Suggested Citation


Abstract

This article utilizes modern privacy theory to examine the differing approaches of Canadian and U.S. law enforcement to the use of camera technology and advancing video analytics. The article documents the deployment of camera technology in two comparably-sized urban centers in Canada and the U.S. The reception of camera technology in Canada and the U.S. to policing strategies utilizing sensors like cameras and video analytics tools like license plate and facial recognition are in sharp contrast. The article then offers a summary of Canadian and U.S. legal privacy protections following Alan Westin’s privacy model. This analysis suggests that the differences in the use of technology stem from philosophical and legal assessments of privacy rights. Specifically, protection for privacy concepts like anonymity and reserve explains the differing approaches. Understanding those differences is useful for administrators on either side of the border to plan their use of emerging imaging sensor technology and analytics.

Introduction

Police authorities in Canada and the U.S. make very different use of emerging surveillance technologies to support their policing strategies. Comparing the use of these technologies in cities of comparable size and diversity like Chicago and Toronto draws that difference into clear focus. In large measure, it is likely the differences stem from philosophical and legal assessments of privacy rights. Protection for privacy concepts like anonymity and reserve help to explain the differing approaches. Understanding those differences is useful for administrators on either side of the border to plan their use of emerging imaging sensor technology and analytics. Comparing the differing approaches offers a perspective on how the changing legal environment in both countries may be moving toward common ground.

Despite the existence of legal structures that offer differing protections for aspects of privacy, cross pressures of increased threats to public safety and desire for enhanced police accountability support adoption of advancing surveillance technologies. Understanding the underpinnings of those legal structures through the prism of the privacy definitions offered by Alan F. Westin helps explain the differing approaches in adapting technology to address common policing problems. It also demonstrates how differing values placed on aspects of privacy are balanced with competing practical concerns. Comparing those approaches demonstrates a movement toward common ground with U.S. jurisdictions enhancing protections to retrain some technology uses and Canadian jurisdictions relaxing restrictions to permit technology use.

These differing approaches offer law enforcement administrators examples of how specific privacy concerns can serve to shape the use of specific technologies. It also demonstrates how, in the face of differing privacy approaches, technology can be adapted to differing privacy concerns to address common problems.
Police Use of Cameras and Analytics

Toronto and Chicago share population and demographic traits. Both cities are large dense urban areas with population sizes approaching 3 million. Both cities have diverse populations. Both experience complex urban law enforcement challenges. However, the technology profiles with respect to the use of advanced surveillance technology stand in stark contrast.

Toronto’s Experience

Canada has one of the highest standards of privacy rights in the world. Freedom from state surveillance is something Canadians value highly. The presence of statutory enactments to protect individual privacy requiring showings of government need has had the effect of minimizing monitoring capacities. Accordingly, the use of surveillance cameras by the Toronto Police Service (TPS) was a relatively recent adoption that has only been marginally expanded.

In 2007, TPS installed 34 closed-circuit television (CCTV) cameras. Twenty-four of those cameras are installed in Toronto’s downtown core; 4 are used for rapid deployment and the remaining 6 are used on a case-by-case basis in areas where there is a significant crime issue, usually related to increases in victimization by violence.

The number of cameras remained unchanged for 12 years until 2019. In that year, gun violence began to rise across the city and the Province of Ontario invested 3 million dollars to add 40 more cameras. These cameras are being installed over a 3-year period.

There are 8 principles that govern the use of CCTV cameras in public places:

1. The use of CCTV is to be considered only after other measures of deterrence or detection have been considered or rejected as unworkable;
2. The use of each camera is justified by verifiable crime reports and significant safety concerns from the public;
3. CCTV cameras are used to view public areas only;
4. Ongoing assessments of the impact on privacy are carried out and reported;
5. Ongoing consultation is conducted with the community as to the necessity and acceptability of CCTV;
6. All records and stored video are under the control of the TPS;
7. There will be public notification before, during and after installation of CCTV cameras;
8. Large signs indicating the presence of CCTV cameras are displayed prominently at the perimeter of the area under observation.

These principles limit the use of cameras to public areas where they are highly visible, with presence published by signage, and with installation preceded by both extensive crime analysis and community consultation. They are also generally limited to post-event use of their images. This approach does not leverage real-time capabilities of video or afford much benefit from the
integration of cameras with other technologies. This is an area where there is significant legal and operational difference in practice between Canada and the U.S. For example, gunshot detection software is currently prohibited in Canada as the possibility that voices could be captured by the software means it cannot be used without a judicially authorized wiretap.\

In August of 2020, the TPS began deploying body worn cameras (BWC) to front-line officers. The only other major city deployment of this technology in Canada was in Calgary in 2019. The justification for BWC technology in Toronto was increased accountability, along with the opportunity for technological business process enhancements which could be realized by the camera, cloud storage and disclosure system. This technology allows for new digital innovations such as cloud storage, immediate disclosure of digital evidence to stakeholders, and the possibility of other new capacities such as digital notebooks. This technology has also brought up ethical and legal questions regarding when someone can be filmed by the police in public versus when a person can assert their right to privacy. Given that the technology is so new in Canada, many of these questions are still to be answered.

Concerning the application of analytics like facial recognition (FR), the experience in Toronto is also limited. Due to a lack of precedence-setting criminal case law regarding FR and video surveillance in public spaces, the principles for use are like those regarding CCTV cameras. It is accessed post-offense and is comparable to police photos legally obtained through the Identification of Criminals Act. Like fingerprint analysis, images captured in connection with an offense are subsequently analyzed against a criminal photograph database to find points of intersection sufficient to determine a match. This match then needs to be validated by investigators. Reports written by the Ontario Information and Privacy Commissioner outline the similarities in ensuring the right to privacy in public spaces is maintained whether it is online, in real life (IRL), or through the use of technology. When the TPS sought to expand the use of FR in a manner arguably inconsistent with these narrow parameters, those efforts met with fierce public criticism and were quickly discontinued.

It is important to note that quasi-public spaces may use FR that citizens are deemed to have accepted if they chose to enter such spaces. For example, airports use FR to ensure border security, and provincial drivers license offices use FR to prevent fraud, while casinos and sporting events use the software to ensure security. In this way, not all public places are subjected to the same standard of privacy as the distinction between public and private places continues to be blurred.

To conclude, the TPS CCTV camera experience is limited and primarily focused on post-event digital evidence coverage. The program will expand the number of cameras by more than double the current number to a total of 74 cameras by the end of 2022. The principles that oversee this program remain a key feature to ensure the limited right to privacy that is enjoyed in public spaces remains intact. With the introduction of body-worn camera technology, the ethical and legal implications of police surveillance in public places will continue to evolve with ongoing assessment of measures necessary to manage emerging technologies and their usage. The recent implementation of body worn cameras by the Toronto Police Service (TPS) is a current example of how new technologies will change legal considerations regarding anonymity in public spaces. While FR continues to be used in the manner outlined above, the expansion of FR use is a concern. This concern is exacerbated as a citizen’s likelihood of being digitally captured in public increases with more officers wearing body worn cameras and with CCTV usage expanding.
Chicago’s Experience

Use of cameras and other sensors in Chicago has been a long-standing practice. Commencing in July 2003, the Chicago Police Department (CPD) instituted its public safety camera program with the deployment of what it called police observation devices. This program involved the placement of surveillance cameras in high crime areas across the City. By today’s standards, the initial efforts offered little in the way of capabilities for use. Storage was conducted on-site with retrieval of data requiring physically accessing the hard drives. The range for the real time transmission of video images was relatively limited.

Chicago’s initial efforts were transitioned into a program called Operation Virtual Shield (OVS). Initiated in January 2005, OVS sought to create an integrated city-wide camera and sensor network. OVS provided a unified access to camera images though a centralized viewing platform operated at the City’s Office of Emergency Management and Communications (OEMC). Camera images came from cameras operated by several city departments, including the police, as well as sister agencies like the Chicago Public Schools (CPS), Chicago Housing Authority (CHA), and Chicago Transit Authority (CTA). By 2018, OVS reportedly allowed for the viewing of over 32,000 camera views.

The use of the CPD video surveillance technology is governed by a departmental General Order that sets forth principles and general guidelines for the use of the technology. That General Order outlines the various purposes for which the technology can be used. It also specifies requirements for use in an “ethical manner” in accordance with “accepted legal concepts regarding privacy.” Provisions in the guidelines portion of the General Order require legal training for operators, limit the areas which can be observed to public areas, and prohibit profiling or bias-based” use of the technology. Use is limited to proper law enforcement purposes and unauthorized “recording, viewing, reproduction, retention, or distribution” of images is prohibited.

In addition to offering real-time access to images, the OVS system records and retains images from city-owned cameras, including those of CPD. City-owned cameras are only a portion of the total. While the federated OVS system affords the ability to view real-time images at the OEMC, agencies like CTA, CPS and CHA that operate the camera systems retain ownership over digital images. Those agencies also remain responsible for maintaining the cameras and retaining camera images. As an example, the CTA, which as of 2020 boasts over 38,000 cameras in its system (including on trains and buses as well as on transit platforms), provides OEMC access to some of its cameras. The CTA cameras that feed into the OVS system are not recorded or retained in the OVS system. They are only viewed in real time. Persons seeking recordings must process those requests through CTA. The CPD has developed a Special Order, outlining processes for recovery of image data from the CTA’s surveillance system.

The reach of Chicago’s OVS system extends beyond cameras operated by the City or related governmental agencies. It also includes an ability to access the images of public-facing cameras from private-sector organizations. Initially, the ability to access camera views of public areas captured by private cameras, was limited to cameras of larger corporate properties like the Willis Tower and Boeing corporate headquarters, but that access has
expanded over time. Most recently the ability of CPD to access private camera images has even expanded to residential cameras through a pilot with the Amazon Ring. CPD is experimenting with access to those cameras to address neighborhood disorder problems. This program has been met with a strong response from the American Civil Liberties Union.

Another major evolution of Chicago’s camera system involved an initiative by CPD to take the camera data captured thorough OVS and combine it with other information systems in a common platform. The additional systems included: sensor data like gunshot detection; geospatial information systems like computer aided dispatch system; and other information and analytic tools. That common information platform was then used in Strategic Decision Support Centers (SDCs) established in police districts across the City to better inform decision-making at the operational level. A study of the SDCs, conducted by the Rand Corporation on behalf of the Department of Justice’s Bureau for Justice Assistance noted that significant reductions in violent crime could be anticipated as a result of this technology adoption. The move toward greater integration and distribution of sensor information and application of analytics is even being taken to the level of individual CPD officers by equipping them with smart phones so they can access that information directly.

In addition to a vast expansion of its fixed camera systems, the City of Chicago has embraced use of mobile technologies and the adoption of wearable body cameras. Beginning in 2015, the City began piloting the use of body cameras. By the end of 2017, the full complement of Chicago’s patrol officers had been equipped with body cameras. The use of that equipment is subject to detailed department rules and extensive state statutory requirements. Issues of data collection, storage, and dissemination are all governed by state statute. Unlike the other portions of Chicago’s video programs, the body-worn cameras are limited to post-event use. However, technology developments may offer an ability to use data in near real time.

Chicago has also been at the forefront of adopting technology like FR. The City has been formally utilizing FR technology in connection with investigations since 2013. CPD promulgated a Department Notice in August 2013 to govern the use of FR technology. The City has indicated that its use of FR does not include real time use of such software in connection with its camera system. The CPD experienced some success in solving crimes with the assistance of the FR technology. However, the City has been accused by privacy groups of providing little information in response to public information inquiries regarding its use of FR technology.

As with the Toronto police experience, the introduction of advanced analytics like FR has not been without controversy. Like Toronto, Chicago was utilizing the technology of Clearview AI. However, when concerns over the use of Clearview AI were raised by the ACLU alleging privacy violations under Illinois law, the City announced that it was discontinuing the use of that company’s services. The ACLU later sued Clearview, alleging privacy violations. While use of Clearview AI was discontinued, CPD continues to utilize other FR software for investigatory purposes.

In summary, the CPD experience is characterized by a decades-long pursuit of sensor technology to support police operations. Despite concerns raised by the American Civil Liberties Union, the CPD use of video programs has continued apace. The success of these technologies in addressing crime and disorder problems seems to be well accepted. A recent news story outlining how the City’s use of combined video technology to apprehend a bank robber provides a good example of the efficacy of the City’s combined system.
Understanding Privacy Concepts

Before looking at the issue of the legal treatment of surveillance technology, it is useful to understand a little bit about privacy concepts. This requires the acceptance of a common definition. The definition of privacy advanced by Westin has seen wide acceptance in the development of privacy regimes and offers a good starting point. Westin posits:

privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy, or, when among larger groups in a condition of anonymity or reserve.  

Westin’s definition respects the need for balance between the competing desire of the individual for privacy with the desire for social interaction. The final balance is a matter of individual preference and societal influence. Westin’s definition coalesces around four mechanisms by which privacy is achieved: solitude; intimacy; anonymity; and reserve. The intrusion posed by surveillance poses differing degrees of challenge against each mechanism.

Solitude, arguably the most perfected degree of privacy, is likely least affected. Because solitude by its nature involves separation from society, physically and psychologically, it least likely to be impacted by surveillance of public activity. The individual in solitude is generally unobserved by others. This is the state where the individual can be “…especially subject to that familiar dialogue with the mind or conscience.” In solitude the mind can achieve peace, paving the path for original thought. The presence of surveillance is antithetical to solitude.

Intimacy involves the act of disseminating information about oneself to a small unit or group. In intimacy, highly personal information is revealed. Westin describes it as a “corporate seclusion” for purposes of achieving “…a close, relaxed, frank relationship between two or more individuals.” Intimacy is often found in relations among family, friends, and close work associates. Because solitude presupposes no real sharing, surveillance opportunities are limited. As the circle of sharing expands in intimacy, the possibility of surveillance intrusion expands. As outlined below, this state of privacy may be impacted by digital surveillance techniques. While an individual may seek to share information within a small intimate group, those individuals may not accord the same sense of importance to maintain that information within that setting.

Contrasted with solitude and intimacy, which are exercised mainly outside of the public view, anonymity is principally a privacy expectation occurring in a public environment. Anonymity is “…when the person is in public places or performing public acts but still seeks, and finds, the freedom from identification and surveillance.” It is the ability of the individual to “…merge into the ‘situational landscape.’” Anonymity is profoundly affected by enhanced surveillance technology. New technologies not only increase capabilities to observe and catalogue conduct — they also improve the ability of ensuring an individual actor can be identified.

Like anonymity, reserve, is an exercise of privacy in public. The concept of reserve is that of placing “…psychological barriers against unwarranted intrusion.” This occurs by limiting
the communication of information about oneself to others. Westin equates this “mental distancing” to “social distancing.” Westin, referencing the earlier work of Simmel, observes that individuals act to withhold certain information deemed necessary by the individual to “...protect the personality.” It is this withholding of information to maintain the public’s perception of who the individual truly is that is the essence of reserve. Though surveillance may serve to undermine reserve in some circumstances, it generally does not have the same effect as it does on anonymity. Surveillance may expose to the public some actions a person may choose to hold private but the consequences to reserve are less the result of the collection of information than by its dissemination.

With respect to this last aspect of privacy, Judge Richard Posner makes some observations about privacy and secrecy.

“Privacy” is a word of many meanings. The meaning that is most relevant to this essay is secrecy—the interest in concealing personal information about oneself. But I need to distinguish between a person’s pure interest in concealment of personal information and his instrumental interest, which is based on fear that the information will be used against him.

The “pure interest in concealing information” would be what Westin calls reserve. Secrecy under this analysis seems to be a subset of information being concealed. This secret information is information that is perceived to be potentially harmful.

Legal Treatment of Privacy Concepts

Looking at the structure of privacy as a multifaceted concept, Canadian and U.S. legal systems take differing approaches to protecting each of those facets. The Canadian approach is much more comprehensive. It extends robust protection to all the aspects of privacy identified by Westin. The U.S. approach is less comprehensive with some aspects of privacy receiving less protection. This is particularly reflected in the adoption of emerging body camera technology and FR solutions.

The Canadian legal system is characterized by a comprehensive federal approach to privacy protection. All the facets of privacy identified by Westin are addressed by Canadian law. Canadian courts have defined privacy as “the right of the individual to determine when, how, and to what extent he or she will release personal information.” The Canadian Charter of Rights and Freedoms (CCRF) ensures the right of everyone to be secure against unreasonable search and seizure. This provision under Section 8 is to “protect individuals from unjustified state intrusions upon their privacy.” The analysis applied under Section 8 is to determine if the public’s interest in being left alone must be overcome by the government’s interest to intrude on the right to privacy to advance its goals, in particular that of law enforcement. The determination of whether or not an individual has a reasonable expectation of privacy is contingent on the court’s examination of the totality of the circumstances. This is a key area of distinction between U.S. and Canadian law: the concept of an expectation of privacy from government surveillance in a wide range of situations including in public places, depending on a variety of factors for consideration.
Unlike in Canada, there is no central federal legislation that guarantees comprehensive privacy protections for individuals. The U.S. approach requires a piecing together of varying federal, state, and even local protections. The Fourth Amendment to the U.S. Constitution is generally thought to contain the principle federal protection for individual privacy. However, privacy protections have been found in other portions of the U.S. Constitution. While initially the Fourth Amendment focus was narrow and property based to areas like the home, it has been expanded to extend privacy protection to an expanding range of public conduct. Using Westin’s privacy analysis, the following are examples of how constitutional protections have been applied.

### Comparative Analysis Under the Westin Privacy Construct

Utilizing the Westin framework, the protections for privacy demonstrate some substantial differences between Canadian and U.S. legal approaches. The differing perspectives on certain aspects of privacy help explain differing use patterns concerning surveillance in general and the use of more traditional tools like fixed-camera networks. It also helps in the understanding of use patterns with respect to emerging technology trends like the use of wearable cameras and the increasing application of analytics tools.

### Solitude

The assessment of CCRF Section 8 includes the person’s subjective expectation of privacy and whether this was objectively reasonable in the totality of the circumstances. This would also take into consideration territorial privacy, including the Semayne’s case concept that everyone’s house is their castle. The Supreme Court of Canada has stated that the home is the place where the reasonable expectation of privacy is the greatest. Part of the reason for the highest expectation of privacy being their home is the fact that this is the place where people engage in their most intimate and private acts.

Similar protections are found in the U.S. The plain language of the Fourth Amendment offers protection to individuals principally focused on security of individuals in their “… persons, houses and papers....” In 1928, the U.S. Supreme Court first addressed protections for privacy against the use of what was then a high-tech surveillance technology directed at activity in the home in *Olmstead v. United States*. There the Court applied a trespass-based analysis noting that since the intrusion of the wiretap occurred off the property, no Fourth Amendment infringement was found.

In the 1960s, the Court moved from a property-focused analysis of the Fourth Amendment to one focused on the individual’s expectations of privacy. In *Katz v. United States*, the Court found that areas outside the home, in that case a phone booth which had been bugged, were protected under the Fourth Amendment so long as the individual in the phone booth has a subjective expectation of privacy that society was willing to recognize as reasonable. In *Jones v. United States* the Court concluded that both the reasonable expectation of privacy and trespass-based analysis were valid to establish Fourth Amendment protections.
The protection of both home and person are well established under the Fourth Amendment. With respect to the home, its special status is noted in the Court’s decision *Kyllo v. United States*.62 There the Court concluded the privacy interest of the home’s occupant made use of standoff thermal detection by law enforcement a Fourth Amendment violation. Similar conclusions are found with respect to the integrity of the person. See, *Terry v. Ohio*.63

**Intimacy**

Intimacy also enjoys similar protections in Canada and the U.S. Private conversations are generally exempt from state scrutiny in Canada.64 More specifically, there is an expectation of privacy around private conversations that the state can only violate with judicial authorization obtained based on the commission of an offense.65 This protection of intimacy is not necessarily established by either territory or the number of people present when a conversation takes place.66

Privacy protections also relate to intimate relationships. In 1969, an omnibus bill was passed in the House of Commons to decriminalize same-sex relationships and abortions in limited circumstances. In announcing this bill, then Justice Minister Pierre Trudeau famously stated, "there’s no place for the state in the bedrooms of the nation."67 This liberal principle has extended into other areas of Canadian law, for example the recent decision for exemptions to sections of the Canadian Controlled Drug and Substances Act to allow for supervised drug injection sites.68

In the U.S., just as the Supreme Court has recognized the importance of protecting solitude through protection of persons and the home, so to is protection of intimacy a focus of constitutional import. In *Kyllo*, the Court observed that Fourth Amendment protections of the home are designed to protect the intimate aspects of an individual’s life.69 However the protection of privacy in intimate relationships is not limited to those occurring inside the home or those guaranteed by the Fourth Amendment.

In *Roe v. Wade*70, the Court noted a history of prior decisions having identified privacy protection for intimate relationships under the First, Fourth, Fifth, Ninth, and Fourteenth Amendments to the Constitution. Those protections extend outside the home to social relationships,71 as well as a continuum of other relations that foster individual growth and development. 72

**Anonymity**

Even in public places, there is a limited right to anonymity in Canadian law. In fact, Westin’s definition of public privacy is used in numerous Canadian cases to assert the right to be free from surveillance and identification in public venues or while performing public acts.73 It is interesting to note that such public spaces include movements on the internet.74

In determining whether or not there is a reasonable expectation of anonymity while in public, several factors will be considered by the court including the degree of exposure or seclusion, the limitation of attention paid, various social rules, the dispersion of information over space and time, and the ephemeral nature of the use of public space.75 The court has aptly noted that
privacy-invasive technologies are a rogue factor that disrupts normal expectations of public privacy and further undermines the distinction between public and private places.\textsuperscript{76}

In stark contrast to Canada, the protections for anonymity in the U.S. are much less developed. It is certainly the state of privacy that is offered the least protection under U.S. law. Protections are largely limited to associational rights under the first amendment. Moreover, a range of statutory provisions that limit or constrain anonymity in public have been found to pass constitutional muster. Overall, a fair characterization of the law with respect to anonymity is that it is generally limited.\textsuperscript{77}

The only area in which anonymity has been afforded constitutional protection has been in those cases where the Court has found it a prerequisite to effective political activity. In \textit{NAACP v. Alabama},\textsuperscript{78} the court addressed the ability of members of political organizations to maintain their anonymity. In that case the Court concluded that where compelling disclosure of the identity of group members would impair associational rights, First Amendment protections prohibited such governmental activity.

In contrast, however, the Court noted that in other circumstances, identity information can be compelled by the State. Upholding a Nevada stop and identify law, the Court affirmed the ability of police to require individuals suspected of committing crimes to provide identifying information.\textsuperscript{79} Such information was not protected under the Fourth Amendment or the provisions against self-incrimination under the Fifth Amendment.

So long as the surveillance techniques employed were not designed or applied in a way that served to chill the exercise of associational rights by techniques like the identification and cataloguing of group members, it is likely those surveillance techniques would be permitted in the U.S. This allowed for liberal expansion of camera surveillance programs and growing concern by advocacy groups about government ability to track individuals.

\textbf{Reserve}

There is a \textit{prima facie} protection of personal information from disclosure to the state without a warrant in Canadian law.\textsuperscript{80} While this can be considered a quasi-constitutional protection,\textsuperscript{81} there are also distinct provincial laws which specifically raise this level of protection.\textsuperscript{82} With most personal information now residing on the internet or an electronic storage system, the Supreme Court of Canada has made it clear that a warrant is required to obtain any personal information, including identifiers such as an internet protocol address.\textsuperscript{83} The courts have come to the same conclusion regarding other technologies such as the use of cell phone records to pinpoint the geographic location of the cell phone at a specific date and time, as well as vehicle transponder records.\textsuperscript{84} This \textit{prima facie} protection of personal information is consistent with Weston’s concept of reserve.

Going forward, Canadian courts will need to consider not only the implications of big data, but the use of this information in artificial intelligence and machine learning. It is no longer the mere protection of personal information that needs to be considered, but how the integration of various data sets can lead to new personal information being developed and how such conclusions regarding the individual are to be assessed.
In the U.S., the protections for reserve are growing. With respect to reserve, the protections of the Fourth Amendment have evolved to extend protections of individuals from large data collections created by or accessible to government. Beginning in the late 1970s some Supreme Court Justices began expressing concern over the privacy considerations created by government data collection and developments in supercomputing which allow that data to be processed and analyzed. Similar concerns were raised by members of the Court in the late 1980s concerning government retention of criminal history information.

The forty-year debate over Fourth Amendment protection for reserve was finally advanced in favor of protections in a 2018 decision concerning governmental access to cell site location information (CSLI). CSLI information is created automatically by the operation of cellphones seeking to connect with cell towers to maintain service and is routinely collected by cell phone providers to calculate use charges. The Court in Carpenter concluded that given the details of life this information disclosed, an individual had a protectable privacy interest in the data, even though it was possessed by a third party. Given the privacy interest in the data, the Fourth Amendment precluded government access to it in the absence of a warrant based on probable cause.

The decision in Carpenter placed great reliance on two concurring opinions previously offered in the case of Jones v. United States, which had examined government practices in GPS tracking of suspects. Those concurring opinions, which included five of the nine justices, articulated significant concern over the ability of government to amass data, any piece of which was permissible to collect, into a comprehensive dossier on individuals that implicated privacy concerns.

The decision in Carpenter, combined with the concurring opinions in the Jones case, strongly supports the protection for Westin’s concept of reserve. The new protections offered for reserve should give some pause to law-enforcement administrators with respect to the retention of data and use of large data compilations.

Privacy Impact on Surveillance Technology Development

Having examined the differing legal approaches in Canada and the U.S. to privacy through the lens of the Westin framework, our focus now shifts to impacts on law enforcement use of developing technologies like FR and body cameras. While adoption of these technologies is more pronounced in the U.S., concerns of privacy have served to limit applications in many U.S. jurisdictions. In converse fashion, despite legal impediments, Canadians have engaged in some measured use of some of these technologies in response to concerns of accountability and desire to enhance law enforcement effectiveness.
FR and Body Camera Technology in Canada

Given the philosophical underpinnings of Canadian law with respect to privacy, there is little surprise that the use of both body cameras and FR is limited. The Canadian public’s lack of tolerance for expanded use of FR outside of limited post-incident investigative parameters was clearly demonstrated in 2020 by reaction to disclosures of police use of the Clearview AI FR software in early 2020. Journalists learned that several police agencies including the Royal Canadian Mounted Police (RCMP), Calgary Police Service, and Toronto Police Service (TPS) were all using the FR software that compared images of persons of interest to an extensive photo bank of billions of images obtained from social media accounts. The backlash was immediate and strong, prompting formal objections from the Canadian Civil Liberties Association and investigations from federal and several provincial privacy authorities. As a result, Clearview AI announced in July 2020 that it would no longer offer its software in Canada.

The slow adoption of body camera technology demonstrates a similar concern about expanding surveillance capability of the police beyond the current narrowly accepted uses. In a country where protections for anonymity and reserve are well-established, slower adoption of technologies like body cameras that can directly impact those interests is a likely result. While countervailing concerns over police accountability have served to influence decisions on body camera deployment. The surveillance and privacy concerns offer significant counterweight.

While concerns over police accountability and response to criminal activity may result in moderation of some the current limits on use of surveillance technologies, the strength of Canada’s existing centralized privacy protections mean that the process will likely be a slow one. While emerging technologies can certainly change societal privacy expectations, the pace of adoption of that technology will likely need to be measured and transparent. The reaction to police uses of Clearview AI illustrates how police adoption of emerging technology in a manner inconsistent with that guidance can cause significant public discontent.

FR and Body Worn Cameras in the U.S.

As with the Canadian experience, the legal landscape in the U.S. around the expansion of body cameras and the application of FR analytics continues to evolve, though in the absence of a centralized national focus on privacy, the expansion of both technologies is significantly more pronounced. As with many emerging technologies, the pace of development far outstrips the legal process addressing the use. As the legal system adapts, the law changes. This unstable legal environment hampers long-term planning for use of technology and makes for inconsistent technology applications. The uneven legal approach to technology also creates a reluctance to adopt it.

Recent legal developments in the U.S. around FR demonstrates the effect of legal instability attributable to the lack of a national standard. Unlike the more centralized approach in Canada, local sensitivity to and concerns about privacy are drivers in the U.S. Those sensitivities have significantly shaped the usage of analytic technology across the U.S.
radically different ways. Jurisdictions like Chicago have embraced technology like FR, but such adoption is hardly universal across the U.S. Several jurisdictions have followed the Canadian path, enacting bans and moratoriums on the use of FR technology pending further study of the privacy impacts of the technology.92

In contrast to FR, the adoption of body worn cameras in the U.S. has been more widely accepted within the U.S. policing community. Prior to 2013, approximately one-third of the police agencies across the U.S. were utilizing that technology. However, in the wake of widespread unrest after an August 2014 police shooting in Ferguson MO and subsequent incidents where police violence was alleged, the number of departments in the U.S. using body worn cameras rapidly expanded. By 2016 the number of jurisdictions utilizing body-worn cameras had increased to 47%. Among the country’s 45 largest police jurisdictions (employing 1000 or more officers), 80.5 % had procured body cameras by the end of 2016 with 70% having body cameras deployed.93

Unlike Canada, the federal government in the U.S. openly promoted body camera use. In a 2015 the U.S. Department of Justice initiated a funding program to assist agencies in developing the body worn program.94 The program provided $23 million in federal funding to assist 73 agencies across 32 states to procure body camera equipment and receive training. In 2016 an additional $20 million was awarded to 106 law enforcement agencies.95 In June 2021, the U.S. Department of Justice announced its intent to promulgate guidelines for use of body cameras by law enforcement.96

Unlike FR technology, the use of body cameras has also been advocated in the U.S. by a variety of civil rights advocacy groups.97 Body cameras are considered by those groups to be important measures to ensure transparency in policing and to achieve greater accountability for police misconduct. An example is the position of the ACLU. Concerning body worn cameras, Jay Stanley, ACLU Senior Policy Analyst observed

Although we at the ACLU generally take a dim view of the proliferation of surveillance cameras in American life, police on-body cameras are different because of their potential to serve as a check against the abuse of power by police officers.

***

We’re against pervasive government surveillance, but when cameras primarily serve the function of allowing public monitoring of the government instead of the other way around, we generally support their use 98

Consistent with the position outlined above, the ACLU support for body worn cameras is limited. Certain uses of the cameras are vigorously opposed by the ACLU. As an example, the organization advocates limited officer discretion in activating cameras and deactivating body cameras. It also opposes officer review of body camera images in connection with the preparation of reports. Lengthy retention periods are sought for keeping video images which may evidence police misconduct and relatively short retention periods are advocated for other video images. The ACLU advocates relatively unfettered access for subjects of body camera
video and open public access to video, appropriately redacted to protect the privacy of subjects. The ACLU has offered model legislation for states considering the use of body cameras seeking to codify protective measures.

As states and local jurisdictions in the U.S. grapple with the introduction of body cameras, the approaches vary greatly. Issues like officer discretion in activating and deactivating cameras; retention periods for images; rules for dissemination requirements under local freedom of information or sunshine laws; and provision for redaction to protect privacy receive no uniform treatment. Moreover, the costs attendant on the operation of these systems are left to be borne by local agencies. In some instances, mandated requirements for extended retention, public access to video and redaction to protect privacy have served to compel abandonment of body cameras. In other cases, the cost of these measures has prevented adoption of body camera technology.

The Illinois Officer-Worn Camera Act (IOWCA) under which Chicago operates is an example of a state statute with exacting requirements which have prevented other jurisdictions from adopting body cameras, largely due to cost. The IOWCA did not initially require agencies to utilize body cameras, but did set out requirements for retention and public access in those circumstances where an agency chooses to use cameras. In 2021 the IOWCA was amended to mandate all Illinois municipalities adopt body worn cameras for their officers. This makes Illinois one of seven states mandating body -worn camera use.

The IOWCA also specifies when officers can activate and deactivate cameras and creates an evidentiary presumption against the officer in the event the camera is not properly activated. In 2021, the legislature enacted criminal penalties for officers assigned body cameras, who intentionally fail to follow state mandated provisions for body camera use. Many Illinois police chiefs have indicated the complex statutory provisions governing body camera use have made the implementation of such programs too costly, serving as an impediment to adoption. It is unclear what the effect will be in Illinois from the 2021 changes mandating body cameras and imposing criminal penalties for failure to comply with statutory provisions.

The intersection of body camera use and the application of FR technology demonstrates how the integration of differing technologies can provide opportunities for law enforcement and at the same time raise new privacy concerns. While generally in support of body cameras, the ACLU vigorously opposes the application of FR software to the body camera images. This is consistent with the overall philosophy of the body camera as not so much a law enforcement tool as it is a measure of control over law enforcement. Three states (California, Oregon, and New Hampshire) have enacted legislation prohibiting the use of FR technology to analyze body camera images. In June 2020, federal legislation prohibiting use of FR with body cameras was also proposed. This confluence of two controversial technologies causes further instability in the U.S. legal environment.
South of the Border: Legal and Privacy Underpinnings of Canadian and U.S. Approaches to Police Video Usage | By Shawna Coxon and Don Zoufal

Perspectives About Future Use of Cameras and Analytics

The differing legal protections for privacy explain a great deal about the differing approaches to camera usage and advanced analytics. Both the Canadian and U.S. legal systems offer substantial protections for solitude and intimacy. The protection for reserve is greater in Canada, but the U.S. appears to be moving in that direction. The main difference in legal treatment between the two countries centers around the issue of anonymity.

While Canada embraces anonymity as an important pillar in privacy protection, that concept is not similarly embraced by U.S. jurisprudence. The absence of that protection leaves U.S. law enforcement greater latitude in the use of public area surveillance systems. As analytic capabilities increase particularly with tools like FR and license plate recognition, the ability to maintain anonymity in public space contracts. These tools have been successfully used by law enforcement in places like Chicago. However, the concern about this contraction of anonymity is leading a growing number of jurisdictions to limit law enforcement use, in a manner more like the Canadian approach.

The proliferation of camera technology along with the emergence of analytics is not just a phenomenon particular to law enforcement. The expansion in use of cameras and analytics is becoming commonplace in commerce and social networks as well. These developments may be changing expectations of anonymity. As courts grapple to address protection of this state of privacy, the notions of a diminishing expectation in the preservation of anonymity may well change some of the protections afforded. Conversely it may result in a backlash heightening concerns over preserving anonymity protections.

The pressures of crime and the use of camera technology to combat it as well as the desire to use cameras to ensure greater police accountability are running up against the desire on both sides of the border to protect privacy. The use of body-worn cameras provides a particularly complex challenge for civil rights advocates who seek on one-hand protection from inappropriate police interactions and on the other-hand protection of individual privacy rights. Balancing safety, accountability, and privacy concerns can prove to be a difficult task with no clear path forward.

Only time will tell with respect to changes on either side of the border regarding protections for anonymity, meanwhile law enforcement use of technology will likely continue to proceed down divergent paths. Legal requirements, rather than crime problems or effectiveness of technology tools, are likely the most important drivers that will control use of cameras and analytics in both countries. The fact that technology use is expanding in Canada while some restrictions are being placed in the U.S. suggests that there may be a common ground of privacy protection in the use of surveillance technology in the public space. Understanding the roots of legal differences concerning legal privacy protections may help law enforcement managers make better choices in technology selection and use.
About the Authors

Deputy Shawna Coxon is a senior criminal justice leader with 25 years of policing experience. She is the Deputy Commissioner of Strategy, Governance and Performance of An Garda Síochána (AGS), Ireland’s National Police and Security Service. AGS is responsible for all local and federal police services in Ireland. Deputy Commissioner Coxon is responsible for overseeing An Garda Síochána’s corporate planning process, establishing leadership programmes and ensuring that strategy implementation is achieved in a co-ordinated and integrated fashion across the organization. Prior to this appointment, Shawna Coxon was a Deputy Chief of Police with the Toronto Police Service, responsible for policing in the fourth largest city in North America. As a Deputy Chief of Police, she led three different commands at different times, specifically the Human Resources Command, the Priority Response Command and the Communities and Neighbourhoods’ Command. Deputy Commissioner Coxon has her MA in Criminology from the University of Toronto and her PhD in Criminal Law from Leicester University in the U.K. She has both published and spoken internationally. She has a passion for policing, innovation, technology and futurism. She may be reached at shawna.coxon@garda.ie.

Don Zoufal holds an M.A. in Security Studies through the Center for Homeland Defense and Security at the Naval Postgraduate School. He also holds degrees from the University of Illinois in law (J.D.), public administration (M.P.A.), and history and political science (B.A.). Since 2011, Don has been a Lecturer in the Master of Science in Threat and Response Management Program at the University of Chicago. He also currently works as an independent consultant for CrowZ Nest Consulting, Inc., providing strategic and policy advice on public safety issues and technologies. He previously served in a series of executive level governmental appointments: First Deputy of the Chicago Office of Emergency Management and Communications; Deputy Commissioner for Safety and Security for the Chicago Department of Aviation; General Counsel for the Chicago Police Department; and Chief Legal Counsel for the Illinois Department of Corrections. Don is also a retired Colonel in the U.S. Army Reserve. He may be reached at don@crowznestconsulting.com.

Bibliography

Non-Legal Sources


**Legal Sources**

**Legal Enactments (Canada)**

Canadian Constitution

Criminal Code of Canada


Civil Statutes


**Case Law (Canada)**

Canadian Supreme Court
South of the Border: Legal and Privacy Underpinnings of Canadian and U.S. Approaches to Police Video Usage | By Shawna Coxon and Don Zoufal


Canadian Provincial Courts

British Columbia

Ontario


Saskatchewan

Legal Enactments (United States)

U.S. Constitution
**State Statutes**

**California**  

**Illinois**  


**New Hampshire**  

**Oregon**  

**Local Ordinances**

**Boston, MA**  

**Oakland, CA**  

**Portland, OR**  

**San Francisco, CA**  

**Somerville MA**  
Case Law (United States)

U.S. Supreme Court


Case Law (United Kingdom)
Notes


3. See, the Privacy Act and the Personal Information Protection and Electronic Documents Act.


11. CBC News, “Police to Double Number of CCTV Cameras in Toronto Amid Spike in Shootings.”


15. Ibid.

16. Ibid.

17. Ibid.


24. Ibid.


29. Ibid.


32. Byrne, “Groups Call on Chicago Mayor Lori Lightfoot to Ban City’s Use of Facial Recognition Technology.”


34. Ibid.


37. Ibid.

38. Ibid., 31.

39. Ibid.

40. Ibid.

41. Ibid.

42. Ibid, 32.

43. Ibid.

44. Ibid.


46. Ibid.


50. Ibid, p.159-160.


54. See, e.g., Olmstead v. United States, 277 U.S. 438 (1928), discussed infra.


59. 277 U.S. 438 (1928).

60. 389 U.S. 347 (1967).


63. 392 U.S. 1 (1968). “This inestimable right of personal security belongs as much to the citizen on the streets of our cities as to the homeowner closeted in his study to dispose of his secret affairs. For, as this Court has always recognized, ‘No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.’ “[Citation Omitted] 392 U.S. at 8-9.


65. R. v. Duarte, [1990] 1 S.C.R. 30, para. 8. Note: The consent of one of the participants can be an exemption under specific circumstances.


69. 533 U.S. at 37.

70. 410 U.S. 113 (1973).


74. Ibid.


76. Ibid.


78. 357 U.S. 449 (1957).


81. Ibid.


92. See, e.g., San Francisco, CA (S.F. Admin. Code Ch. 19B), Oakland, CA (* Oakland Mun. Code 9.64.), Somerville, MA (Somerville Ord. No. 2019-16, § 9-25), Boston, MA (Bos. Ord. No. 16-62), and Portland, OR. (City Council Approves Ordinances Banning Use of Facial Recognition Technologies by City of Portland Bureaus and By Private Entities in Public Spaces,) (Sept. 9, 2020), cited at https://static1.squarespace.com/static/5967c18b7f7c50a0244ff42c/t/5f3ad787ba3fd27776e44aaf/1597691785249/Ordinance+to+ban+use+of+FRT+in+Places+of+Public+Accommodation+plus+code+amendment+-Final.pdf.

South of the Border: Legal and Privacy Underpinnings of Canadian and U.S. Approaches to Police Video Usage | By Shawna Coxon and Don Zoufal


98. Ibid., 2.


100. Ibid.


Copyright

Copyright © 2021 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS). Cover photo by Enrique Alarcon on Unsplash.