more 'reason' for an 'expectation of privacy' than in the closed cubicle of a public washroom."[70]

A 2010 decision of the British Columbia Supreme Court dealing with the criminal prohibition against making a voyeuristic visual recording of a person in circumstances that give rise to a reasonable expectation of privacy indicates that we "maintain a reasonable expectation of some privacy" in public settings such as a park:

> One can conceive of many examples where a person, sitting in a park, has his or her privacy interests interfered with. A person, sitting on a park bench, who reads or writes in her diary does not reasonably anticipate that someone may, with a telephoto lens, be reading that diary. A person sitting on a park bench with a friend does not expect that their conversation may be overheard and recorded with sophisticated eavesdropping equipment. A woman who lies on a blanket in a park does not anticipate a person can, with a telephoto lens, peer up her skirt.
>
> In each of these cases, though the person in question sits or lies in a public setting, they continue to maintain a reasonable expectation of some privacy. The person's expectation is certainly lower and different than if they were in their own home, but it nevertheless exists and can be violated.[71]

In this case, the Court concluded that we have a reasonable expectation that — while we may be observed by others or incidentally captured in a third party's photograph or video — we will not be surreptitiously filmed with the zoom feature of a camera, particularly for a voyeuristic purpose. In reaching this conclusion, the Court was mindful of "the quality and nature of the information or interest at issue" and that:

> … the use of technology can transform what is reasonably expected and intended to be a private setting into something that is completely different [and that] through the use of technology [it is possible] to not only see or hear more acutely but to create a recording and to capture and preserve an image or communication.[72]

In reaching these conclusions, the British Columbia Supreme Court commented on an observation made by Justice Binnie in *R. v. Tessling*. Drawing on a number of Supreme Court of Canada decisions dealing with physical rather than technology-driven searches, in *Tessling*, Justice Binnie observed that "it is true that a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place."[73] This is a form of "risk analysis" (e.g., that when we are in public, we take the risk of being exposed). Taking note of other Supreme Court decisions dealing directly with electronic surveillance in which the Court clearly rejected the application of such a risk analysis, the British Columbia Supreme Court ruled that "the suggestion that because a person is in a location which is ostensibly public they can no longer continue to have any reasonable expectation of relative privacy is not tenable. … [T]he assessment and interpretations of privacy expectations must keep pace with technological developments. The failure to do so would lead to the inevitable erosion of [the] normative standards that are central to reasonable privacy expectations."[74]

Of course, surreptitious public space surveillance by law enforcement brings additional considerations to bear and the case law reflects this. Courts have determined, for example, that law enforcement may,

in the course of conducting an investigation, take pictures and videos of people at a shopping complex or walking from their front door to their garage from a publicly accessible adjacent roadway.[75] As Justice La Forest put it in 2002:

> We cannot reasonably expect the police to refrain from observing or overhearing persons they consider to be suspicious. To require the police to have cause or obtain authorization for such surveillance would unjustifiably limit their ability to investigate and prevent crime. Indeed, it may be permissible for the police to use a video camera to observe and record a particular suspect's movements in public spaces. For this type of targeted surveillance, the relatively minor intrusion into privacy may possibly be balanced by the state's interest in effective law enforcement.

In contrast, Justice La Forest then observed that "comprehensive and continuous video surveillance is a very different matter:"

> It permits the police to systematically observe, often at high resolution and across a broad spatial expanse, everyone present within the camera's or cameras' range. This type of video surveillance is equivalent to having individual police officers closely follow, 24 hours a day, every person within a certain geographical space. That would be a police state, not a free society. We may not have a reasonable expectation that the police will never observe our activities in public spaces, either incidentally or as part of a targeted investigation. But surely it is reasonable to expect that they will not always do so.

We agree. In our view, unfettered law enforcement use of, or access to, video surveillance technologies that are capable of facilitating indiscriminate monitoring, particularly where that monitoring may be close and continuous, is likely to intrude upon our right to a reasonable expectation of privacy, whether those technologies are employed overtly or covertly. In light of the expanding use of video surveillance technologies, not to mention the increasing sophistication of sensoring devices, biometrics, and facial recognition systems, the future of privacy may well lie in ensuring that the necessary protections are built right into the design of surveillance systems.

With respect to covert video surveillance, recall that, in Canada, the police use of any device or investigative technique, including a television camera or similar electronic device, generally requires prior judicial authorization whenever its use would intrude on a person's reasonable expectation of privacy. How are we to ensure a constitutionally appropriate regulatory framework with respect to overt video surveillance?

Fortunately, we grappled with this issue first-hand in 2007 during our mass transit system investigation concerning the use of video surveillance cameras by the Toronto Transit Commission (TTC) in buses, streetcars, and subways, as well as on subway platforms and other transit property.[76] Our investigation report (the "*TTC Report*") brought to the fore questions about personal privacy in public spaces. In public spaces, law-abiding people may be visible and audible to others,[77] but they should reasonably expect that they will generally be able to go about their lives without being tracked and identified.

Video surveillance is often implemented in public spaces because of an expectation that it will deter crime. Aside from research suggesting that some video surveillance may deter crimes like

car theft in "hot spots," this does not appear to be supported by the research.[78] However, as was demonstrated in Boston, cameras — including privately owned and operated cameras — can serve as an effective tool in the detection, arrest, and prosecution of offenders. When an incident occurs in the presence of video surveillance cameras, the authorities can respond quickly and appropriately. In this context, the value of surveillance technologies to law enforcement appears to be clear. At the same time, given its inherently invasive nature, privacy must be considered right from the outset, wherever and whenever surveillance technologies are contemplated.

While there is "evidence to suggest that the general public recognizes that video surveillance may be justifiable in certain high risk locations,"[79] the public may be significantly less tolerant of more widespread surveillance — for example, on residential streets — or of routine, active, real-time monitoring. In addition, the public may not view a *degree* of video surveillance as unreasonable if the resulting video recordings are routinely destroyed, in a reasonably short time frame. At the same time, all legal privacy requirements must be met.

In this context, in Ontario, the state must be able to demonstrate that the collection of personal information is in accordance with the statutory privacy rules in *FIPPA* and *MFIPPA*. In general terms, the collection should be restricted to that which is reasonably necessary to meet legitimate societal objectives, and subjected to controls over retention and subsequent use and disclosure. The state should also be open and accountable for its information-handling practices.

It follows that, even where the deployment of video surveillance cameras is justified — for example, for compelling safety and security purposes, law-abiding individuals are still entitled to the privacy afforded by the ability to merge into the "situational landscape." Accordingly, necessary public spaces video surveillance must be restricted to ensure that:

- Personal information will only be collected for legitimate, limited, and specific purposes;
- The collection of personal information will be limited to the minimum amount necessary for the specified purpose(s);
- Personal information will only be used and disclosed for the purpose(s) specified; and
- Personal information will be deleted pursuant to precise and appropriately limited retention schedules and in such a manner that the personal information cannot be reconstructed.

With respect to the TTC — having found that its video surveillance program was justified — our report rejected a "privacy versus security" paradigm in favour of a positive-sum, *Privacy by Design* model. Under this model, privacy and security coexist through the use of Privacy-Enhancing Technologies (PETs) and strong procedural controls.

PETs refer to information and communications technologies that incorporate measures to protect privacy by eliminating or minimizing the collection, retention, use, and disclosure of personal information. This is often referred to as "data minimization," and increasingly represents a vital component of privacy protection. An example of a PET described in the *TTC Report* is object-based encryption that can be used to obscure the images of individuals captured by video surveillance. Where an incident takes place requiring further investigation, the images may be decrypted, but only by authorized parties. When deployed successfully, this technology reduces the risk of

random, invasive, and unlawful surveillance of individuals, while permitting the use of images for legitimate safety and security purposes — a doubly-enabling, positive-sum solution.

Beyond the effective implementation of PETs, *Privacy by Design* calls for privacy to be built proactively into an organization's information practices, by default. In the *TTC Report*, we recommended that, among other things, the TTC:

- Install accessible signage providing clear notice of collection to all passengers;
- Require all employees accessing or using the video surveillance system to sign a written agreement with the TTC regarding their duties and obligations in respect of video surveillance, including a strong undertaking of confidentiality;
- Retain *used* surveillance images (i.e., those viewed for incident-driven, law enforcement purposes) for a maximum of one year;
- Only retain *unused* images for a maximum of 72 hours (with surface vehicles — buses, streetcars — overwriting unused footage every 15 hours);
- Keep abreast of research on emerging PETs and adopt these technologies, whenever possible;
- Implement a two-signature sign-off protocol for police requests for incident-driven remote access to images recorded by the TTC surveillance system, with the Police Chief or his designate being the second sign-off; and
- Undertake comprehensive privacy audits on an annual basis.

Consistent with the TTC's policy of limiting law enforcement access to recorded images to the investigation of specific incidents, the two-signature sign-off protocol is critical to ensuring that privacy is strongly protected when providing the police with remote access to captured information for law enforcement purposes. The TTC provided a copy of a Memorandum of Understanding between the TTC and the Toronto Police Services Board (TPSB) addressing the police's remote access to and use of recorded images from TTC surveillance cameras. Incident-driven remote access would take place from a computer, located within police headquarters, connected to the TTC's surveillance system through a fibre-optic cable. To ensure proper oversight of remote access, the TTC and TPSB agreed on a double sign-off request protocol. This protocol requires that any requests from the police to the TTC for access to images captured by video surveillance be signed off both by the police officer requesting access, and by the Chief of Police, or his or her designate. This additional protection against any unauthorized access to and use of surveillance images is an excellent example of *Privacy by Design* in action, and has been working very effectively since being put into place.

The recommendations in the *TTC Report*, as well as in our *Guidelines for the Use of Video Surveillance Cameras in Public Places* (the *Guidelines*), still resonate today.[80] Once an appropriate decision has been made to deploy an overt video surveillance system, a *Privacy by Design* approach will ensure that surveillance is implemented in a privacy-protective manner that meets multiple legitimate needs — a positive-sum approach.

The application of *Privacy by Design* to surveillance technologies is not confined to video surveillance in mass transit systems. *Privacy by Design* principles may be applied to virtually any surveillance technology in a positive-sum manner, to achieve both the protection of privacy and the security of the public. We know that video surveillance technologies present a particular challenge for privacy due to their extraordinary potential for data capture and retention. Recent events serve to remind us that there are legitimate uses for some degree of surveillance in high-risk locations. The challenge is to rein in, as tightly as possible, any potential surveillance-driven erosion of privacy. We can do this by ensuring that strong controls are in place, through the implementation of appropriate legal rules and administrative policies and procedures, the use of independent audits and other measures to ensure strong oversight and accountability, and the continued development and implementation of innovative PETs to preserve privacy, while effectively providing security in public spaces.

Geolocational Tracking

Every day, millions of people move about while making use of location-enabled portable computing devices and services. Many of us are inseparable from our cellphones, smartphones, and other mobile devices and enjoy their associated location-related functionalities. More and more of our cars and trucks feature GPS-assisted mapping and roadside assistance services. However, these enormously useful tools come with a downside — they allow our movements and activities to be tracked. Indeed, this surreptitious technology is sophisticated enough in its current form to be configured to "track our every movement for indefinite periods … without visual surveillance."[81]

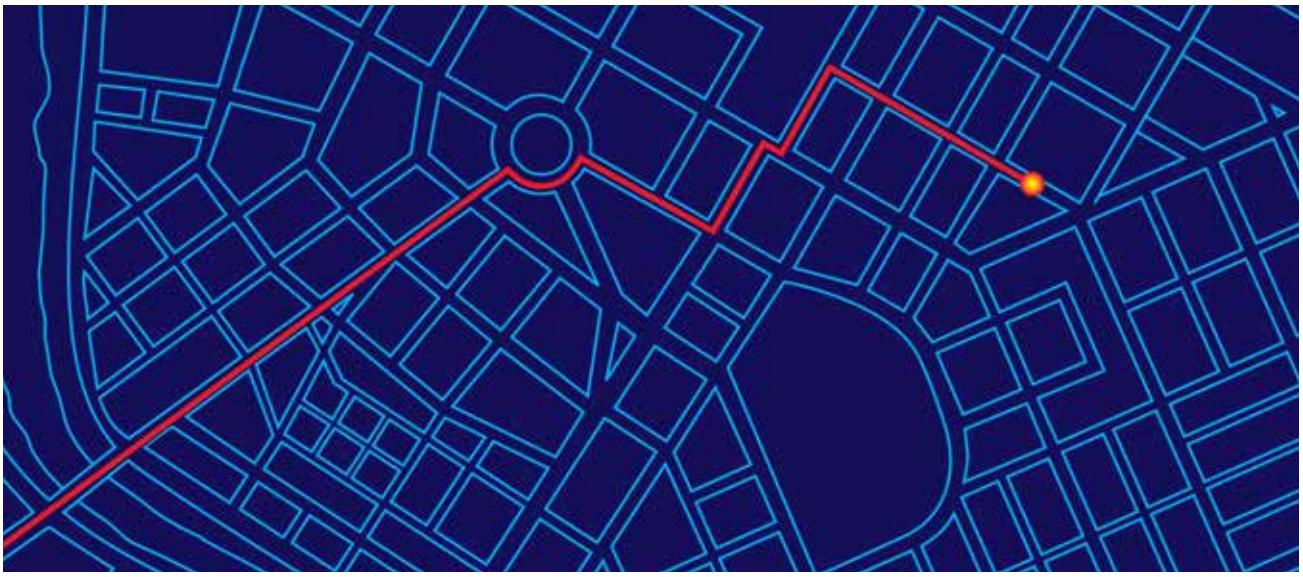
Geolocational monitoring by the state may sometimes involve a police officer having to physically install a GPS tracking device on, for example, a person's vehicle. Alternatively, this functionality can be activated remotely — for example, on a GPS-enabled device already in the possession of a person of interest. Such remote activation may require the cooperation of a third party such as a communications service provider. Geolocational tracking may also be effected by the police deploying a "stingray" (or "IMSI catcher") to trick nearby mobile phones and other wireless communications devices into connecting to the surveillance device rather than a legitimate communications tower. When devices unwittingly connect to the police, the stingray can see and record their unique device ID numbers and traffic data, as well as information that points to their precise location.

Close attention to the technical capacities and potential uses and abuses of this technology tells us that such monitoring is a form of intrusive surveillance that should generally require supervision under a system of prior judicial authorization. After all, geolocational tracking allows for close and continuous surveillance. The privacy implications of GPS-facilitated locational monitoring were described by U.S. Supreme Court Justices Sotomayor and Alito in *U.S. v. Jones*. Justice Sotomayor focused on the wealth of information collected through even short-term use of this powerful tracking technology:

> GPS monitoring generates a precise comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations … "Disclosed in GPS data … will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrists, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and so on." The Government can store such records and efficiently mine them for information for years into the future. … And because GPS monitoring is cheap in comparison to conventional surveillance techniques and by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility."[82]

Justice Alito expanded on the implications for future police practices, pointing to the possibility of more frequent resort to the use of such sophisticated and intrusive GPS surveillance in a wider array of investigations:

> The surveillance at issue in this case — constant monitoring of the location of a vehicle for four weeks — would have required a large team of agents, multiple vehicles, and perhaps aerial



> assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.[83]

In view of the facts of the case before it, however, and out of respect for the limited role assigned to the judiciary in a democracy, the majority of the U.S. Supreme Court was only prepared to declare that the Fourth Amendment requires a probable cause warrant where police installation of a GPS tracking device involves a trespass on a suspect's property. Other "vexing problems," the majority said, should be left to be resolved as future cases required.[84] At the same time, the Court appeared to appreciate that the regulation of this form of surveillance may properly move elected officials to enact a constitutionally appropriate regulatory framework.[85] Such legislative protections may be necessary to ensure the protection of privacy and freedom. As Justice Sotomayor expressed it, "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse [and] may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[86]

As indicated above, the use of a tracking device has long required a warrant in Canada. To obtain permission to install, maintain, and use a tracking device on anything, including a thing carried, used, or worn by a person, the police must first satisfy a justice of the peace or judge that there are reasonable grounds to *suspect* an offence has been or will be committed and the tracking device will provide relevant information about that offence. The terms of the relevant *Criminal Code* provision, section 492.1, would appear to capture GPS or any other electronic monitoring of the location of a person's mobile device or vehicle, whether that monitoring is activated remotely or first requires that the authorities gain physical access to a person's cellphone or car. However, in addition to incorporating a lower suspicion-based rather than belief-based threshold, the warrant regime does not require notice to individuals that they have been subject to tracking, or reports to Parliament on how frequently and in what circumstances such tracking is conducted. The same shortcomings apply with respect to section 487.11, the *Criminal Code* provision for warrantless use of a tracking device in exigent circumstances — it too lacks notice and reporting safeguards.

We believe that a positive-sum regulatory framework governing electronic locational surveillance must allow for some necessary electronic locational surveillance, while securing our right to privacy. It must ensure that a warrant is generally required, irrespective of how that surveillance is activated (e.g., *via* a trespass or remotely) or whether, in any particular case, it is used for brief periods or in a prolonged or continuous sweep. In addition, it must also provide for much greater transparency and accountability. In other words, it must also provide for appropriate post-use notice to those targeted for tracking. As the Supreme Court of Canada recognized in *R. v. Tse*, such privacy protections would not impact the ability of the police to investigate offences or "act in emergencies." It would, however, "enhance the ability of targeted individuals to identify and challenge invasions to their privacy and seek meaningful remedies."[87]

In view of the foregoing, legislative changes appear to be required in Canada (as well as in the U.S.) to ensure proper supervision and accountability in the use of this sophisticated form of surveillance technology. Recalling the principles that guide our review of law enforcement uses of new surveillance technologies, it is our view that, in addition to the existing warrant requirement, the authority to employ geolocational tracking should generally be restricted to limited classes of state actors such as police officers. Moreover, in order to ensure that law enforcement remains transparent and accountable for its use, police services should, as a matter of routine, provide the public with periodic reports on their use of geolocational tracking. Finally, and, as indicated, the authorities should provide appropriate notice to those targeted for geolocational tracking.

DRONES: Drone-based Surveillance

The word "surveillance" comes from the French word for "watching over." "Sur" means "from above" and "veiller" means "to watch." In this context, it is easy to appreciate that drone technology represents the "cold technological embodiment of observation."[88]

Drones, also referred to as remotely piloted aircraft (RPAs) and unmanned aerial vehicles (UAVs), present unique privacy challenges, due to their ability to carry a variety of sensors and to gather information from virtually any vantage point — often for long periods, and on a continuous and covert basis. Regarded as effective, low-cost alternatives to manned aircraft, drones can also sustain a greater amount of G-force, allowing for more complex flight manoeuvring. Indeed, improvements in navigation and sensor technology have made drones more reliable in terms of flight control, while advanced telecommunications technologies permit control at high altitudes, over considerable distances.[89]

Drones have attracted enormous controversy for their deadly use by the Central Intelligence Agency and the U.S. military in Pakistan, Afghanistan, and other countries. Meanwhile, in February 2013, U.S. President Barack Obama signed the *FAA Modernization and Reform Act* into law. The *Act* explicitly allows the Federal Aviation Administration (FAA) to permit the domestic use of unarmed drones, but fails to address the privacy of Americans. Transport Canada has been issuing Special Flight Operation Certificates allowing the use of drones in Canada since 2007.

Of course, drones may be deployed in a myriad of contexts, for a wide range of purposes. And, like so many technologies, drone-based surveillance can be properly deployed to provide enormous benefits. Drones may assist with fighting fires and protecting remote critical infrastructure like hydroelectric lines and oil and gas pipelines. They may also be used by law enforcement agencies in search and rescue operations, at hostage-taking incidents and other emergencies, and to document crime scenes and accidents. But drones may also be used to record people's lawful participation in events such as political protests, as well as to conduct sustained, intrusive, and surreptitious surveillance of persons of interest.

Indeed, in the hands of law enforcement, drones may be equipped with sophisticated zoom cameras, infrared thermal imagers, radar, location-based tracking tools, communication interception and listening devices, and other surveillance technologies that can record and transmit digital data to ground control systems. These technologies have become cheaper and more sophisticated, allowing data capture at greater distances, with greater resolution and granularity. Advanced video analytics can apply artificial intelligence to collecting and processing considerable amounts of video data. When combined with facial recognition software, this could be used to continuously track individuals in public, as well as in private spaces (e.g., through windows or perhaps even walls). Moreover, since they can provide effective aerial surveillance at a fraction of the cost of manned vehicles such as helicopters, it follows that drones could also facilitate a substantial increase in intrusive surveillance.

Meanwhile, the use of drones is expected to rise. In the U.S., the FAA has issued 1,428 licences to police, universities, and federal agencies between 2007 and the beginning of 2013. Of these, 327 were still listed as active in February 2013.[90] The FAA has estimated that as many as 30,000 drones could be in use domestically in the U.S. by 2020, spurred on by the Department of Homeland

Security and other government agencies. That estimate includes commercial and government drones, but not private drone hobbyists or the peeping Toms already popping up in media reports. For example, on May 29th, 2013, it was reported that, earlier that month, a Seattle woman looked out of her upper-floor window to find an aerial drone hovering outside! "On the sidewalk next to her house ... she found the man operating the drone [who] claimed that he was doing research and that what he was doing was 'perfectly legal.'"[91] Whatever the purported justification for this kind of intrusive activity, it should not go unregulated because it was on public property. Whether acting on their own behalf, or on behalf of the state, citizens' privacy must be protected.

In addition, the FAA recently announced that it has "achieved the first milestone included in the 2012 FAA reauthorization — streamlining the process for public agencies to safely fly [drones] in the nation's airspace," by: (i) developing "an automated, web-based process to streamline" the authorization process; (ii) creating "expedited procedures ... to grant one-time [authorizations] for time-sensitive emergency missions such as disaster relief and humanitarian efforts;" and (iii) "[c] hanging the length of authorization[s] from the current 12-month period to 24 months."[92]

The FAA is now working to select six drone test sites. Drone testing, however, will be focused on ensuring that drones do not "collide with planes or endanger people or property on the ground." And, while the FAA has announced a public consultation directed at protecting privacy interests associated with test site operations, the chief of the FAA's Unmanned Aircraft Systems Integration Office has acknowledged that "the FAA has no authority to make rules or enforce any rules relative to privacy."[93] That responsibility appears to lie primarily with Legislators and the Courts.

Between January 2007 and January 2012, Transport Canada issued 293 Special Flight Operation Certificates for drone operations. These certificates do not address privacy. The "ultimate goal" of Transport Canada's UAV program is stated as being "to 'normalize' UAV operations within civil airspace, [but] the industry technology is not mature enough, and the regulatory structure is not in place, to support routine operations."[94] In our view, the challenges are, however, not limited to

immature collision avoidance systems for drones operating beyond the visual range of their human pilots — privacy issues must also be addressed, directly and explicitly.

Legislation to provide for a constitutionally appropriate regulatory framework for the domestic use of aerial drones is moving ahead — in the U.S. Faced with mounting privacy-related concerns from American citizens, we are delighted to see lawmakers at the municipal, state, and federal levels taking a proactive, privacy-protective stance. In this context, it should come as no surprise that as of May 28th, 2013:

- Cities and towns such as Charlottesville, Virginia, St. Bonifacius, Minnesota, and Seattle, Washington have moved to restrict drone use in their communities;
- Twenty-eight state Legislators are actively considering passing drone legislation, most to require law enforcement to get a probable cause warrant before using a drone in an investigation;[95]
- Five states — Florida, Idaho, Montana, Tennessee, and Virginia — have already enacted laws restricting the use of drones by either imposing warrant requirements or moratoriums;[96]
- The Department of Homeland Security has set up a working group to study the impact of government UAVs on civil liberties and civil rights, as well as other legal and policy issues; and
- A comprehensive bipartisan drone bill was introduced before the U.S. House of Representatives in February by Ted Poe (R-Texas), Trey Gowdy (R-S.C.), and Zoe Lofgren (D-Calif.). Since referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, H.R. 637, the *Preserving American Privacy Act of 2013* (*PAPA*), would significantly restrict the use of drones. Like similar bills from the last session of Congress (where it was first introduced),[97] under *PAPA*, court authorization would be required for government and law enforcement drone-based surveillance, with exceptions for exigent circumstances, consent-based surveillance, and surveillance for the purpose of U.S. border control. *PAPA* would also prohibit the arming of drones and make the intentional *private* use of drone surveillance *unlawful* if it invades an individual's reasonable expectation of privacy in a "highly offensive" manner, regardless of whether there is any trespass.[98]

In contrast, it appears that, for the time being, Canadians may have to rely on the prudence of law enforcement and the oversight provided by Privacy Commissioners and the Courts. Canadian Legislators have yet to grapple *directly* with the emerging privacy issues associated with drone use. The reason may be that, thus far, the public perceives drones to be a largely American phenomenon. However, while they may not yet be in widespread use by police in Canada, the RCMP have a fleet of approximately 20 drones. Meanwhile, in Ontario, the OPP and the Halton Police Service are actively using drones. In addition to using them for purposes related to search and rescue operations, hostage-taking incidents, and other emergencies, as well as the documentation of crime scenes and accidents, the police appear to have used drones to investigate drug offences.[99]

In this context, it is time for a proactive public discussion of the issues. The key is to ensure that we receive the benefits associated with drone-based technologies, while continuing to provide strong

privacy protections, *including* in public spaces. Once more, we turn to the principles and lessons that emerged during the course of our retrospective. They will instruct us as to how to ensure a constitutionally appropriate regulatory framework with respect to drone-based surveillance.

And, once again, we recall that, in Canada, the police use of any device or investigative technique, including a television camera or similar electronic device, generally requires prior judicial authorization wherever its use would intrude on a person's reasonable expectation of privacy. Moreover, recalling our discussion of ground-based video surveillance, we join with our Canadian Courts in asserting that Canadians "maintain a reasonable expectation of some privacy" on public roads and other public settings such as parks, public squares, plazas, and playgrounds.

This conclusion is consistent with the weight of the case law dealing with manned aerial video surveillance by the police over occupied and unoccupied private land, as well as over Native reserves. As affirmed by Courts in New Brunswick,[100] Ontario,[101] Saskatchewan,[102] and British Columbia,[103] "an expectation of privacy, which society is prepared to recognize is reasonable, can exist in respect of unoccupied lands," as well as occupied lands, particularly with respect to individuals entitled to be present on those lands. This body of law tells us that even low-tech manned aerial surveillance of open private spaces generally requires a warrant, especially when that surveillance is conducted at low altitudes.[104]

In one of the two cases where a Provincial Court would have permitted warrantless aerial video surveillance of open spaces, the Supreme Court of Canada effectively set that finding aside, explicitly leaving the critical issue of the constitutionality of "open-space searches" to a more appropriate future case.[105] In the remaining case, the Court determined that the police may conduct some aerial surveillance from an airplane flying over adjacent private land at an altitude in excess of the minimum altitude for permissible aircraft flyovers (over 500 feet for rural areas, over 1,000 feet for built-up areas), where they used a commonly available zoom lens camera.[106]

In our view, an analysis that places too much emphasis on the altitude, angle, or availability of surveillance tools and tactics must be rejected. The key question is whether the surveillance provides a *close or penetrating gaze*. In this regard, we join with Justice Drapeau, writing for the Court of Appeal of New Brunswick, where he states that:

> For my part, I reject the suggestion that the application of s. 8 to [open spaces in an occupied residential lot] is contingent on the presence of view-proof walls or roofs. Such an approach would deny s. 8 rights to most open spaces in residential properties, and it would limit s. 8 rights to the few who can afford such privacy shields. As a rule, lawful occupants have an expectation of privacy in all open spaces within their residential lots that is qualitatively sufficient to invest them with s. 8 protection against unlawful aerial as well as terrestrial searches.[107]

As the Saskatchewan Court of Queen's Bench said in 2008, "there has been no determination by the Supreme Court of Canada regarding the right to privacy on open, privately owned land."[108] That remains the case to date. What of the Supreme Court of Canada's 2004 ruling in *R. v. Tessling*? In that decision, the Court determined that police did not need a warrant to conduct surveillance of the patterns of heat distribution on the external surfaces of a private residence from an airplane using an unsophisticated infrared radar camera (FLIR). In reaching this conclusion, the Court's focus

was squarely on "the quality of information that [*existing*] FLIR imaging can actually deliver."[109] The Court was careful to remind us that:

> If, as expected, the capability of FLIR *and other technologies* will improve and the nature and quality of the information hereafter changes, it will be a different case, and the courts will have to deal with its privacy implications at that time in light of the facts as they then exist.[110]

While the intrusiveness of a drone operation will depend on its surveillance 'payload,' as well as the circumstances, manner, and length of its deployment, it is self-evident that drone-facilitated surveillance has the capacity to facilitate close, continuous, and indiscriminate monitoring.

Bearing in mind our 2012 paper, *Privacy and Drones*, as well as the approach emerging out of U.S. Legislatures, we make the following further recommendations about the constitutionally appropriate governance of the state's use of drone-based surveillance.

As indicated throughout this paper, data-gathering by the state should be restricted to that which is reasonably necessary to meet legitimate social objectives, and subjected to controls over its retention and subsequent use and disclosure. The state should be open and accountable for its information-handling practices. Compliance with these rules and restrictions should be subject to independent scrutiny. In particular, we recommend that the authority to employ intrusive drone-based surveillance powers should generally be restricted to limited classes of state actors such as police officers. Barring any genuine urgencies, the police should secure a warrant before conducting any sophisticated drone-facilitated surveillance that targets one or more individuals, including people participating in political activities including speeches, demonstrations, picket lines or other forms of non-violent protests. The police should also be required to provide appropriate post-use notice to those targeted for any drone surveillance.

At the same time, not all drone-facilitated police surveillance will be intrusive of privacy interests. Like geological inspections or environmental surveys, police surveillance of a remote piece of

energy infrastructure will rarely intrude upon the privacy of any member of the general public. In such circumstances, a warrant may not be necessary. Of course, any personal information collected by law enforcement through such uses of drones will generally be governed by applicable privacy legislation and should not be used for secondary law enforcement purposes.[111]

Other law enforcement uses of drone-based surveillance in search and rescue operations, at hostage-taking incidents, and to document crime and accident scenes also call for a different approach. Drone use in geographically-confined, time-limited, emergency situations of these kinds may not require a warrant. However, to ensure that the state remains transparent and accountable, all drone use should be subject to additional restrictions, as well as subsequent, timely, and public scrutiny. In particular, the decision to deploy a drone should be made by a senior officer. In all cases, images of identifiable individuals captured by drone-based surveillance technologies should not be retained longer than one year following their collection — or shared with third parties at all — unless there is reasonable suspicion that the images contain evidence of criminal activity or are relevant to an ongoing investigation or pending criminal trial.

Moreover, clear written policies and procedures governing the use of aerial surveillance technologies should be adopted and made available to the public. To help ensure necessary transparency and accountability, law enforcement agencies should also be required to issue annual public reports on their use of drones. This will help both lawmakers and the public understand how drones work in practice. Such reports could, for example, indicate:

- The purpose for which drones have been used and the circumstances under which their use has been authorized, and by whom (i.e., a Court or a senior officer);
- The specific kinds of information that the drone(s) have collected about individuals;
- The length of time for which the information will be retained;
- The possible impact on individuals' fundamental rights including the right to privacy;
- The specific steps the police service takes to mitigate the impact on individuals' privacy, including protections against unauthorized use and disclosure; and
- An individual point of contact for citizen complaints and concerns.

Throughout, any move to regularize drone use — for example, within a municipality — should be preceded by a full public discussion. Consultations should be conducted with all relevant stakeholders to examine the necessity of any proposed drone program and the policies required for a justified and proportionate program that is acceptable to the public.

Finally, we must make a commitment to proactively embed privacy into the design of these new technologies. By adopting a *Privacy by Design* framework, we can limit the negative impacts that may otherwise be produced. The prospect of having our every move monitored, and possibly recorded, raises profound privacy and civil liberty concerns. We must avoid, as many privacy scholars and regulators have cautioned, "sleepwalking into a surveillance society."[112] Instead, we encourage law enforcement authorities to take a proactive *Privacy by Design* approach to developing and operating a drone program which truly respects privacy.

Privacy by Design principles should be adopted into all aspects of drone operations, particularly in any circumstances where personal information may be collected, retained, used, disclosed, and/or disposed of. Where possible, the collection of personally identifiable information should be

avoided. Drone operators should ensure that they are transparent with respect to any collection of personal information. In addition, consideration should be given to employing object-based encryption to obscure any images of individuals that are captured by drone-based surveillance. Under this approach, where an incident takes place requiring further investigation, the images may be decrypted, but only under the authority of two authorized officials. If deployed successfully, this technology could reduce the risk of random, invasive, and unlawful surveillance of individuals, while permitting the use of images for legitimate safety and security purposes. In addition, access to drone data recordings would be restricted to authorized personnel only. Logs would be kept of all instances of access to, and use of, recorded material, to enable a proper audit trail. Where records are maintained electronically, the logs should also be electronic. Such measures would ensure that the proposed design and operation of a drone system strictly limits privacy intrusions to those which are absolutely necessary to achieve required, lawful goals.

Conclusions

In a free and open society such as ours, privacy plays a critical role. It is a constitutional right "integral to an individual's relationship with the rest of society and the state."[113] Legislatures, Courts, and Privacy Commissioners continue to provide further instruction and guidance on how to protect this fundamental right. A *Privacy by Design* approach is central to designing a regulatory framework governing state surveillance, whether we are considering the use of video surveillance, an ALPR system, geolocational tracking, drones, or any other new surveillance technology.

Now more than ever, calls for increased public surveillance must be vigorously questioned. Technologies capable of facilitating broad programs of continuous and indiscriminate monitoring must be subject to strict controls. As Justice Ian Binnie stated in 2004:

> Efforts to counteract terrorism are likely to become part of our everyday existence for perhaps generations to come. … The danger in the "war on terrorism" lies not only in the actual damage the terrorists can do to us but what we can do to our own legal and political institutions by way of shock, anger, anticipation, opportunism or overreaction.[114]

The same cautions apply in respect of any proposal to obtain "a little temporary safety" at any cost. Excessive surveillance is anathema to freedom and liberty, and must thus be opposed.

In the words of Justice Binnie's colleagues, Justice Iacobucci and Justice Arbour, however, "we must not forget that the legislative and executive branches also desire, as democratic agents of the highest rank, to seek solutions and approaches that conform to fundamental rights and freedoms."[115] Fortunately, it is our experience that, where the use of a particular surveillance technology is justified, proportional, and effective at delivering public safety **and** privacy, a proactive, *win-win*, *positive-sum* approach is available that will ensure that privacy, accountability, and transparency are embedded into the legal and technical design specifications of any proposed surveillance system.

While eternal vigilance is required to secure our fundamental rights, including the right to personal privacy, we remain confident that we can have both public safety and personal privacy in public spaces. There is neither reason, nor need, to settle for anything less.

Endnotes

1 *R. v. Wise*, [1992] 1 S.C.R. 527 at para 82.

2 Phil Mattingly, "Boston Police Chief Urges Surveillance Increase After Attack," *Bloomberg*, (9 May 2013) online: <http://www.bloomberg.com/news/2013-05-09/boston-police-chief-urges-surveillance-increase-after-attack-1-.html>.

3 Richard A. Posner, "Privacy is Overrated," *New York Daily News*, (28 May 2013) online: <http://www.nydailynews.com/opinion/privacy-overrated-article-1.1328656> . See also Commissioner Ann Cavoukian Letter to the Editor, *New York Daily Times* (1 May 2013) online: <http://www.nydailynews.com/opinion/2-school-lunch-privacy-ed-article-1.1332648?pgno=1>.

4 Benjamin Franklin, *Memoirs of the Life and Writings of Benjamin Franklin* (London: Henry Colburn, 1818) at 270.

5 Danielle Citron and David Gray, "A Technology-Centered Approach to Quantitative Privacy," (14 August 2012) at 4. See also Danielle Citron and David Gray, "The Right to Quantitative Privacy" (2013) 98 *Minnesota Law Review* at 4.

6 *Supra* note 1.

7 *R. v. Tessling,* [2004] 3 S.C.R. 432.

8 An important means of achieving proper privacy is through the *Privacy by Design* (*PbD*) approach. *PbD*'s approach is to embed privacy in the design specifications of information technologies and systems, accountable business practices, and physical design and networked infrastructures, as the default, right from the outset. *PbD* principles accommodate all legitimate interests and objectives in a positive-sum, *win-win* manner. *PbD* avoids the pretense of false dichotomies, such as privacy versus security, demonstrating that it is possible, and far more desirable, to have both. *PbD* represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches after the fact. *PbD* requires an evolution in the way that private organizations and government institutions think about privacy — moving from a reactive mode to a proactive one. Similarly, enshrining a *PbD* approach in statutes, regulations, administrative codes, and best practices may require an evolution in how policy and lawmakers approach privacy rule-making. For example, surveillance-related rule-making should ensure that surveillance is accountable, limited, and transparent.

9 FIPs refers to the *Fair Information Practice Principles*, online: < http://www.priv.gc.ca/resource/tool-outil/english/fair-info-practices.asp>.

10 *R. v. Patrick*, [2009] 1 S.C.R. 579 at para 20. See also *R. v. A.M.*, [2008] 1 S.C.R. 569 at paras 35 and 36; *R. v. Dyment*, [1988] 2 S.C.R. 417 at pp. 427-428; and *H.J. Heinz of Canada Ltd. v. Canada* (*Attorney General*), [2006] 1 S.C.R. 441 at para 22.

11 *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403 at para 71, per La Forest J. dissenting in the result; and *Lavigne v. Canada (Commissioner of Official Languages)*, [2002] 2 S.C.R. 773 at paras 24-25.

12 *Supra* note 5 ("A Technology-Centered Approach to Quantitative Privacy") at 17.

13 Office of the Information and Privacy Commissioner of Ontario, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report — Privacy Investigation Report MC07-68* (3 March 2008) at 2.

14 *Hunter et al. v. Southam Inc.,* [1984] 2 S.C.R. 145.

15 *R. v. Ward* 2012 ONCA 660.

16 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11. ss. 8 and 24(1).

In the majority of section 8 cases, search and seizure issues arise in the context of criminal proceedings where the primary focus is on a specific factual context of a particular police investigation, the rights of the accused, the admissibility of evidence, and the application of the section 8 and 24(1) tests. While these issues are obviously important, they are not the focus of this paper. Our focus is on ensuring the privacy rights of the public at large in the face of increasingly sophisticated surveillance technology.

17 Jed Rubenfeld, "The End of Privacy," (2008) 61:1 *Stanford Law Review* 121.

The Fourth Amendment provides that: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

18 *Freedom of Information and Protection of Privacy Act* R.S.O. 1990, Chapter F.31 (*FIPPA*); *Municipal Freedom of Information and Protection of Privacy Act* R.S.O. 1990, Chapter M.56 (*MFIPPA*).

19 *Supra* note 13.

20 Massimo Calabresi and Michael Crowley, "Homeland Insecurity; Do we need to sacrifice privacy to be safer?" *Time Magazine* (13 May 2013) at 28.

21 *Constitution Act*, *1867*, 30 & 31 Vict, c.3, (U.K.) reprinted in RSC 1985, App II, No 5., s. 91.

22 *Cash Converters Canada Inc. v. Oshawa (City)* 2007 ONCA 502 at paras 30-31, quoting the *Williams Commission Report (Public Government for Private People: The Report of the Commission on Freedom of Information and Protection of Individual Privacy* (1980) 3) at 504-505, the report that led to the enactment of Ontario's public sector privacy legislation.

23 *Criminal Code*, R.S.C., 1985, c C-46.

24 At the same time, note that, for example, under s. 21(1)(c) of *FIPPA* and s. 14(1)(c) of *MFIPPA*, the privacy protective rules regulating the handling of "personal information" by Ontario public sector institutions do not apply to a narrow

class of "personal information" that is maintained "for the express purpose of creating a record available to the general public." (The fact that an individual has disclosed the information to the public, for example, via the press, does not render it public within the meaning of these provisions. See *Investigative Report I94-011P* quoted in *MO-1366 [2000] O.I.P.C. No. 203* at para 44 and *I95-24M [1996] O.I.P.C. No. 80* at para 13. Further, note that our office has determined that: "Other institutions cannot claim the benefit of the exclusion for the same personal information unless they, too, maintain the information for the purpose of making it available to the general public. In our view, this interpretation is not only reasonable, but also in keeping with one of the fundamental goals of the Act, namely 'to protect the privacy of individuals with respect to personal information about themselves held by institutions.' … Information contained in police daily arrest sheets (*Order M-849*), dockets listing daily matters being heard under the *Police Services Act* (*Order M-1053*), a list of all doctors registered with the College of Physicians and Surgeons of Ontario (*Order P-1635*) and a list of the names and addresses of all persons licensed to drive in the province of Ontario (*Order P-1144*) have all been found to not satisfy the requirements of ss. 14(1)(c) and 21(1)(c)." [*MO-1366* at para 45].

25 For example, s. 39(3) of *FIPPA* provides certain law enforcement-related exemptions from the general duty to provide all affected individuals notice of indirect collections of their personal information.

26 *Copeland and Adamson*, [1972] 3 O.R. 248 (OHCJ).

27 *R. v. Tse* 2012 SCC 16 at para 17, quoting Justice La Forest in *R. v. Duarte*, [1990] 1 S.C.R. 30.

28 *Ibid* at para 16.

29 *Supra* note 1, at para 69 (quoting the majority in *R. v. Wong*, [1990] 3 S.C.R. 36) and para 81.

30 *R. v. Wong*, [1990] 3 S.C.R. 36. See also *Supra* note 23, s. 487.01, but note *Supra* note 7 at 30.

31 *Supra* note 27, at para 28.

32 *Supra* note 27, at para 85.

33 *Supra* note 27, at para 98.

34 Bill C-55, *An Act to Amend the Criminal Code (Response to the Supreme Court of Canada Decision in R. v. Tse)*,1st Sess, 41st Parl, 2013.

35 Note that, in *R. v. Tse* (*supra* note 27) at para 57, the Supreme Court signalled that it had strong "reservations about the wide range of people who, by virtue of the broad definition of 'peace officer,' can invoke the extraordinary measures permitted under s. 184.4 [of the *Criminal Code*]."

The definition of "peace officer" includes "mayors and reeves, bailiffs engaged in the execution of civil process, guards and any other officers or permanent employees of a prison, and so on." Without ruling on the point, the Court stated that the emergency warrantless wiretap powers "may be constitutionally vulnerable" for this additional reason (see paras 55-57).

In addition, at para 89 the Supreme Court had welcomed rather than required "added safeguards, such as the preparation of reports for Parliament." The Court did observe that, as a "matter of policy, a reporting regime that keeps Parliament abreast of the situation on the ground would seem to make good sense."

36 *R. v. TELUS Communications Co.* 2013 SCC 16 at para 58.

37 *Ibid* at paras 75 and 5.

38 *Supra* note 36 at para 33.

39 *Supra* note 15.

40 *Supra* note 15 at para 75.

41 *Supra* note 15 at paras 72-74.

42 *Supra* note 15 at para 71.

43 *Supra* note 15 at paras 74, 95-109.

44 See, for example, Lukas Feiler, "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection" *European Journal of Law and Technology*, Vol 1, No 3 (2010). Online: <http://ejlt.org/article/view/29/75> and EC, *Commission Directive 2006/24/EC* of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

45 As indicated in letters from various private sector entities supporting *CISPA*, U.S. companies are already engaged in some critical infrastructure protection-related information-sharing. Online: <http://intelligence.house.gov/hr-3523-letters-support>.

46 U.S. Presidential Exec Order, "Improving Critical Security Infrastructure" (12 February 2013).

47 Chris O'Brien, "Senate Indicates it Won't Consider CISPA," *LA Times* (29 April 2013) online: <http://www.latimes.com/business/technology/la-fi-tn-senate-cispa-20130429,0,357666.story>.

48 Ann Cavoukian, "The Issue," online: RealPrivacy < http://www.realprivacy.ca/issue>.

49 Malvin Gutterman, "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance" (1988) 39 *Syracuse Law Review* at 647. See also *United States v. White* 401 U.S. 745. And see the discussion of "Project Champion" in Pete Fussey and Jon Coaffee, "Urban spaces of surveillance," The Routledge Handbook of Surveillance Studies, edited by Kirstie Ball, David Lyon, Kevin Haggerty. Routledge: New York (2012) at 207-208.

50 Jason W. Patton, "Protecting privacy in public? Surveillance technologies and the values of public places," *Ethics and Information Technology* (2000) 2: 3 at 183; and Alan F. Westin, *Privacy and Freedom* (New York: Athenum, 1967) at 31.

51 *R. v. Poncelet,* [2008] SKQB 157 at para 27.

52 *United States v. Jones* 625 F. 3d 544 at 3.

53 *Supra* note 5 ("A Technology-Centered Approach to Quantitative Privacy").

54 *R. v. Kang-Brown*, [2008] 1 S.C.R. 456 at paras 79 and 104.

55 As discussed in *Supra* note 52, in U.S. Supreme Court cases from the 1980's, the use of a beeper was effected with the consent of the original owner of the vehicle or container being tracked. See *U. S. v. Knotts*, 460 U.S. 276 [1983] and *U. S. v. Karo*, 486 U.S. 705 [1984].

56 Office of the Information and Privacy Commissioner of British Colombia *Investigation Report F12-04: Use of Automated Licence Plate Recognition Technology by the Victoria Police Department* (15 November 2012) online: <http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF12-04.pdf>.

57 *Supra* note 1 at para 14.

58 *Brown v. Durham (Regional Municipality) Police Force*, [1998] 116 O.A.C. 126 at paras 67, 77.

59 *Supra* note 18 (*FIPPA*) at s. 38(2). See also *Supra* note 18 (*MFIPPA*) at s. 28(2).

60 *Supra* note 18 (*FIPPA*) at s. 2(1). See also *supra* note 18 (*MFIPPA*) at s. 2(1).

61 *IPC Investigation I94-048M: A Regional Police*, [1994] O.I.P.C. No. 428 at 2-3.

62 *R. v. Mellenthin*, [1992] 3 S.C.R. 615 at 624.

63 *Supra* note 58 at para 38.

64 *R. v. Ladouceur* 2002 SKCA 73 at paras 43, 54.

65 Office of the Privacy Commissioner of Canada, *2011-2012 Annual Report to Parliament on the Privacy Act: The Privacy Act 1982-2012 — Three Decades of Protecting Privacy in Canada* (October 2012), at 19 online: <http://www.priv.gc.ca/information/ar/201112/201112_pa_e.pdf>.

66 *Supra* note 56 at 3.

67 *Supra* note 56 at 6 and 28.

68 *Supra* note 13 at 2.

69 Justice Gérard La Forest, Opinion (5 April 2002) online: <http://www.priv.gc.ca/media/nr-c/opinion_020410_e.asp>.

70 *R v. Silva,* [1995] O.J. No. 3840 at para 46. See also *R. v. Baker,* [1998] B.C.J. No. 1854; but also see *R. v. LeBeau,* [1988] O.J. No. 51 where the Ontario Court of Appeal determined the accused had no reasonable expectation of privacy in the circumstances.

71 *R. v. Rudiger* 2011 BCSC 1397 at paras 91-92.

72 *Ibid* at paras 101, 93, 98.

73 *Ibid* note 71 at para 40.

74 *Ibid* note 71 at paras 113 and 117.

75 *R. v. Hounsell,* [1994] N.J. No. 319 and *R. v. Bryntwick* [2002] O.J. No. 3618.

76 *Supra* note 13.

77 *Supra* note 1.

78 *Supra* note 13 at 3-10. And see John Papazian, "The Lens of Law Enforcement: A Geospatial Statistical Program Evaluation of Denver's HALO Camera Surveillance System," 2013 *Sanford Journal of Public Policy* 4 at 109, online: <http://sites.duke.edu/sjpp/files/2013/04/Papazian-The-Lens-of-Law-Enforcement.pdf>; and Rajiv Shaha and Jeremy Braithwaite, "Spread too thin: analyzing the effectiveness of the Chicago camera network on crime," *Police Practice and Research: An International Journal* (2012) online: <http://www.tandfonline.com/doi/abs/10.1080/15614263.2012.670031#.UaYP6kA4tBl>.

79 *Supra* note 13 at 26. And see Charles Farrier, "Civil Liberties and CCTV Camera Surveillance. Landmark Court Decision in Australia," *Global Research* (9 May 2013) online: <http://www.globalresearch.ca/civil-liberties-and-cctv-camera-surveillance-landmark-court-case-in-australia/5334423>.

80 The *Guidelines* are intended to assist organizations in determining whether the collection of personal information by means of overt video surveillance is lawful and justifiable as a policy choice, and if so, how privacy-protective measures may be built into the system. Before deciding whether to use overt video surveillance, the *Guidelines* recommend that organizations consider the following:

- A video surveillance system should only be adopted after other measures to protect public safety or to deter, detect, or assist in the investigation of criminal activity have been considered and rejected as unworkable. Video surveillance should only be used where conventional means (e.g., foot patrols) for achieving the same law enforcement or public safety objectives are substantially less effective than surveillance or are not feasible, and the benefits of surveillance substantially outweigh the reduction of privacy inherent in collecting personal information using a video surveillance system.
- The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.
- An assessment should be made of the effects that the proposed video surveillance system may have on personal privacy and the ways in which any adverse effects may be mitigated.
- Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video surveillance program and its acceptability to the public.
- Organizations should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required, lawful goals.

Once a decision has been made to deploy overt video surveillance, the *Guidelines* set out the manner in which video surveillance cameras should be implemented in order to minimize their impact on privacy.

81 *Supra* note 1 at para 75.

82 *Supra* note 52 at 955-956.

83 *Supra* note 52 at 963-963.

84 *Supra* note 52 at 954.

85 *Supra* note 52 at 962, 964, per Alito J.; 956 per Sotomayor J.

86 *Supra* note 52 at 956.

87 *Supra* note 27 at para 98.

88 Calo, R. (2011), "The drone as privacy catalyst." 64 *Stan. L. Rev*. 29 online: <http://www.stanfordlawreview.org/online/drone-privacy-catalyst>.

89 At present, there are three main types of drones: micro and mini drones, tactical drones, and strategic drones. Micro drones, weighing as little as 100 grams (about 3.5oz), fly at low altitudes (below 300 metres, or approximately 1,000 feet). Mini drones, which weigh up to 30 kilograms (approximately 66 pounds), fly at altitudes between 150 and 300 metres (approximately 500 and 1,000 feet). Tactical and strategic drones are considerably larger and heavier (from 150 to 1,500 kilograms and up to 15,000 kilograms, or from approximately 330 to 3,300 pounds and up to 33,070 pounds, respectively) and fly at much greater altitudes (from 3,000 to 8,000 metres, or approximately 10,000 to 26,250 feet) and up to 20,000 metres (approximately 66,000 feet), respectively, and for longer periods of time (35 to 40 hours or more). Tactical and strategic drones are associated predominately with military applications.

90 See Brian Bennett and Joel Rubin, "Drones are taking to the skies in the U.S.," *LA Times* (15 February 2013) online: <http://articles.latimes.com/2013/feb/15/nation/la-na-domestic-drones-20130216>.

91 See Ben Wolfgang, "FAA chief says drones will force change at agency," *The Washington Times* (7 August 2012) online: <http://www.washingtontimes.com/news/2012/aug/7/faa-chief-says-drones-will-force-change-at-agency/>. And see Matt Hickey, "Is Seattle Being Buzzed By Drone-Equipped Peeping Toms?" *Forbes*, 29 May 2013, online: <http://www.forbes.com/sites/matthickey/2013/05/28/is-seattle-being-buzzed-by-drone-equipped-peeping-toms/>.

92 See "FAA Makes Progress with UAS Integration," Federal Aviation Administration (page last modified 14 May 2012) online: <http://www.faa.gov/news/updates/?newsId=68004>.

93 *Supra* note 91 and see "Unmanned Aircraft Systems (UAS) – Online Session on UAS Test Site Privacy Policy," Federal Aviation Administration online: <http://www.faa.gov/about/initiatives/uas/>.

94 See Alexandra Gibb, "Privacy concerns hover over RCMP drones in British Columbia," *TheThunderbird.Ca* (29 March 2012) online: <http://thethunderbird.ca/2012/03/29/privacy-concerns-hover-over-rcmp-drones-in-british-columbia/>; "Unmanned Air Vehicle (UAV)," Transport Canada online: <http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-brochures-uav-2270.htm>.

95 See Allie Bohm, "Status of Domestic Drone Legislation in the State," *American Civil Liberties Union* online: < http://www.aclu.org/blog/technology-and-liberty/status-domestic-drone-legislation-states>.

96 *Ibid*.

97 *The Preserving American Privacy Act* was first introduced by Republican Reps. Poe and Gowdy in 2012 as H.R. 6199. Like two other comparable drone bills from the last session of Congress (Sen. Rand Paul's (R-Kentucky) S.3287, *The Preserving Freedom from Unwarranted Surveillance Act of 2012*, and Rep. Ed Markey's (D-Mass) H.R. 6676, *The Drone Aircraft Privacy and Transparency Act of 2012*), H.R. 6199 died when the session concluded. All 3 bills set warrants as the general rule for most law enforcement drone-based surveillance.

98 See progress of H.R. 637 at: <http://thomas.loc.gov/cgi-bin/query/z?c113:H.R.637.IH>. And see Senator Rand Paul's comparable bill, S. 1016, *The Preserving Freedom from Unwarranted Surveillance Act of 2013*, introduced before the Senate on 22 May 2013, which aims to protect individual privacy against unwarranted governmental intrusion through the use of drones by imposing a warrant requirement with exceptions for the patrol of national borders, imminent danger to life or a high risk of a terrorist attack.

99 "Not just for modern warfare: RCMP to expand use of drone mini-helicopters," Douglas Quan, Postmedia News, 13/01/27, <http://news.nationalpost.com/2013/01/27/not-just-for-modern-warfare-rcmp-to-expand-use-of-drone-mini-helicopters/ …> "RCMP expands its drone fleet as watchdogs worry Canadians may face aerial snoops", Steve Mertl, Daily Brew, Jan. 28, 2013 <http://ca.news.yahoo.com/blogs/dailybrew/rcmp-expands-drone-fleet-watchdogs-worry-canadians-may-211447954.html ...> "Police drones sparks debate over personal privacy," Jennifer Quinn, Feb. 5, 2013, <http://www.thestar.com/news/world/2013/02/05/privacy_vs_security_when_does_the_use_of_drones_cross_the_line.print.html>.

100 *R. v Kelly,* [1995] N.B.J. No. 98 (C.A.) at 49-50.

101 *R. v. Lauda* 121 O.A.C. 365 AT 60-72, and see [1998] 2 S.C.R. 683. While *Lauda* is not an aerial surveillance case, in it, the Ontario Court of Appeal held that there may be a reasonable expectation of privacy in an open field, a finding not overturned by the Supreme Court of Canada.

102 *Supra* note 51 at paras 14-32.

103 *R. v. Douglas* 2000 BCPC 9 at paras 101-111.

104 In view of the Supreme Court of Canada's decision in *R. v. Boersma,* [1994] 2 SCR 488, a case dealing with a physical, on-the-ground search on Crown lands, it is not clear whether an individual would have a reasonable expectation of privacy with respect to drone surveillance over such lands.

105 *R. v. Patriquen,* [1994] N.S.J. No. 573 (CA), [1995] 4 S.C.R. 42 (SCC) at para 1.

106 *R. v. Kwiatkowski* 2010 BCCA 124 at paras 40-41.

107 *Supra* note 100 at para 50.

108 *Supra* note 51 at para 24.

109 *Supra* note 7, at para 28.

110 *Ibid* at para 29.

111 Note that the collection of personal information by a drone operator in the course of commercial activity is likely to be regulated under the *Personal Information Protection and Electronic Documents Act (PIPEDA)* S.C. 2000, c.5., as well as comparable legislation in British Columbia and Alberta. While the collection of personal information for personal or domestic purposes as well as for journalistic, artistic or literary purposes may not be covered by *PIPEDA*, in Ontario, any egregious, drone facilitated violation of privacy may attract civil litigation under the new tort of intrusion upon seclusion. See also *Jones v. Tsige* 2012 ONCA 32.

112 Comments of the then-UK Information Commissioner Richard Thomas, as reported in BBC News, "Britain is 'surveillance society'" (2 November 2006) online: <http://news.bbc.co.uk/2/hi/uk_news/6108496.stm>.

113 *Jones v. Tsige* 2012 ONCA 32 at para 39.

114 *Application under s.83.28 of the Criminal Code (Re)* 2004 SCC 42 at paras 115-116.

115 *Ibid* at para 8.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner,
Ontario, Canada

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca
Telephone: 416-326-3333
Fax: 416-325-9195

June 2013