Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement

Nicholas Koutros and Julien Demers[*]

Despite popular perception of increased government surveillance, particularly since 9/11, a longitudinal study of the Annual Reports on the Use of Electronic Surveillance, published by Public Safety Canada between 1973 and 2011, demonstrates the opposite trend. This article first outlines this decline to situate the use of electronic surveillance by federal law enforcement. The second section of the article advances legal, political, and practical influences which are likely contributing to the diminished use of wiretapping by police. The purpose of this article is to present quantitative evidence to better inform the ongoing debate around extending "lawful access" regimes in Canada. By using official government statistics as a foundation, this article provides a practical grounding to the theoretical academic and legal research that often informs law, legislation and public policy governing the use of surveillance technology.

INTRODUCTION

Although wiretapping had been used as early as the American Civil War, it did not become a serious concern for legislators, the courts, or the public until the Prohibition era in the United States.[1] At that time, as voices replaced Morse code as a public means of communication, wiretapping expanded to be used both for "low" criminal investigations by law enforcement agencies (LEA) to gather evidence and for "high" espionage.[2] By 1928, the relative disinterest of courts in the practice of electronic surveillance reversed following the landmark case of *Olmstead v. United*

---

[*] Nicholas Koutros, MA, Carleton University, with a co-op option in the Policy branch of the Office of the Privacy Commissioner of Canada. He currently works as a privacy and security consultant. Julien Demers is a JD student at the University of Ottawa, French Common Law program, and a former research assistant and event coordinator for the Office of the Privacy Commissioner of Canada. The authors would like to thank Chris Parsons and Chris Soghoian for their review of early drafts of this article. We would like to express particular appreciation to Chris Prince for his guidance and patience during our time at the OPC and beyond.

1 Alderic Jimenez, e.g., *Privacy: An Overview of Federal law Governing Wiretapping and Electronic Eavesdropping* (New York: Nova Science, 2010) at 3-4; David Watt, *Law of Electronic Surveillance in Canada* (Toronto: Carswell, 1979) at 10-11.

2 Susan Landau, *Surveillance or security?: The risks posed by new wiretapping technologies* (Cambridge, Mass: MIT Press, 2010) at 72-73 [Landau]; see also US National Wiretap Commission, *Report on Electronic Surveillance* (Washington, DC: 1976) at 33–38, online: National Criminal Justice Reference Service <https://www.ncjrs.gov/App/publications/Abstract.aspx?id=39007>.

States, which opened the door to expanded use of wiretapping.[3] Fast forward 80 years and society has become ever more reliant on electronic modes of communication. Now, many face-to-face interactions are conducted through the myriad modes of communication available at the click of a button. However, this convenience comes with the corollary of increasing concern over the use of surveillance in the hands of both law enforcement and private enterprise. Yet parliamentarians in Canada have not updated the statutes related to electronic surveillance since the late 1970s.[4]

In the period between the Prohibition of the 1920s and the counter-culture of the 1960s, little was written, and less was said publically, on the issue of electronic surveillance even within civil society.[5] While literary circles became familiar with the spectre of "Big Brother" following George Orwell's novel *1984*, published in 1948, the public interpreted the massive manpower necessary to create the panopticonal country of Oceania as a commentary on autocratic regimes; something that could never come to pass in a democratic state. It was not until the height of the Cold War that "total surveillance" became felt to be a possibility, or indeed a virtual inevitability, by ordinary citizens.[6]

When providing testimony to the United States Senate in 1965, a private investigator demonstrated an audio recorder disguised as a martini olive which cap-

---

3 This case focused on a Seattle bootlegger calling back and forth to Canada in order to smuggle British spirits into Washington State from Vancouver. The US Supreme Court ruled that the Fourth Amendment of the Constitution (forbidding unreasonable search and seizure) did not apply to the use of wiretapping by government investigators because "there was no searching . . . the evidence was secured by the sue of the sense of hearing and that only." *Olmstead v. United States*, 277 U.S. 438 (U.S. Sup. Ct., 1928), online: <http://supreme.justia.com/cases/federal/us/277/438/case.html>[*Olmstead*].

4 Note: In this article the terms "wiretapping" and "electronic surveillance" are often used interchangeably. It should be noted that wiretapping is a specific type of electronic surveillance which involves intercepting circuit-switched telephony for the purpose of surveillance, whereas "electronic surveillance" covers the entire range of interception modes. "Prior to the *Protection of Privacy Act* there was no legislation to regulate and control the use of electronic surveillance devices by law enforcement personnel. In common law eavesdropping was recognized as a nuisance offence." See Norman MacDonald, "Electronic Surveillance in Crime Detection: An Analysis of Canadian Wiretapping Law" (1987)10:3 Dal LJ 142; see also Stanley Cohen, *Invasion of Privacy: Police and Electronic Surveillance in Canada* (Ottawa: Carswell, 1983) at 78 [Cohen]; and, Law Reform Commission of Canada, "Electronic Surveillance," *Working Paper No 47* (1986) at 1–5, online: <http://www.lareau-law.ca/LRCWP47.pdf> [Law Reform Comm of Canada].

5 Cohen, *supra* note 4 at 33.

6 For example, "Electronic devices have come to stay. They have a clear place in our modern life in business and ordinary day-to-day existence. They may be generally divided into 'wiretapping' and 'bugging.'" From Government of British Columbia, *Report of the Commission of Inquiry into Invasion of Privacy* (BC: 1967), online: <http://www.llbc.leg.bc.ca/public/pubdocs/bcdocs_rc/286439/286439_report_com_invasion_privacy.pdf>.

tured the attention of both Senators and television audiences alike.[7] Previously, the public understood that these techniques were confined to the shadowy world of espionage and detective novels. By "bugging" a public space such as Congress, the public began to realise that the technology could be used covertly by anyone and virtually anywhere. In the decade that followed, surveillance powers in the hands of both public and private entities became a perennial concern for many political groups, religious minorities, civil society, privacy scholars, security experts, the courts, and the public at large.[8]

While an established group of researchers in Canada have wrestled with the spread of surveillance technologies and their impact on citizens' legal rights and sense of privacy, little work has been done to analyse actual police use of wiretapping.[9] The purpose of this article is to backstop theoretical work by introducing quantitative evidence to demonstrate how wiretapping is actually being used within Canada. To do this, we have examined open-source data published in Annual Reports to Parliament to analyse the trend of electronic surveillance in Canada from 1973 to 2012 in order to provide a longitudinal analysis of the entire dataset through the past 32 years.[10] It is our intention that these statistics, and the trends which we have extrapolated from them, will encourage a fact-based discussion over the appropriateness and necessity of electronic surveillance techniques in Canada.

At first glance, the trends in the annual reports appear to demonstrate that the use of electronic surveillance by law enforcement agencies (LEA) has been steadily declining. At the same time that many LEAs have publically advocated for an expanded surveillance infrastructure; known in parliamentary vernacular as "lawful access." The second section of this article will explore some of the underlying drivers of why LEAs feel that expanded lawful access is necessary, and why some civil liberties advocates disagree. After outlining some key events that have likely affected the use of electronic surveillance, this article will provide seven theories that we believe to be influencing the trend. The final section will reflect on what we have found by proposing subsequent avenues for research.

---

7 Robert Ellis Smith, *Ben Franklin's Website: Privacy and Curiosity from Plymouth Rock to the Internet*, (Providence: Privacy Journal, 2000) at 167.

8 While there are dozens of examples, the most high-profile of these is the widespread interception in the United States conducted by the National Security Agency (NSA) and other intelligence gathering organizations following the attacks of 11 September 2001. See Andrew P MacArthur, "The NSA Phone Call Database: the problematic acquisition and mining of call records in the United States, Canada, the United Kingdom and Australia" (2007) 17 Duke J Comp & Int'l L 441, online: <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1086&context=djcil>. See also the Electronic Frontier Foundation's complaint, *EFF v. Department of Justice*, Complaint, (30 Aug 2012), Case No 12-01441 (DDC), online: <https://www.eff.org/document/complaint-19>.

9 There have been several noteworthy Canadian researchers working in this area from the vantage point of technology, law and policy.

10 These reports were originally compiled by the Solicitor General of Canada until that office was amalgamated into the Ministry of Public Safety and Emergency Preparedness in 2003. The reports tabled by the Solicitor General are housed within the Library and Archives Canada. Reports tabled by Public Safety may be found online.

The purpose of this article is not to validate or invalidate the necessity for an expanded lawful access regime. Rather, we argue examining the actual usage of electronic surveillance in Canada is essential in light of legislative change, industry research, and governmental investment into expanded surveillance apparatuses; particularly following anti-terrorism initiatives post-9/11. We have found that evidence provided in annual reports is incomplete and is no longer able to encompass the advances in technology. This is alarming because the reports are currently the only avenue for the public to ground any fact-based discussion on the merits and dangers of police surveillance. At the very least, this article will illuminate some of the deficiencies within the existing public reporting scheme and encourage transparency from within the LEAs themselves.

Overall, we expect that no *single* influence is responsible for the decline of electronic surveillance; such a discrete conclusion cannot be drawn without broad, long-term analysis of actual police applications, warrants, and other records that are not open-source. Therefore, this article cannot weigh the impact of any single influence against another on the overall downward trajectory of electronic surveillance because there are simply too many variables that must be accounted for. Rather, we seek to demonstrate that current reporting regimes are inadequate in the contemporary environment because it does not offer any context, analysis, or justification for electronic surveillance as currently practiced in Canada. Until this can be remedied, the onus to justify the need for greater powers must ultimately fall upon LEAs. After all, protections of *Charter* rights — the fundamental basis for the societal protections found in laws restricting surveillance — demand a clear accounting based on publically disclosed qualitative data examined against the context of historical trends; an element that is sorely lacking in contemporary reporting mechanisms.

I. CANADIAN STATISTICS ON ELECTRONIC SURVEILLANCE: OVERALL TREND ANALYSIS

> *Conceptually, it is difficult, some would say impossible, to conceive of privacy as severable from the notion of individual liberty and autonomy. Life, liberty, security of the person and enjoyment of property are only meaningfully guaranteed if privacy is an explicitly guaranteed condition on the grant of such rights.*[11]

In his dissenting opinion in *Olmstead v. United States*, Supreme Court Justice Louis Brandeis predicted, "the progress of science in furnishing the Government with the means of espionage is not likely to stop with wiretapping" and, therefore, "there is no difference between the sealed letter and the private telephone message."[12] The opinion expressed by Justice Brandeis succinctly underlines the overall tone of Canadian surveillance jurisprudence. Simply put, various Canadian statutes and provisions have created an expectation of privacy when using electronic communications which is similar to that of a letter in the mail. Therefore, the power of the government to intercept private communications should always be tempered on the side of caution regardless of the mode in which a communication is sent.

---

11 Cohen, *supra* note 4 at 52.

12 *Olmstead*, *supra* note 3.

This notion is expressed in multiple statutes at a very basic level, particularly in the *Protection of Privacy Act (1974)* which amended the *Criminal Code* to ban individual ownership of surveillance technologies and erected a clear "lawful access" regime for LEAs, (which we will discuss in more detail below). Basically, the *Protection of Privacy Act* sets out a process wherein LEAs are required to first seek *both* ministerial and judicial authorization, in the form of a warrant, in anticipation of intercepting the communications of a suspect.[13] In 1977, the act was amended to require LEAs to provide notification to investigative subjects within 90 days of the date upon which the authorization was issued and to comply with strict court restrictions on how, what, and where suspects may be monitored.[14] Taken together, these two acts constitute Part VI of the *Criminal Code of Canada* which outlines "Invasion of Privacy."

Most significantly for the purposes of this article, the *Protection of Privacy Act* required the Minister of Public Safety and Emergency Preparedness (and previously the Solicitor General of Canada) to "prepare and present to Parliament an Annual Report on the use of electronic surveillance."[15] Federal authorities have filed these reports faithfully each year, beginning with statistics for 1974.[16] The reports set out the length of time surveillance is conducted, describe the crimes being investigated, the location of individuals under surveillance, and precisely how many cases are brought to court (while success in obtaining a conviction is unreported, as we discuss below). The reporting structure, however, does not mandate any examination of historical trends. Although each report displays the data from the previous four years, no long-term review of the figures has been published since the regime was first implemented. The following section seeks to correct this by examining the trends that can be extrapolated when the entire dataset is viewed together. The trends are not presented in any particular order.

---

13 *Criminal Code*, RSC 1985, c. C-46, Part VI, online: Justice Canada <http://laws-lois.justice.gc.ca/eng/acts/C-46/page-87.html#h-61>.

14 Exceptions are made in cases where an investigation is ongoing, involves organized crime or terrorism-related offences. Notification in these investigations is being delayed up to three years.

15 Public reporting was perceived as a key control for limiting surveillance of electronic communications. In the report the Minister must include information such as the number of applications made for authorizations (judicial warrant) and for renewal of authorizations. See Ministry of Public Safety and Emergency Preparedness, *Annual Report on the use of electronic surveillance*, (Ottawa: Public Safety Canada), online: <http://www.publicsafety.gc.ca/abt/dpr/index-eng.aspx>.

16 Although the 1977 amendments to the *Protection of Privacy Act* have not been modified in the past 35 years, compiling statistics based on the reports has proven to be extremely challenging. Although many of these statistics change significantly in each successive year, for the sake of clarity and consistency we included only the number reported the final time — generally in the report four years later (i.e., the number we use to report 2006 is found in the report for 2010). While we do not believe that this will significantly alter the overall trend, it is important for observers to recognize the source of our numbers. Overall this contributes to a perception that the methodology has not yet been standardized and that it remains difficult to collect quantifiable data to make sound policy choices.

(a) Trend One: Overall Court Authorizations

Prior to starting any electronic surveillance operation, LEAs are compelled to seek a warrant from the court. Each of these is recorded and filed with the Minister of Public Safety who, in turn, is required by the *Criminal Code* to provide Parliament with statistics annually in the interest of public transparency. By examining the total number of court authorizations issued per year over time, Figure 1 (below) clearly demonstrates that the number of court authorizations granted for electronic surveillance has steadily declined since reporting began in 1974.[17]

At the peak in 1976, roughly 1300 warrants for electronic surveillance were issued; however, by 2011 the reported number of authorizations dwindled to a mere 116, a decrease of nearly eleven-fold. Indeed, the last year in which more than 200 federal court authorizations were issued was 1996, with a record low of 108 in 2010. These figures include audio and video interception, emergency authorizations, and cases where LEAs have been granted a time renewal to continue surveillance under an existing warrant. Therefore, counting the number of authorizations granted by the court provides a useful baseline statistic because it is the basic element common to all types of electronic surveillance outlined in Part VI of the *Criminal Code*.

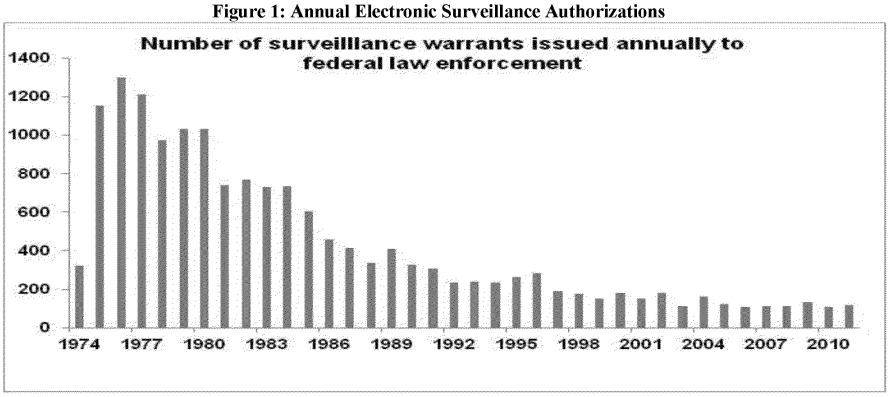
Below we will discuss theories based on various historical, social, and technological developments as to why this decline may have occurred. If reporting methodology is assumed to have remained consistent since 1974, the negative trend observed below in Figure 1 is noteworthy on its own. As with any longitudinal statistics, changes in reporting methodology within organizations over the thirty-seven-year period may have impacted data consistency. That said, at first glance, it would seem that Canada stands apart from many other jurisdictions globally where reporting shows use of electronic surveillance is clearly on the rise.[18] We believe that legislative developments, bureaucratic policies, jurisprudence, and an evolving social environment have exerted downward pressure on the use of surveillance. However, this trend-line in isolation is not sufficient evidence to conclude that the use of electronic surveillance is declining, and we will discuss why further below.

---

17 Solicitor General of Canada, *Annual Report on the use of electronic surveillance*, [28 Volumes] (Ottawa: Library and Archives Canada).

18 United Nations Office on Drugs and Crime, *Current Practices in Electronic Surveillance* (New York: United Nations, 2009)

Figure 1: Annual Electronic Surveillance Authorizations



(b) Trend Two: Individual Notifications

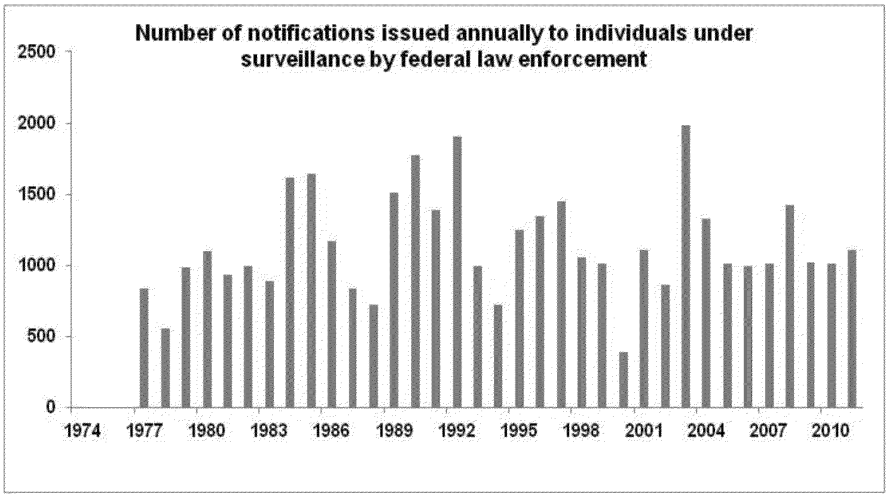
Notification was included in the *Protection of Privacy Act* by amendments in 1977 to reassure the public that innocent suspects would be informed if they happened to be subject to an unsuccessful investigation through written notice mailed to these individuals. To date, close to 40,000 such notices have been issued at an average rate of 1140 notifications per year (see Figure 2 below). The obvious question raised by these figures is their inconsistency with Figure 1, which notes the number of annual authorizations. Taking 2006 as an example, only 106 surveillance warrants were issued; yet a total of 996 individuals were notified they were under surveillance in that year. Clearly, there is an incongruity between Figure 1 and 2 that must be explained.

To resolve this disparity, several points within the 1977 amendments are crucial to note. First, notification may be delayed up to three years if: (a) the investigation is still ongoing after the authorization has concluded; (b) the investigation is related to either terrorism or organized crime; or (c) a judge views the extension to be in the interests of justice. In other words, notifications connected to these crimes often come long after the fact.[19] Ultimately, a "ripple effect" should be observable because all individuals under surveillance must be notified at most three years later. When the total number of authorizations in Figure 1 is compared with the total number of notifications in Figure 2, these figures differ significantly.

---

19 For example, note the absence of notifications in the year 2001despite widespread fears concerning terrorism, as compared to the spike in notifications three years after in 2003.

Figure 2: Annual Individual Notifications of Surveillance[20]



Despite this inconsistency, Figure 2 is valuable as it demonstrates that, while the courts are issuing fewer warrants for electronic surveillance, investigators are listing more individuals as targets under each authorization sought. To be clear, in 1995 a single typical court authorization allowed wiretapping thirty separate individuals. In other words, it is crucial to note the disconnect between any total statistic for warrants issued as compared to overall persons identified and affected by surveillance. Unfortunately, 1995 was the final year that the number of individuals named in an authorization was included in the Annual Reports prepared for Parliament and the statistic vanished without explanation in 1996.[21] Without this data, it is impossible to know for certain how many individuals named in the authorization were ultimately notified that they were mistakenly surveilled. Further, it means that it is virtually impossible to determine whether the decrease in authorizations sought by federal LEAs is simply a function of having more suspects named on each authorization or whether LEAs are steering away from electronic surveillance as a whole.

---

20 Note: The notification requirement did not begin until 1977 amendments to the *Protection of Privacy Act*.

21 No particular explanation is provided in subsequent years why the reporting structure and level of detail was altered, although numerous commentators have highlighted the general opaqueness of the figures provided in the Annual Reports produced for electronic surveillance. See for example Cohen, *supra* note 4 at 21-218; Louise Savage, "An analysis of the federal and provincial Annual Reports relating to the use of court authorized electronic surveillance by law enforcement officials in Canada" cited in Law Reform Commission of Canada, *supra* note 4 at 10; Department of Justice Canada, *Report of the Canadian Committee on Corrections — Toward Unity: Criminal Justice and Corrections* (Ottawa: Department of Justice Canada, 1969) at 85, 87, online: <http://www.lareau-legal.ca/CCCorrectionsPart1.pdf>.

(c) Trend Three: Types of Crimes Targeted with Electronic Surveillance

A critical and often overlooked point central to any discussion of surveillance law or the privacy risks of new monitoring technologies is that it is neither legal nor practical for authorities to investigate all types of crime using electronic surveillance. Interception of communications is an extremely complex operation requiring strict evidentiary processes, technical expertise, operational supports, and significant resource investment by LEAs and their partners.

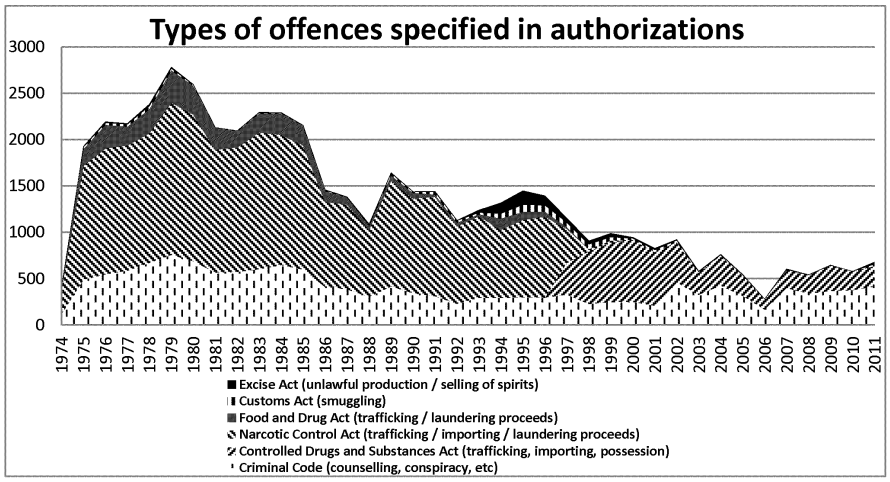
Until 2002, the overwhelming focus of federal court authorizations for wiretapping involved the smuggling, production, and distribution of narcotics, precursors, and other illicit items — likely because statutes such as the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* [2000] and others allows for assets seized by police to be used to subsidize the cost of the investigation. Figure 3 reinforces this theory. Crimes customarily associated with wiretapping, such as terrorism and espionage, are typically used by legislators to justify expanded lawful access regimes yet barely register when directly compared to federal LEA's focus on contraventions of the *Narcotic Control Act*.

However, when that statute was replaced in 1997 with the *Controlled Drugs and Substances Act*, warrant applications related to trafficking, importing and possession never recovered due to changes found in the regulatory framework of the legislation, which compelled LEAs to modify the way they approached such investigations. Four years after this act was promulgated, the reported data demonstrates that broader *Criminal Code* offences (like murder, extortion and money laundering) overtook drug investigations in federal court authorizations for wiretapping for the first time. As a result, it is increasingly difficult to generalize about the nature of criminal activity being targeted through electronic surveillance because a broad range of *Criminal Code* offences have recently emerged in the data. However, it should be noted that electronic surveillance is likely still primarily used for investigating drug-related crime since any number of *Criminal Code* offences specified in the report are usually used to charge members of organized crime or criminal gangs who are suspected of drug trafficking. Broadly speaking, Figure 3 underscores a long-standing assertion by police that electronic surveillance is used primarily to gather evidence in drug-trafficking and organized crime offences, but this dynamic clearly evolved after the 1997 *Controlled Drugs and Substances Act*.

The most disconcerting element of this particular trend is what was *not* found in this section of Public Safety Canada's annual reports. Generally, these reports contain very little discussion or analysis — typically only a single page for "general assessment" at the beginning of each section. Since 1999, however, the report signed by the Minister of Public Safety has recycled the exact same wording in many sections of the report. No mention is made of effectiveness, legal problems, resource demands, or administrative hurdles and there is no compelling discussion of the importance of interception of private communications for the investigation, detection, prevention and prosecution of offences as frequently reiterated by LEAs arguing for lawful access legislation. Legislators granted invasive powers in Part VI of the *Criminal Code* on the understanding they would be kept up-to-date and informed. However, one suspects they were not anticipating that the reporting authority would cut and paste the content year after year. In this regard, the reports

point more to degradation in the overarching system of accountability, rather than any clear decline in surveillance.

Figure 3: Types of Offences Targeted With Electronic Surveillance



(d) Trend Four: Locations of Electronic Surveillance

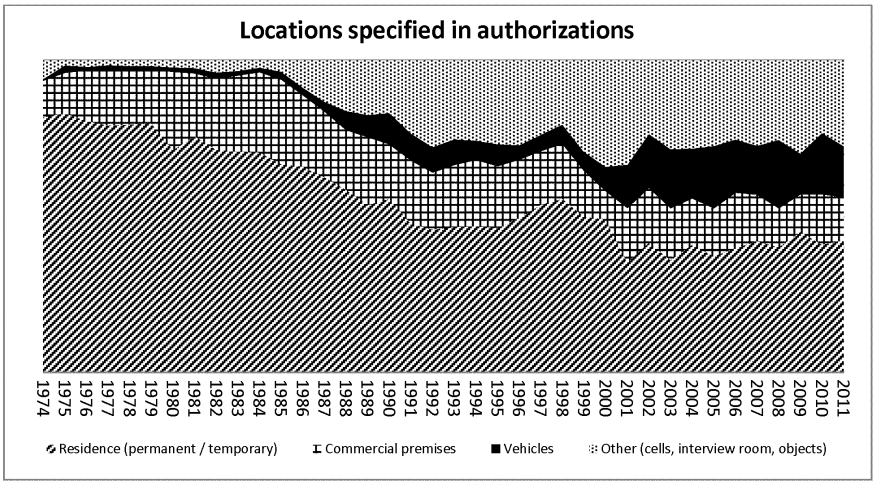
The issue of how a wiretap or surveillance device is placed, who is targeted, and where the actual interception occurs raises substantive legal issues. These set the parameters of an investigation and, in practice, govern what controls and limits the court imposes as investigators undertake their surveillance, how the evidence gathered may be treated in court, and may even prompt a judge to refuse the warrant application outright; even though statistics demonstrating the number of denied warrant applications are not publically available. After all, under Canadian law, private communications can occur anywhere — on street-corners or in cars, in homes or over phones. Accordingly, courts at all levels have the power to shape surveillance practices dramatically.

The legal aspects of intercepting private communications will be discussed in greater detail in the second half of this article, but using location as an analytical lens can be demonstrative of this trend (see Figure 4). For example, the bugging of detention cells, police interview rooms, or covert recording using an informant or undercover investigator (i.e., "wearing a wire") was a common practice in the 1970s and 1980s. After 1990, owing to the court ruling on *R. v. Duarte* (which we discuss below), these activities required a court authorization.

An increasing canon of surveillance related jurisprudence, coupled with changes in how Canadians communicate electronically, likely explains the growth of the "other" category in Figure 4. Beside this, the two obvious trends to note are the relative decline in residential phone lines or premises being put under surveillance and the increase in the number of vehicles being targeted. In 1974, 82 percent of all authorizations targeted individual residences. By 2010, this dropped to 42 percent. By contrast, a single authorization was sought to target a vehicle in 1974,

whereas over the past decade, roughly 20 percent of authorizations have specifically listed vehicles as targets of surveillance.[22]

Figure 4: Location of Authorizations



(e) Trend Five: Organizations Conducting Electronic Surveillance

Another crucial caveat in this discussion is that the statistics compiled for the federal annual reports only represent a narrow slice of the overall electronic surveillance conducted by Canadian authorities. Due to separate statutory mandates and jurisdictions, as well as varied reporting and oversight parameters, it is impossible to present a conclusive statistical account of electronic surveillance across all levels of government. As an instructive example, however, it may be useful to explore how changes in the mandate of just one organization affected the surveillance operations and reporting of another. In the federal context, this is best demonstrated by the rupture of the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) — the former being responsible for criminal investigations and the latter responsible for intelligence gathering. In practice their mandates have historically overlapped to a great extent.

In 1984, CSIS was created by extracting the mandate of the RCMP's Security Service and placing it within the ambit of a civilian body. Along with the personnel who staffed the Security Service divisions went many of the long-standing investi-

---

22 Recent research by Christopher Soghoian seems to indicate that 95 percent of all wiretap authorizations in the US are now being directed at mobile objects such as cellular telephones and automobiles. Canada, with similar market penetration for mobile devices, does not appear to be mirroring this trend although "basket clauses" in warrant applications may be inserted by authorities to cover off monitoring of secondary lines and cellular phones. In these cases it may not be readily apparent in the authorization precisely how the warrant is executed by the LEA and may not, therefore, always be at the forefront of the authorization. See Cohen, *supra* note 4, at 144–147; Law Reform Commission of Canada, *supra* note 4 at 39–42.

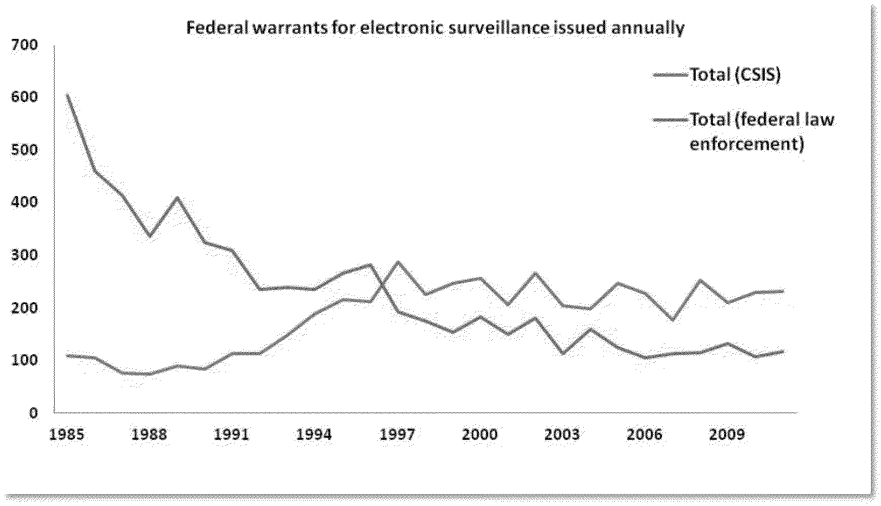
gation activities of the RCMP, a good number of which hinged upon wiretapping and other forms of electronic surveillance. Figure 5 (below) shows how, after 1985, these court-authorized interceptions shifted from the reporting requirements listed under Part VI of the *Criminal Code* to those set out in the *CSIS Act* and subsequently detailed in the Annual Reports of the Security and Intelligence Review Committee (SIRC). When the trend lines are compared, the total number of warrants sought by the RCMP fell considerably, only to be countered by an increase in warrants sought by CSIS; as can be seen in Figure 5 below. From 1984 to 1988, the number of authorizations sought by federal LEAs dropped to almost half previous levels, from 573 to 287 warrants.[23] The balancing trend at CSIS did not decrease as dramatically as the RCMP. CSIS now operates under an average of 231 court authorizations to intercept each year, in comparison to the RCMP and its federal partners which obtain only 141 authorizations to intercept annually.

Drawing a correlation between the decline in RCMP warrants and subsequent rise of CSIS investigations is problematic because a number of other variables have no doubt affected the figures. These might include the easing of tensions in the Cold War, difficulty in justifying some ongoing investigations, or a more narrow reading of reporting requirements in national security cases. However, these are little more than educated guesses. Penetrating the opacity of CSIS is extraordinarily difficult simply due to the nature of its mandate. Any researcher attempting to explore these issues should be warned that, as with most national security organizations, it is very difficult to gather much statistical data or first-hand explication on "sources and methods" without first obtaining a security clearance, which in turn prohibits public dissemination of the information. We must concede, therefore, that it is entirely possible that no line of correlation (or causation) can be drawn between the RCMP and CSIS when it comes to the use of electronic surveillance.

---

23 "In 1983, the last full year in which warrants were issued under the *Official Secrets Act*, the Solicitor General approved 525 warrants. The average length of time a warrant remained in force was 253 days. However, a direct comparison of warrants issued under the two statutes is not possible because of differences between them. Under the *Official Secrets Act*, in general, each warrant authorized the use of only one covert technique, such as a wiretap, against one target . . . Under the new Act [the *CSIS Act*], however, one warrant can authorize the use of many devices against many targets": Security Intelligence Review Committee, *Annual Report* (Ottawa: SIRC, 1986) at 18-19, online: <http://www.sirc-csars.gc.ca/pdfs/ar_1985-1986-eng.pdf>.

Figure 5: Electronic Surveillance Warrants by Organizations



(f) Trend Six: Methods of Surveillance

As noted above, it is important to view the statistics presented here with caution and attention to the limitations of reporting as currently structured. The drawbacks of the current data elements required to be reported under Part VI of the *Criminal Code* will be discussed in further detail below. For the moment, we will use a single example of how the data presented in Canada on electronic surveillance might be widely misread.

At first glance — and as noted previously — a casual observer might examine the total number of warrants issued in Figure 1 for electronic surveillance and immediately note the overall downward trend as an indication that police are using electronic surveillance less. Depending on the orientation of the user, this may be interpreted as an indication that Part VI is so restrictive that investigators are no longer even trying to use the technique. Alternatively, this may indicate that all is well with the control regime we have for interception of communications in Canada. With all indicators down, privacy protective legislation must be keeping LEAs within reasonable limits.

However, the premise of both of these arguments is flawed because they are both based on the assumption that the reporting requirements fully encompass the tools available to LEAs. Unfortunately, the assumptions made by the original legislators about what can and cannot be intercepted; what qualifies as private communications in the global context; the number of people who can be listed on an authorization; and even the definition of intercept itself (as we discuss below) no longer hold true in the contemporary environment.

Basing reporting requirements on invalid assumptions may be concealing a much more concerning trend. As reports from the previous Solicitor General of Canada plainly demonstrated, just a single warrant for interception in 1995 could involve the targeting of thirty separate suspects. Furthermore, a single interception device planted under the authority of that single warrant might gather hundreds of hours of private conversations, including innocent civilians on the other end of the

line, which are not named in the authorization and are never notified they have been surveilled. The 1995 report was a watershed in many ways and remains a useful reference. It was the last report detailing total hours of intercepted communications (156,627 hours). It is also the last year a detailed discussion was set out regarding the usefulness of wiretapping in investigating and detecting crime. Finally, it was the last year that concrete details on drug seizures and their street value was provided. After 1996 these points vanish from the report, never to resurface.[24] Therefore, we must caveat all of our findings and analysis with the disclaimer that is very difficult to draw any kind of positive correlation in support of any argument for or against lawful access infrastructure due to the incomplete evidence provided in the annual reports.

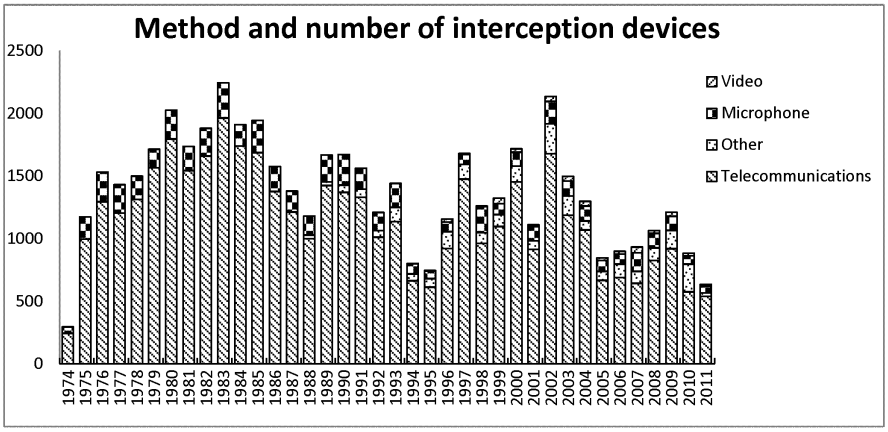
All qualifications aside, some clear patterns have emerged over the 38 years for which we have data on electronic surveillance in Canada. Firstly, there is the overwhelming use of the phone tap, with more than 80 percent of all authorized interceptions taking place using this technique (Figure 7). Microphone "bugs" — whether installed in buildings, vehicles or worn on persons — are expensive and risk discovery, and are only used in roughly one authorization out of ten. Use of audio-video surveillance (requiring a separate form of warrant under section 487.01 of the *Criminal Code*) only became a separate category for reporting methods of surveillance in 1994 and remains rarely used despite reductions in the size, cost, and power of micro-cameras, networking, and storage.

Further, as we discuss below, these reports do not take into account the role of third-party administrators in electronic surveillance such as telephone and internet service providers. The technological underpinnings of communications infrastructure have fundamentally changed in the past two decades, forcing investigators to adapt their means of interception. However, surveillance powers as set out in law were largely predicated on the assumption LEAs themselves would be personally monitoring communications through a circuit-switched communications infrastructure. Since the 1970s, the vast majority of telecommunications are conducted through packet-switched networks and private telecommunications service providers (TSPs) are often wholly responsible for administering these orders and turning over evidence that they collect to LEAs, typically in real-time. Although new technologies now provide alternatives to direct surveillance, reporting requirements have yet to incorporate this change and therefore likely only capture the small percentage of overall volume of electronic surveillance in Canada which does not involve the TSP in some capacity.

---

24 Solicitor General of Canada, *supra* note 17 — as required by section 195(1) of the *Criminal Code*.

Figure 6: Methods of Surveillance Techniques

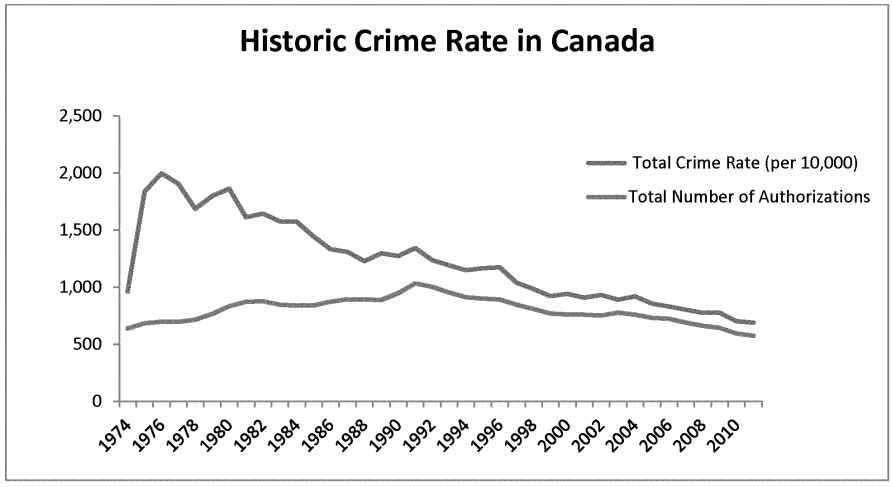


(g) Trend Seven: Declining Crime Rates, Costs and Conviction Rates

Intuitively, an obvious explanation to explore for a decline in use of wiretapping would be the aggregate decline in the crime rate across Canada. Indeed, at a superficial level, there does appear to be some correlation (see Figure 6 below) in that the general trajectory of national crime rates corresponds approximately to a similar decrease in the total number of wiretap authorizations issued. After all, given that: a) lawful electronic surveillance under the *Criminal Code* requires that police demonstrate that crime of certain severity is being investigated; b) that an impartial judge must be convinced that evidence of that crime will be captured with the surveillance measure; and c) the overall crime is falling, then it should come as no surprise that LEAs do not need to use this invasive tool as frequently as in the past.

Continuing with that logic, falling rates of crime (particularly serious crime) mean fewer overall warrants for wiretapping are likely to be approved by senior officials within investigative agencies or applications filed with the courts. While review of provincial wiretap data may point to counter-trends (which is outside of the scope of this article), we suspect overall downward pressure to be evident at all levels of policing. Examination of the use of wiretapping at the provincial and local level is yet another area unexplored by public research at this time.

Figure 7: Annual Authorizations vs. Historic Crime Rate[25]



A close look at available data on police-reported crime, however, provides a counter-point to this theory. As many police organizations assert, the total volume of reported crimes is actually about the same today as it was in the early 1980s; same number of burglaries, same number of domestic disputes, and so forth. What has changed is the total population and demographics of Canada. Without going into a lengthy digression on this point, which is better suited to criminology reviews, we would highlight one telling indicator. By our estimate, in 1980 there was a single wiretap authorization issued for every 2,000 reported crimes. In comparison, a wiretap warrant is issued for roughly one out of 19,000 reported crimes in 2010. Clearly, this type of surveillance has fallen out of fashion in the LEA community. In the next part of the article, we will explore reasons why this might be the case.

25 Crime rate trend line from: Statistics Canada, *Police-reported crime statistics in Canada* (2010), online: <http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11523/c-g/desc/desc01-eng.htm>.

II. INFLUENCE OF THE JUDICIARY (LEGAL CHALLENGES AND COURT RESPONSES)

(a) Theory One: The Protection of Privacy Act (1974)[26]

> *The crucial question to be addressed is ever when and in what circumstances will we allow police to resort to intrusive powers . . . the intrusions of the police must be structured, confined and checked within a regime which is compatible with the demands of the Rule of Law. Intrusions should not be legitimated which fall outside of a sequence of crime and investigation.*[27]

The first group of factors which may be exerting pressure on the use of wiretapping are the legal constraints established by federal legislation designed to protect civil liberties.[28] As discussed in the section above, the *Protection of Privacy Act (1974)* can be viewed as the foundation for the lawful access regime in Part VI and therefore acts as the catalyst for the tension between law enforcement and civil rights advocates. It represented the first attempt by the legislature to regulate the interception of private communications by LEAs. Further, it declared all forms of electronic eavesdropping illegal, with the exception of national-security operations and wiretaps authorized by a superior-court judge, and established a full reporting system for police compliance (i.e., Annual Reports). At the same time, the need for this tool became increasingly important for law enforcement as it shifted its focus in the early 1970s from street-level policing to intricate investigations into organized crime.

When the *Protection of Privacy Act* was first debated in 1972, the Commissioner of the RCMP Joseph Carriere condemned the bill stating that it would, "virtually wipe out the criminal investigation system and organized crime would not only flourish but be virtually free of any barriers."[29] Even after the bill was passed, the RCMP continued to bristle under the yoke of the requirements under section VI of the *Criminal Code*. Two years later, Bill C-176 went before Parliament to balance what the law enforcement community considered to be unnecessarily cumbersome requirements.[30] The amendments to the *Protection of Privacy Act* would increase the range of targets permissible under the *Criminal Code*, but imposed strict reporting requirements to "notify persons under surveillance 90 days after the in-

---

26 *Protection of Privacy Act*, SC 1973-74, c. 50.

27 Cohen, *supra* note 4 at 28.

28 Referring to reported data, the use of electronic surveillance rises during the 1970s, although this does not necessarily mean that the Act of 1974 was ineffective in constraining traditional police wiretapping procedures. In fact, the law enforcement community in Canada acknowledged from the outset that this legislation would represent a significant burden in their investigation procedures.

29 See Greg Marquis, *Policing Canada's Century: A History of the Canadian Association of Chiefs of Police* (Toronto: University of Toronto Press, 1993) at 332 [Marquis].

30 Bill C-176, 1st Sess, 29th Parl, 1973.

stallation of listening devices"; sparking further tension between LEAs and civil liberty advocates.[31]

According to Dr. Greg Marquis, a historian of Canadian policing and criminal justice, the Act "hamstrung the police [because] mandatory notification jeopardized long-term intelligence operations" even more than the original act by exposing police informers and allowing suspects to destroy evidence by informing them of the investigation.[32] Although the intention was to ensure a degree of accountability and transparency by creating an expectation among Canadians that they would be informed if their actions were being monitored, LEAs bristled at what they considered to be an unreasonable burden. Even today, the RCMP and its partners continue to reiterate the same arguments formed in the early 1970s that the accountability mechanisms within lawful access provisions in Part VI would make it difficult for police to respond to crime and follow up investigative leads.

At the same time, the RCMP became intensely focused on bringing down organized crime by focusing on the leaders.[33] Marquis notes that "the 1974 restrictions had severely handicapped the prosecution of professional criminals. Although authorized taps had resulted in the arrest of more than 1,200 persons in 1975, these had included few untouchables of organized crime."[34] The RCMP, having operated within the parameters set out in the *Protection of Privacy Act* for two years, claimed that the Act itself had already hindered many investigations. To introduce a firm 90-day notification requirement on top of this would not provide LEAs with sufficient time to gather evidence to prosecute the leadership of complex criminal outfits. However, critics at the time argued that the prosecutions had failed because the leadership of organized crime had outmaneuvered the RCMP at every turn and expanded electronic surveillance would only be effective in catching those who could likely be arrested through other means.[35]

Subsequently, "the panic over organized crime allowed the Liberal government to extend the scope of electronic surveillance" by restricting some of the provisions in the 1974 Act.[36] By 1976, the original 1974 Act was felt to be an impediment to gathering criminal intelligence to bring legitimate criminals to justice.[37]

---

31 *Ibid.* at 334.

32 Marquis admits that the immediate impact of the *Protection of Privacy Act (1974)* is difficult to reconstruct. Other experts on the history of policing in Canada argue that the new law did not severely hinder police business as they understood the bill to simply be a "bureaucratic nuisance." Based on the rapid increase in the number of interceptions collected immediately after the bill was passed, it appears that this latter approach is more likely. This may be the result of a perception in the minds of LEAs at the time that evidence gathered within the parameters set out in the *Act* implicitly grants *carte blanche* for admission into court, regardless of the spirit of the law. However, as we discuss in later sections, this perception changed following the landmark ruling in *R. v. Duarte*.

33 Marquis, *supra* note 29 at 334-335.

34 *Ibid.* at 334.

35 *Ibid.* at 334.

36 *Ibid.* at 355.

37 *Ibid.* at 353.

Bill C-51 (1977) amended Part VI of the *Criminal Code* by extending the 90-day notification to three years in addition to relaxing a number of the other provisions found elsewhere in the *Protection of Privacy Act*.

Despite having little to do with organized crime specifically, the 1977 amendment "listed a variety of offences for which wire-taps could be authorized, including treason, high-jacking, bribery, perjury, fraud upon government, rape, murder, kidnapping, extortion, counterfeiting, and trafficking."[38] Consequently, the 1977 amendments had weakened the notice requirements while at the same time expanded the range of potential wiretapping targets. Nonetheless, the statutes enacted in the 1970s reflected the Canadian public's concern over the use of the surveillance technologies and Parliament responded by enacting a statutory framework which strictly defined how, when, and why LEAs could use electronic surveillance.

(b) Theory Two: The Canadian Charter of Rights and Freedoms (1982)

> *It is for the individual to decide what persons or groups he or she will associate with, what books he or she will read and so on. One does not have to look far in history to find examples of how the mere possibility of the intervention of the eyes and ears of the state can undermine the security and confidence that are essential to the meaningful exercise of the right to make such choices*.[39]

The introduction of the *Canadian Charter of Rights and Freedoms* into Canada's constitutional framework shook "the very foundations of investigation, arrest and prosecution procedures."[40] From 1960 to 1982, Canadian civil liberties had been nominally protected through the *Canadian Bill of Rights*, but these provisions had offered only partial safeguards. There was no mention of privacy or even of unreasonable search and seizure. By protecting civil rights and freedoms within the constitution itself "[t]he new order [. . .] would make the 1980s a challenging era for Canada's police community."[41]

Section 8 of the *Charter*, which enshrines the right of individuals "to be secure against unreasonable search or seizure," complicated investigations using electronic

---

38 *Ibid.* at p. 336. It is difficult to cite the growing public awareness of organized crime as the singular driver of bills such as C-51 and the 1974 *Protection of Privacy Act*. Rather, the data in Table 3 demonstrates that electronic surveillance is most commonly used for enforcing the *Narcotic Control Act* in conjunction with *Criminal Code* offences such as Trafficking (ss. 5(1), Possession of property obtained by crime (s. 354), Conspiracy (s. 465), and Commissioner of an offence for a criminal organization (s. 467.11). Most often, these are charges which are only levied against members of organized crime outfits. Although this does not prove causation, it is important to note that electronic surveillance is most often used to combat organized crime. In effect, the RCMP used this to argue that a decline in the use of electronic surveillance would reduce the deterrent effect and therefore increase the volume of organized crime.

39 *Thomson Newspapers Ltd. v. Canada (Director of Investigation & Research)*, [1990] 1 S.C.R. 425 at 141, La Forest J, online: <http://scc.lexum.org/en/1990/1990scr1-425/1990scr1-425.html>.

40 Marquis, *supra* note 29 at 377.

41 *Ibid.*

surveillance.[42] Unlike other rights, which are absolute, Section 8 implies that law enforcement must exercise judgement in determining what is "reasonable" prior to executing a search. Lawyers within LEAs are forced to weigh the reasonableness of the request before submitting it to the court. This significantly altered the legal landscape and meant that senior officials and counsel who were reviewing requests to conduct surveillance had to be more cautious and judicious in their approval of invasive searches because failure to prove reasonableness may result in the entire case being dismissed due to a *Charter* violation during the course of the investigation.

It would be several years after the introduction of the *Charter* that the intricacies of surveillance law would be subject to detailed judicial scrutiny by the Supreme Court of Canada (SCC). In *R. v. Duarte*, Mr. Duarte was apprehended by the Toronto Police after discussing a narcotics deal with an undercover police officer. He argued that the Toronto Police had obtained this evidence illegally by using a police informant to bypass the warrant application process.[43] As the *Protection of Privacy Act* was originally written, section 184(2)(a) provided an exemption which did not compel LEAs to obtain a warrant if "a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it."[44] However, the defendant claimed that surreptitious recording of a private conversation without a warrant had violated his Section 8 right against unreasonable search and seizure even though the police had acted within the bounds of the *Criminal Code*. The case served as a critical precedent in surveillance jurisprudence in Canada because it reinforced the interpretation that the unreasonable test requiring a court authorized warrant regardless of the strict wording of the statutes.[45] In considering *Duarte*, Supreme Court Justices were forced to weigh the constraints of Part VI of the *Criminal Code* provisions against the new expectations found within the *Charter*.

The SCC declared that gathered evidence as the result of an unreasonable search was not admissible into court even if it strictly abides by Part VI of the *Criminal Code*. At a broader level, *R. v. Duarte* demonstrated that LEAs must act according to the spirit of the *Charter*, rather than the strict letter of any single statute. Implicitly, this imposed self-regulation on the part of investigating officers because it compelled them to consider whether their search would be unreasonable even if it was still within the parameters of Part VI of the *Criminal Code*. Now, the

---

42 Interestingly, while counter-intuitive and difficult to verify decades later, section 8 of the *Charter* may have actually driven the rise in lawful wiretapping authorizations observed in Figure 1. The *Charter* may have discouraged the police in their reliance on wiretapping, but realizing this increased scrutiny may have prompted police to apply for more wiretap warrants so as not to put existing cases in jeopardy of being thrown out at trial.

43 *R. v. Sanelli*, *(*sub nom. *R. v. Duarte)* [1990] 1 S.C.R. 30.

44 *Criminal Code*, *supra* note 13, s. 184(2)(a)). The one party consent exception to the rule against interception was even upheld in the case of *R. v. Cremascoli*, *(*sub nom. *R. v. Goldman)* [1980] 1 S.C.R. 976, online: <http://scc.lexum.org/en/1979/1980scr1-976/1980scr1-976.html>.

45 Ian J McKinnon, "Recent Decisions from the Supreme Court of Canada Relating to Electronic Surveillance" (1992) 50:2 The Advocate at 211–213.

interpretation of section 184 indicates that court involvement must be in anticipation of the surveillance unless the officer can demonstrate that it is necessary during an emergency. This requirement cannot be waived if one of the parties consent to the search.[46] Even today, *R. v. Duarte* serves as the critical precedent for weighing the test of "reasonableness" in reference to Section 8 of the *Charter*.

(i) Influence of Parliament (Legislative Change and Demands for Reform)

> *Judicial routines and legal rules make up the cornerstone of due process and the rule of law — they are the central building blocks of a free and democratic society . . . the objective should be establishing an optimal balance between security and liberty . . . the executive branch may be the appropriate branch for developing security measures, but that does not make it the most adept branch at establishing a balance between security and liberty.*[47]

The second major influence which may be the widespread use of wiretapping originates from Parliament. Generally, lawful access legislation is intentionally vague and focused on limiting electronic surveillance of those suspected of being involved in serious crimes.[48] However, the political orientation of the governing party has very little to do with the introduction of expanded lawful access regimes to the House of Commons. Both Liberal and Conservative governments have put forward these bills because of the high profile of the Public Safety portfolio, especially following 9/11. Conversely, both parties are quick to criticize the ruling government's policies on lawful access when sitting in opposition.

---

46 It should be noted, however, that the common thread between *R. v. Duarte* and other section 8 precedents was the presence of Justice La Forest as a Supreme Court judge from 1985 to 1997. Although it falls outside of the scope of this article, and expertise of the authors, to analyze the degree of privacy activism on the part of the court, it is clear that the jurisprudence established in the 1980s and 1990s has done much to assert the authority of Canadian law over LEAs, especially at the federal level. However, it is nearly impossible to trace the ripple effects of high court decisions to correlate trends in electronic surveillance. Rather, it may be sufficient to say that cases such as *R. v. Duarte* and others have bolstered the strong positions taken by privacy advocates both within government and in civil society due in large part to the strong opinions of Justice La Forest on the issue.

47 Daniel J Solove, *Nothing to hide: the false trade-off between privacy and security* (New Haven: Yale University Press, 2011) at 50.

48 Careful scrutiny of new investigative powers through parliamentary committees and increasing awareness through highly visible federal and provincial privacy commissioners may also have prevented function creep so effectively that the benefits of using surveillance outweighs the potential consequence for its misuse. Generally speaking, the political spectrum has little impact upon proposals for lawful access legislation as various governments have attempted to introduce expanded powers, to uniformly negative response. At the same time it is clear that pro-privacy advocacy groups and wider civil society have been instrumental in mobilizing public opposition to these proposals, making parties think twice before proposing surveillance bills. This trend may be most recently observed in the demise of Bill C-30 (41-1).

In tandem with broader discussions around the Constitution and *Charter*, the early 1980s were also a period in Canada where concrete revelations finally came to light through the MacDonald Commission of Inquiry into how surveillance powers and legal authorities had been abused by police at all levels.[49] Following the final report and recommendations of that federal inquiry, Members of Parliament and the public demanded that federal authorities be placed under greater scrutiny and that authorities' use of invasive investigative powers be better regulated. This created a cascading effect that resulted in internal policy memos, directives from the Minister's office, self-regulation by policing lobby groups, and even a number of back-bencher bills. Although these latter measures have never yet passed through the House, these bills are often used by opposition MPs to attack government policies while they are being studied in Committee. The most famous example of this followed the 1970 October Crisis in Montreal.

(c) Theory Three: the Creation of CSIS in 1984

Public allegations regarding the extra-legal activities of the RCMP first appeared in the media in 1972. Initially, mainstream coverage was limited and the response of government tepid because the allegations had been levied by a niche Québécois separatist newspaper, which itself had been under surveillance following the October Crisis. By 1978 the Provincial Government of Quebec itself became completely mired in a legal and political battle with the federal government over a laundry list of RCMP wrongdoing that included acts of arson, break-ins, and theft targeting left-leaning and/or separatist media. By the time the Keable Inquiry finished two years later, the committee's report detailed frame-up attempts, blackmail, mail tampering and illegal opening of mail, and illegal wiretapping by officers.[50] Taken together, the RCMP's reputation in the late 1970s was severely tarnished due to the overzealous response to the Front de libération du Québec.

When the RCMP's "dirty tricks campaign" was exposed:

> Morale within the RCMP sank. By the time the McDonald Commission had begun its work in 1978, then-Solicitor General of Canada, Francis Fox, found himself in the unenviable position of having to make a series of dis-

---

49 The RCMP's Security Service Branch confronted many problems in the 1970s due to the diverging techniques between security intelligence work and police criminal investigations. In 1977, the Trudeau Government established the McDonald Commission to investigate the RCMP after a number of illegal activities or "dirty tricks" by its Security Service Branch came to light. See Security and Intelligence Review Committee, *Reflections: Twenty years of independent external review of security intelligence in Canada* (Ottawa: SIRC, 2005) at 7-11, online: <http://www.sirc-csars.gc.ca/pdfs/rfcrfx_2005-eng.pdf> [SIRC].

50 "Some of the most sensational disclosures have concerned the activities of the RCMP's secret 'dirty tricks' squads. One such grouping, G-4, described to the Keable inquiry by RCMP Sgt. Claude Brodeur, stole dynamite, carried out break-ins, and even burned down a barn allegedly to prevent a meeting between members of the so-called Quebec Liberation Front (FLQ) and the U.S. Black Panthers." Richard Fidler, *RCMP: The Real Subversives* (Toronto: Vanguard, 1978) at 9.

> closures about the RCMP Security Service's activities, including an admission that it had been engaged in extra-legal conduct for over two decades.[51]

This was so damaging to the organization that, following the findings and recommendations of the McDonald Commission (1977–1981), the Trudeau government announced in August 1982 the intention to establish a new organization separate from the RCMP tasked with security intelligence.[52]

Introduced in Parliament in May 1983, Bill C-157 established the Canadian Security Intelligence Service (CSIS), which began operating officially on 16 July 1984.[53] The new legislation also created the Security Intelligence Review Committee (SIRC) and the Inspector General for CSIS to review the activities of CSIS and report to Parliament separately from other federal law enforcement entities.[54] Just as important, "it created a framework to keep those powers in check — and that framework has stood the test of time."[55] For the first time, Canada had legislation that clearly separated security from policing and imposed clear accountability frameworks to ensure that transparency and operational security could coexist.

While these organizations have distinct mandates, their areas of operations often overlap. As Figure 5 (above) demonstrates, comparing the number of authorizations obtained by CSIS to those obtained by the RCMP demonstrates that CSIS, which is notoriously secretive, acts to obfuscate the full scope and scale of state surveillance in Canada. Unfortunately, the distinction between criminal investigations and state intelligence is extremely blurred, particularly following 9/11, and this makes it unlikely that CSIS reports are likely to become any less opaque in the near future. Therefore, further research is required to investigate the role of CSIS' use of electronic surveillance and how this affects the overall trends.

(i) Influences Within Policing Operations (Effects, Costs and Complexity)

> *The boundary between the individual and the state, between privacy and law enforcement, has been tested by the collision of the two forces: the nature of criminal activity (liquor, drugs, terrorism) and the advances of technology (the automobile, the telephone, the internet). Sometimes the courts succeed at adapting the constitutional principles to the shifting circumstances of the modern world. But when judges fail, the line defining constitutional freedoms blurs and meanders*.[56]

---

51 SIRC, *supra* note 49 at 10.

52 Canadian Security and Intelligence Service, *History of CSIS*, (2012) online: <http://www.csis-scrs.gc.ca/hstrrtfcts/hstr/brfcssndx-eng.asp>; a special committee of the Senate was also established to examine the legislation given public concern and considerable political debate.

53 In response to committee recommendations made in its report entitled *A Delicate Balance*, the federal government amended the previous legislation by tabling Bill C-9 in January 1984, which became law in June 1984.

54 Canadian Security Intelligence Service, *supra* 52 at 10.

55 SIRC, *supra* note 49 at 11.

56 David K Shippler, *The Rights of the People: How Our Search for Safety Invades Our Liberties* (New York: Random House, 2011) at 58.

As with all government departments, the use of certain techniques can always be reduced to the question of resource allocation. Electronic surveillance is an expensive and time-consuming process in all jurisdictions, but it is particularly burdensome in a bilingual and diverse country such as Canada. Aside from the manpower required to clear the legal hurdles in obtaining warrants and the technical infrastructure which must be built in beforehand, there are also requirements for specialized transcription, indexing, and annotation procedures to meet with court requirements for disclosure. If one finally factors in Canada's linguistic diversity, the limited resources of LEAs for translation and training, and the multiplicity of non-official languages which require specialized "listeners," these elements translate into wiretapping being a very expensive and resource intensive form of investigation.[57] Beyond this, following the ruling of the Supreme Court in *R. v. Stinchcombe* which imposed finite resource limitations on police to gather evidence, LEAs are now limited in the number of transcripts they are able to submit to the court and that they must mine their records after the investigation is completed to ensure to include only those parts which will assist the Crown in making its case.[58]

In an era of tight budgets and fiscal restraint, LEAs have been forced to allocate resources judiciously for maximum strategic impact. To date, however, Annual Reports for electronic surveillance in Canada have not included figures on the relative costs associated with the exercise of this investigatory tool. As a result, it is virtually impossible for non-practitioners to discern whether the decline is simply a reflection of operational choices not to pursue interception as an investigative avenue or whether electronic surveillance simply is no longer a resource-efficient tool for investigators due to the ancillary costs involved. Although data is surely available to policy makers within Public Safety Canada, the lack of qualitative analysis disclosed by LEAs themselves makes assessing effectiveness difficult.

Open-source information indicate that the sheer volume of data collected through electronic surveillance, coupled with bureaucratic constraints such as transcription and translation, make it virtually impossible for investigators to justify the practice — especially in the present environment of fiscal restraint. However, this is not to say that law enforcement has not found new ways to obtain evidence which are more efficient. Rather, these "unknowns" simply demonstrate that LEAs are no longer utilizing the tools within Part VI of the *Criminal Code*. Nonetheless, even if investigators are somehow able to continue to justify funding for maintaining these operations, their adversaries retain the advantage of being substantially more adaptable to technological change.[59]

---

57 This cost may also explain why the focus tends to be on crimes where seizure of cash and assets — such as organized crime, smuggling and the illicit narcotics trade. The sale of these assets may be used to offset at least some of the organizational outputs consumed using complex, expensive investigative techniques such as electronic surveillance.

58 *R. v. Stinchcombe*, [1995] 1 S.C.R. 754.

59 Collecting evidence via wiretapping may not even be particularly useful in obtaining convictions as successive years of strengthened *Charter* s. 8 precedent and other legal safeguards have rigorously defined the circumstances when introduction of captured private communications are admissible in court. From 1974–2011, only approximately

(d) Theory Four: Cyberspace & Technologies Without Intercept

> *Securitization refers to speech acts that characterize some problem as an existential threat in a calculated attempt to justify extraordinary measures, such as the suspension of civil liberties or pre-emptive strikes. The internet is being securitized.*[60]

The previous theories all assumed that LEAs have the capacity to conduct electronic surveillance and that other factors have made them give pause before using it. However, there is evidence that LEAs, confined as they are to their legislative parameters, simply do not have the capacity to carry out this function in the increasingly complex telecommunications environment. Implied in the term "electronic surveillance" is that it extends well beyond traditional wiretapping to include networks at all levels, satellite telephony, and any other communications facilitated through an electronic medium. Given the sheer number of modes which communication can now be transmitted, LEAs find themselves at a distinct disadvantage in trying to identify the mode in which a suspect is communicating, let alone intercept the message.

At a very basic level, it appears that the breadth of communications media expanded at a rate that LEAs did not have the time, resources, or expertise to keep up. Part VI of the *Criminal Code* was amended in the 1980s to include specific references to computer systems in search and seizure provisions and was expanded again in the 1990s. While technology has evolved considerably since, proponents argue that Canada's laws have not kept pace because "increasingly complex tech-

---

half (49 percent) of suspects arrested due to evidence obtained from electronic surveillance had court proceedings initiated against them. Of that group, convictions were obtained only 58 percent of the time. This puts the overall successful conviction rate for this technique slightly above one in four. When exclusively examining the past 10 years, the conviction rate further lowers to less than 20 percent. Trends in the US appear to corroborate the finding of a declining conviction rate for cases involving electronic surveillance. In the years since reporting requirements were first introduced, wiretaps have resulted in a conviction in fewer than 50 percent of cases. During the Obama administration this rate drops to roughly 32 percent. Although many of these convictions would not be otherwise possible without the evidence procured through surveillance, LEAs in the US and Canada may alternatively be beginning to confront the reality that electronic surveillance often provides investigators with reams of inadmissible evidence. The low rate of conviction does not necessarily demonstrate a consistent trend because it is difficult to reconcile the total surveillance authorizations with the total number of successful convictions. The primary reason for this is that convictions are often two to five years following the initial investigations. Presumably, some kind of "echo" in the statistics would reflect this correlation. Further research must be done in order to match each authorization with its corresponding conviction on a case-by-case basis. See Office of the US Courts, *2011 Wiretap Report* (2011) online: <http://www.uscourts.gov/Statistics/WiretapReports/WiretapReport2011.aspx>.

60 Milton L Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge: Massachusetts Institute of Technology, 2010) at 160.

nologies are challenging conventional lawful access methods."[61] As explained in the 2003 report by the Department of Justice Canada: "the arrival of telecommunications industry deregulation, the Internet, cell phones, wireless e-mail, high speed fiber-optic networks and VoIP has changed the picture considerably. Law enforcement agencies find that these more advanced services present technical and legal challenges to conventional lawful access methods."[62] Where a telephone wiretap may have required a technical specialist and some deft fieldwork in the past, gaining access to a suspect's mobile phone(s), VoIP, or email exchanges now requires specialists in law enforcement, telecommunications, and technology sectors working together.

In particular, the *Criminal Code* has not been updated to reflect the fact that surveillance no longer primarily focuses on immobile modes of communication, such as land line telephones. Part VI of the *Criminal Code* obliges, "interception orders authorized by the courts to specify the location at which the interception will take place."[63] The change in technological compatibility with lawful interception means that, according to Susan Landau,

> Law enforcement's job has become more challenging. When a telephone number determined a location — "this line belongs to that apartment" — wiretapping was straightforward. Now electronic surveillance is very different. If the target calls using his own cell phone, he is easy to track. But when the target uses an internet cafe, an anonymizing service, or VoIP, tracking in real time who is talking with whom is often not possible. This has created quite a shock for law enforcement.[64]

In an era where everyday communication occurs instantaneously across several devices and multiple platforms, piecing together the puzzle has become virtually impossible.

While Landau argues that LEAs have previously been able to adapt and cope with the challenges brought by new technical innovations, there is a fundamental difference with digital technology because it is happening in "Internet Time."[65] In

---

61 Department of Justice Canada, *Summary of Submissions to the Lawful Access Consultation (Lawful Access FAQ)*, (2011) online: <http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html>.

62 A number of technological innovations that affect lawful access have emerged at a dramatic pace since the 1990s. The Government has asserted, in a 2002 report on lawful access, that the rapid expansion in the use of wireless communication devices like cell phones would "pose significant challenges if the infrastructure supporting these devices does not include lawful access capabilities." This has been the contention of Canadian law enforcement for the past decade or more as "[t]he rate at which new wireless technologies and services are introduced in the marketplace makes it very difficult for law enforcement [. . .] to sustain their technical ability to lawfully intercept communications." See Department of Justice Canada, *Summary of Submissions to the Lawful Access Consultation* (2003) online: <http://www.justice.gc.ca/eng/cons/la-al/sum-res/sum-res.pdf>.

63 Department of Justice Canada, *Lawful Access — Consultation Document (Legislative Proposals)*, (2011) online: <http://justice.gc.ca/eng/cons/la-al/d.html>.

64 Landau, *supra* note 2 at 7.

65 *Ibid.*

other words, "[w]e have experienced a profound change in societal behaviour in a matter of a few years — and sometimes even a matter of months — not the decades over which such adoption and change occurred previously."[66] Whether investigators have reacted appropriately to this change, or whether they require new powers to do so, is an ongoing debate both in Canada and around the world.

(e) Theory Five: Online Investigations and Electronic Surveillance

> *You must remember, though you will not understand, that all laws weaken in a small and hidden community where there is no public opinion. When a man is absolutely alone in a Station he runs a certain risk of falling into evil ways. This risk is multiplied by every addition to the population up to twelve — the Jury number. After that, fear and consequent restraint begin, and human action becomes less grotesquely jerky.*[67]

While some large telecommunications service providers (TSPs) in Canada have volunteered to incorporate some form of intercept capabilities on their infrastructure, there is still no universal requirement for all companies to deploy interception capability within their systems. Authorities contend that occasionally police or security officials have a court warrant to intercept but that companies simply do not have the technical capability to comply with the order. Without a uniform requirement for interception capabilities, suspects may choose to elude surveillance by subscribing to smaller TSPs that cannot afford to upgrade. Indeed, some of these "independent" service providers even advertise their lack of intercept capability as a feature of their service.

Both Liberal — and Conservative-led governments have previously attempted to standardize intercept capabilities, but each successive proposal has failed to receive Royal Assent for one reason or another. While the previous two attempts failed because an election was called, the most recent iteration of lawful access legislation was introduced in the 41st Parliament amid polarized public opinion. In February 2012, the Minister of Public Safety Vic Toews introduced Bill C-30, which would require companies to preserve logs of the internet usage of their users upon request and make these available to LEAs on demand by stating in Parliament that critics can "stand with us or stand with the child pornographers."[68] While civil society and privacy advocates immediately denounced the statement, major TSPs such Bell, Telus and Rogers remained completely silent on the issue, which if passed, would have substantially altered the way they interact with the Government of Canada. The fact that major TSPs neither criticized nor praised the proposal lends credence to the theory that, in the debate between privacy and surveillance, TSPs have an interest in cooperating with law enforcement so long as it does not

---

66 *Ibid.*

67 Rudyard Kipling, *Under the Deodars* (Adelaide: 2010) online: <http://ebooks.adelaide.edu.au/k/kipling/rudyard/under/>.

68 John Ibbitson, "Tories on e-snooping: Stand with us or with the child pornographers," *The Globe and Mail* (14 February 2012) online: The Globe and Mail <http://www.theglobeandmail.com/news/politics/tories-on-e-snooping-stand-with-us-or-with-the-child-pornographers/article545799/>.

significantly affect their business operations.[69] Ultimately, C-30 died on the order paper one year to the day later, but even then, TSPs were cautious not to comment on its demise.

On the one hand, LEA requests offer TSPs a new revenue stream as well as a government subsidized infrastructure upgrade which may be substantial depending on the volume of requests which they receive. Currently, TSPs that voluntarily process LEA requests do not publically report on how many they receive per year or what they charge for each request.[70] In the United States, researcher and noted activist Chris Soghoian has found that American TSPs have established a pre-set cost for delivering information to LEAs, with real-time interception ranging from $700-$2400 (USD) in each instance.[71] This means that American TSPs derive a revenue stream of tens of millions of dollars simply for turning over data that is already stored within their systems. It is likely that these prices are similar in Canada, but it is unclear whether Canadian TSPs handle a comparable volume to their American counterparts.

However, on the other hand, TSPs must also be cognizant of myriad federal and provincial data protection laws that may trigger public complaints to the Office of the Privacy Commissioner of Canada or provincial data protection authorities. In addition, TSPs are acutely aware that improper disclosure presents the potential for civil liability, damages, and tarnished public image. In Canada, it is this final element which may be the most important going forward because of the increased attention by Canadians over how their personal information is used.

The result is that major TSPs have taken a middling ground to avoid upsetting the delicate balance they currently maintain.[72] If compelled by future legislation to

---

69 Albert Gidari, "Companies Caught in the Middle" (2007) 41:4 USF L Rev 535.

70 That said, companies most likely maintain such statistics for compliance, accounting, and/or court proceedings. For example, Telus (the third largest TSP behind Rogers and Bell) recently stated they processed ten thousand search warrants and production orders in the preceding three years; that is only a single provider. In the same period, there were 355 federal law enforcement warrants for interception issued and reported in the Annual Report; that is to all companies. Logic would seem to dictate that if criminals are progressively transferring illegal activities from the "streets to cyberspace" then Canadian LEAs may find the traditional electronic surveillance tools much less useful without significant infrastructure upgrades by the TSPs. See *R. v. Telus Communications Co.*, 2011 ONSC 1143; reversed 2013 CarswellOnt 3216 (S.C.C.).

71 Christopher Soghoian, *The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance* (forthcoming) at 15, online: <http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf>.

72 As noted in the Canadian legal reference, "cyberspace presents challenges for the application of Part VI of the Code. Cyberspace offers technology never contemplated by legislation with its roots in the mid-1970s. The jurisdictional debate concerning where a private communication was 'intercepted,' for example, did not occur when wiretapping first commenced, for as a practical matter, execution of the 'wiretapping' was usually conducted close to the target." Michael Geist, "Public No Pushover on Snooping Law" *Toronto Star* (30 October 2006) online: <http://www.michaelgeist.ca/content/view/1504/159>. See also: Robert W Hubbard, Peter M Brauti & Scott K Fenton, *Wiretapping and Other Electronic Surveillance: Law*

build in intercept capability, it is unlikely that LEAs will find that unwillingness on the part of the TSP is an impediment to their investigations, provided that federal funds are allocated to build-in these new capabilities. However, in arguing for future lawful access provisions, LEAs will be unlikely to find these TSPs willing to state their enthusiasm for such bills publically.

(f) Theory Six: Alternatives to Interception & Unreported Data

> *Public support for the responsible exercise of this power can only be engendered where the public receives reasonable information concerning the extent and the nature of its use. Without such information it is natural for fears and suspicions of abuse to exist.*[73]

Significantly, there is no clear evidence or analysis in the public domain that confirms police authorities' consternation that investigations have been seriously hampered by a lack of technical capacity. However, as we discussed above, we have little sense about the true volume which surveillance is being conducted in new communications media such as the internet and other digital networks because current reporting regimes do not extend into cyberspace. As a result, it is the "unknown unknowns" which may be exerting influence on the trends.

Additional research will be required in order to understand how the present lawful access legislation in Canada is being actually used in the operational context because open-source data of day-to-day operations is kept confidential for a variety of reasons. Further, reporting requirements have not been reviewed in three decades and, in relation to new surveillance powers conferred by the *Criminal Code*, the following types of surveillance and monitoring are still not subject to the requirement that governments present a public report on their use:

- Interception without judicial authorization, to prevent bodily harm ["emergency provisions"] (section 184.1)[74]; (see *R. v. Tse*)[75]
- Interception with the consent of one of the parties to the communication [see *R. v. Duarte*] (section 184.2);
- General production orders (section 487.012);
- Production orders for commercial account information (487.013);
- Location tracking devices [bugs/GPS location] (section 492.1)
- Number recorders [i.e.: metadata intercepts] (section 492.2).[76]

---

and Procedure (Canada Law Book, 2000). See also: Gilbert, Kerr & McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage Of Police and Telecommunications Providers" (2007) 51:4 Crim LQ, online: <papers.ssrn.com/sol3/papers.cfm?abstract_id=1302544>.

73 Cohen, *supra* note 4 at 211.

74 It should be noted that this article was submitted concurrent with the first reading of Bill C-55 which would extend reporting requirements emergency intercepts.

75 *R. v. Tse*, 2012 SCC 16, [2012] 1 S.C.R. 531.

76 Dominique Valiquet, *Legislative Summary of Bill C-50: An Act to amend the Criminal Code* (Canada: Library of Parliament, 2012) online: <http://www.parl.gc.ca/

Given the relaxed conditions in comparison to traditional real-time electronic surveillance, these new investigative techniques may be potentially used in lieu of traditional electronic surveillance because they are likely more effective and efficient at finding useful evidence.

We suspect, though we cannot confirm, that these alternate lines of investigation likely explain why there are far fewer wiretap authorizations (which must be reported in details stipulated under section 195 of the *Criminal Code*) compared with previous decades. These alternatives to traditional interceptions are more appealing to police because the application requirements are less stringent and external reporting requirements are non-existent. For example, a "production order" may be used by LEAs to access copies of emails, secure transmitted transaction details (metadata), or information about organizations logged online. Production orders have historically been used on financial institutions that rarely reject complying for fear of being perceived as obstructing an investigation. As with the surveillance powers mentioned above, these production orders require no public reporting because they are access "after the fact" and are considered to be different from "live" surveillance reported in the annual reports and there is no requirement to notify individuals they had been subject to surveillance. With advances in web-logging, bulk storage and other cloud technologies, production orders issued to TSPs have arguably become far more relevant to LEAs than wiretapping and less onerous due to largely compliant TSPs.[77]

When police have authorization to access an e-mail that has already been sent or received by a suspect, it could more easily be obtained with a production order or a warrant for search and seizure, rather than an actual interception warrant; despite the fact that they are essentially the same. Current law does not oblige service providers to collect traffic data or content data to provide law enforcement officers with real-time access through the internet (although provisions in C-30 sought to rectify this).[78] As the Honourable Madam Justice Mackenzie mentioned in the B.C.

About/Parliament/LegislativeSummaries/bills_ls.asp?Language=e&ls=C50&Mode=1&Parl=40&Ses=3&source=library_prb>.

77 Three decades of refining of jurisprudence in support of s. 8 of the *Charter of Rights and Freedoms* has clearly shifted the perception that electronic communications is analogous to eavesdropping in a public place towards a legal perception much more protective of privacy, where intercepting communications is akin to mail tampering laws made a century earlier. There are long term indications that the judicial branch has become less inclined to allow for the inclusion of evidence gathered through invasive surveillance techniques. Successive Supreme Court decisions, most notably during the tenure of Chief Justice La Forest, ruled on many cases involving invasive evidence gathering and created strong precedent which have narrowed interpretation on these techniques. See Daniel Scanlan, *Digital Evidence in Criminal Law* (Toronto: Canada Law Book, 2011); Tamil Israel, "Production orders: impending tools of mass investigation (2012) online: <http://www.slaw.ca/2012/02/09/production-orders-as-tools-of-mass-investigations>; Ian Smith, *A compelling problem: privilege and production orders* (Toronto: Criminal Lawyer's Evidence Update, 2005) online: The Law Society of Upper Canada <http://rc.lsuc.on.ca/pdf/kt/privilegeAndProductionOrders.pdf>.

78 On the contrary, Canada's private-sector privacy law stipulates personal information should only be regularly retained to meet bona fide commercial purposes, not the con-

Supreme Court case of *R. v. Giles* [2007], "there is a difference between intercepting messages and searching messages that have already arrived at their intended destination."[79] When attempting to explain declining use of wiretapping or bugging as an investigative tool, this turns out to be a critical legal distinction by separating electronic surveillance that is publically reported versus monitoring that goes undocumented. For e-mail, SMS messaging, or PIN-to-PIN communications to fall under the legal safeguards of Part VI, the communications must be intercepted in real-time and must be strictly defined as a "private communication." From this standpoint, under the definition found in the *Crown Liability and Proceedings Act*, for an online communication to be deemed a "private communication" it must be:

> oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.[80]

The designation of "private communication" has two requirements: there must be a sender or recipient in Canada, and there must be a reasonable expectation of privacy in the mode of communication. In addition, the definition of "intercept" in section 183 is quite precise; because it necessitates the message be obtained in real time, unlike other words such as "obtain" or "acquire," which are used elsewhere in the *Criminal Code*. Therefore, if a communication is stored, logged, cached, or backed up routinely in any manner then LEAs need only wait for the online exchange to end and, the very next second, the protections and reporting requirements of Part VI fall by the wayside. As a result, short of lawful access with real-time online interception, most modern surveillance is unlikely to be considered "electronic surveillance" as defined in the *Criminal Code* and, therefore, does not fall under normal reporting requirements. The cases electronic surveillance reported in the annual reports are most likely outlier investigations where evidence could not be gathered through any of the means detailed above. As a result, the statistics which are publically disclosed in the Annual Report to Parliament are most likely only a small snapshot of the overall volume of LEA surveillance in Canada. This

---

venience of governmental investigators: "Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information." See *Personal Information Protection and Electronic Documents Act*, S.C., 2000, c. 5, Schedule 1, Principle 5 — Limiting Use, Disclosure, and Retention.

79 In this way, most police monitoring in cyberspace likely falls outside the controls of Part VI in the *Criminal Code* as these apply only to "interception" of "private communication." From a purely practical standpoint, it can be difficult to intercept packet-based email in real-time given that ISPs are not obligated to have such capability. See *R. v. Giles*, 2007 BCSC 1147 at para. 7.

80 *Crown Liability and Proceedings Act*, RSC 1985, c. C-50 s. 16.

attempts to gather evidence and the actual tools used by police remain just as opaque as before 1974.

Practically speaking, this is cause for alarm because this means that the accountability and transparency for police surveillance has become more opaque than even before the *Protection of Privacy Act*. If this is correct then the popular perception of expanded surveillance is likely correct, and Canadians no longer enjoy any reasonable expectation of privacy.[81] Ordinary citizens who seek to discover how they are being surveilled and investigated are likely to find it difficult to even find generalized information because many of these new techniques are not common knowledge outside of a very specialized group (i.e. people who would be interested in reading this article through to its conclusion). This Canadian approach stands in contrast with many other jurisdictions, most notably the United States and United Kingdom, which have at least basic reporting requirements for many modern electronic surveillance techniques.[82]

(g) Theory Seven: Widespread Encryption

> *Cryptography is not a silver bullet. It provides security only for the communications content. In particular, the transactional information — who is communication with whom when — is not encrypted. It is often the case that transactional information is more valuable than content . . . it can indicate that a company merger is about to occur, that nation-states are engaged in negotiation, that someone is having an affair.*[83]

The use of encryption is the final argument which LEAs often raise to support arguments for increased lawful access provisions. Internet communications began to adopt strong encryption measures during the late 1990s because of widespread perception of cyber-security threats posed by "hackers," organized crime, and adversarial nation states. Law enforcement agencies globally signalled concerns that widespread use of strong encryption techniques would block access to critical evidence data and criminals would disappear into the many layers of the internet, what is known now as "going dark."[84] In the past few years, this trend has accelerated

---

81 As a result, the legal reality is that online communications and internet transactions are given considerably lesser privacy protections than traditional telephone conversations and as noted, citizens have no real idea how often these online methods of monitoring are used by Canadian LEAs owing to lack of required public reporting on the part of the RCMP as well reticence on the part of ISPs to voluntarily disclose the information for fear of a negative public reaction. See Hubbard, Brauti & Fenton, *supra* note 72, vol 2, at 15–30.

82 See Interception of Communications Commissioner, *2011 Annual Report of the Interception of Communications Commissioner* (London, UK: Interception of Communications Commissioner, 2012) online: <http://www.intelligencecommissioners.com/docs/0496.pdf>. United States Courts, *Wiretap Report* 2011 (Washington DC, USA: Administrative Office of the US Courts on behalf of the Federal Judiciary, 2012) online: <http://www.uscourts. gov/Statistics/WiretapReports.aspx> [US Courts].

83 Landau, *supra* note 2 at 59-60.

84 Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud* (2012) International Data Privacy Law, at 4 [Forthcoming].

and "encryption is in the midst of becoming the default way that many communications occur on the Internet."[85]

There are certainly methods for Canadian LEAs to gain access to strong encrypted communications, but they are complex, onerous, and put LEAs at a distinct disadvantage. In select intelligence-related cases handled by CSIS, the Communications Security Establishment Canada (CSEC) has the technological ability to intercept and break encrypted communication. However, it is well outside of CSEC's mandate to assist the RCMP in domestic criminal investigations on citizens and may threaten to overwhelm its operational capacity if used regularly.[86] It should be noted that, as with research into CSIS, it is very difficult to gather information on how this organization works and what capabilities it can muster. All that is known is that if the RCMP encounters an encrypted communication, it must decide whether to utilize its in-house resources to gain access; an unpleasant task considering that the vast majority of encrypted messages are unlikely to be relevant.

Alternatively, they could also directly access the content of encrypted communications that have been sent or received by an intercept ready device (or a virtual "honeypot") with a search warrant or general warrant. However, once again, this requires statutory laws similar to the United States' *Communications Assistance for Law Enforcement Act* (*CALEA*), which do not presently exist within Canada.[87]

---

85 For example, social media website Facebook now supports Secure Sockets Layer (SSL), an encrypted protocol that could enable its social networking communications to be unreadable at the ISP level if it is set to default. Major web locker services, such as Dropbox, already use SSL by default in addition to a number of additional measures such as 2-step verification. Peter Swire explains that the growing adoption of strong encryption in cyberspace "limits the usefulness of lawful access order[s]." [*Ibid.* at 5]. Although law enforcement agencies may still intercept encrypted Internet communications, it is virtually impossible to "crack" them if the encryption is used properly. Police can generally access the content of emails only if they are saved or stored on the webmail's servers (where they are not strongly encrypted). Thus, as noted earlier, Canadian LEAs may not be inclined or authorized to intercept and access the content in real-time. Production orders represent the only lawful option to solely acquire encrypted messages online (but only after being received and stored). Again, the legal controls around privacy protection set out in Part VI of the *Criminal Code* would not apply to these circumstances.

86 As the Signals Intelligence Branch of the Ministry of National Defence, CSEC's mandate is to secure electronic information systems and to provide operational assistance to federal LEA. However, it is prohibited by law from directing its "collection" activities at any Canadian citizen (regardless of their location at the time of intercept) or at any person within Canada. See Office of the Communications Security Establishment Commissioner, *Annual Report to Parliament* (Ottawa: CSE Commissioner, 2012) at 10, online: <http://www.ocsec-bccst.gc.ca/ann-rpt/2011-2012/ann-rpt_e.pdf>.

87 *CALEA* is an act passed in 1994 that requires American Internet service providers to have their network technologies "structured in such a way that law enforcement can easily eavesdrop on electronic communications." See Emily Hancock, "CALEA: Does one size still fit all?" in JM Balkin, *Cybercrime: digital cops in a networked environment* (New York: New York University Press, 2007) at 184; Heidi McKee, "Policy matters now and in the future: Net neutrality, corporate data mining, and government surveillance" (2011) 28 *Computers and Composition* 276 at 286; William P Bloss,

Therefore, if LEAs wish to intercept an encrypted message, they must remotely access the computer after the encrypted message has been stored. However, this would fall under the normal search and seizure provisions of the *Criminal Code* and must be weighed against section 8 of the *Charter* as it is akin to executing a search warrant on a domicile.

Perhaps the most striking fact in this argument is the inability of LEAs to justify why they require legislative powers to circumvent encryption. The RCMP does not provide statistics regarding how often encryption obstructs an investigation. However, in the U.S between 2000 and 2011, encryption was encountered fewer than 10 times per year on average.[88] Not once in 11 years did the presence of the encryption prevent a LEA from monitoring a communication. Although this does not necessarily correlate with the Canadian experience, it does suggest that the declining trend in reported electronic surveillance is only negligibly affected by an increase in the use of end-user encryption.

III. CONCLUSION

> *When it comes to privacy and accountability, people always demand the former for themselves and the latter from everyone else*.[89]

In law, as well as technology, Canada often follows the lead of its only land neighbour. In the 1970s, the public revelations of Watergate and the Church Commission in the US brought wiretapping out of the realm of detective fiction and put it on the front page.[90] In this article, however, we have observed and attempted to explain why the use of one very particular form of surveillance — the electronic interception of private communications — appears to be increasingly *unpopular* with Canadian LEAs while the complete opposite trend appears in many other jurisdictions; particularly in the United States and the United Kingdom.[91]

"Transforming US police surveillance in a new privacy paradigm" (2009) 10:3 *Police Practice and Research* 225 at 233.

88 US Courts, *supra* note 82.

89 David Brin, "The Transparent Society" *Wired Magazine* (December 1996) online: <http://www.wired.com/wired/archive/4.12/fftransparent.html>.

90 The prevailing thought at the time was that a revolution in communications technology could only amplify the trend of LEA's use of wiretapping. After all, if electronic surveillance devices were essentially undetectable, nothing prevented them from being installed anywhere, targeting anyone. Indeed, a surveillance society at the expense of citizens' privacy seemed virtually inevitable. In 1969, Federal Minister of Justice John Turner expressed his concerns to the Canadian Bar Association, cautioning "The investigator's dream — making his subject a walking transmitter, and enabling the investigator to hear everything the subject says to anybody else, or even what he mutters to himself — can be realized by the wiring of a person's clothing. We are told that there are transmitters so small that they can be mounted as a tooth in a dental bridge . . . The Orwellian society of 1984 may be here already." John Turner, *Minutes and Proceedings of the 51st Annual Meeting of the Canadian Bar Association* (Ottawa, 1969).

91 See Interception of Communications Commissioner, *2011 Annual Report of the Interception of Communications Commissioner* (London, UK: Interception of Communications Commissioner, 2012) online: <http://www.intelligencecommissioners.com/

We hope this will open up the field for future research on the concrete practices of surveillance in Canada. Who is under surveillance, where, why, and for how long these individuals fall under the scrutiny of the state are all questions that can be asked and should, to some degree, be answered by the Government of Canada. While the government must certainly deploy intrusive and covert *means* to carry out investigations in the public interest, this does not relieve investigators of the onus to enumerate, explain and justify the *ends* of that surveillance to the public afterward.

In this article, we have examined four decades of public reporting concerning how Canadian federal authorities use electronic surveillance. What lessons emerged? Why does it matter now? What further research would be useful? We feel that the data presented in this study reveal four important trends which, while not conclusive, offer a great deal of context to the state of surveillance in Canada:

- *Turning off the tap*: Court authorized surveillance of private communications has fallen dramatically in the period surveyed — for the numerous legislative, judicial and administrative factors cited and there are likely many others we have yet to unearth. However, as we have stressed in the discussion of the figures, this does not mean that government monitoring and tracking has ceased. Indeed, one of the more intriguing discoveries emerging from the historical data is that dozens of individuals can be targeted for surveillance under a single authorization. This explains why statistics tracking numbers for total court-issued warrants indicate a drop, even though individual notifications have remained relatively stable.
- *Rubber stamping*: LEAs argue that the authorization process can impede investigations. Yet courts refused only a handful of warrant applications since 1974. Clearly, police administrators and legal counsel have a very rigorous internal system of checks to catch problem applications before they are reviewed by a court official. However, any argument which portrays authorizations as obstructionist is more likely the result of LEAs' own internal bureaucratic complexity rather than judicial obstinacy.
- *Break in case of emergency*: The statistics show that emergency authorizations have been used only 38 times since 1974 and only 10 times since 11 September 2001. Emergency authorizations have recently been judged deficient because of the Supreme Court's unanimous ruling on *R. v. Tse* (2012) which found that section 184.4, which allowed interception without a prior authorization, lacked proper safeguards and was therefore unconstitutional.[92] *R. v. Tse* suggests that, at minimum, emergency interception should require public reporting. Although Parliament has introduced Bill C-55 in February 2013 to address this deficiency, this form of

---

docs/0496.pdf>. United States Courts, *Wiretap Report* 2011 (Washington DC, USA: Administrative Office of the US Courts on behalf of the Federal Judiciary, 2012) online <http://www.uscourts.gov/ Statistics/WiretapReports.aspx>.

92 *R. v. Tse*, *supra* note 75.

public accountability should be extended to all forms of electronic surveillance.[93]

- *The unknown unknowns*: Without a doubt, the most interesting questions emerging from the reports we reviewed relate to what is *not* reported. There are myriad forms of surveillance available for use by LEAs and we posit that online investigations and electronic evidence gathering now leverages a whole set of techniques and tools quite apart from wiretapping and bugging. These legal powers such as production orders, assistance orders, general warrants, tracking devices and number recorders are all easier powers of search and surveillance to execute (both in terms of legal hurdles and resource requirements). Moreover, authorities are not currently required to notify the general public or Parliament when these powers are used.[94] Electronic surveillance can now take the form of monitoring credit card records, on-board navigation records, website account procurement (i.e. Facebook), or even data parsed together from disparate sources using data mining software. Reporting requirements introduced in the early 1970s simply have not kept up with the range of modalities that LEAs use when conducting investigations.

We believe that the original intent of the 1974 *Protection of Privacy Act* was to ensure invasive surveillance powers are used appropriately. However, over the years LEAs have become hyper-cognizant that public opinion has the potential to ruin both investigations and reputations. Back in Ottawa, numerous structural changes to the law enforcement portfolio and myriad pressures that are natural in a bureaucracy resulted in inconsistent reporting methodology in the annual reports to Parliament. As we found, following the reports year over year demonstrates that the numbers are constantly in flux and the methodology often changes radically without explanation in the interim between one year and the next. Further, while communications infrastructure has radically changed, the reporting mechanisms have not changed at all. As a result, LEAs have been free to operate in the digital modes without oversight all the while being able to produce reports which demonstrate the contrary. Taken together, our findings are important because they demonstrate a failure on the part of Parliament to demand modernized reporting requirements for the networked age.

Restricting the use of wiretapping to serious crimes and requiring detailed Annual Reports were meant to be key components in democratically controlling authorities' surveillance practices. After all, the stakes associated with such surveillance are very high: freedoms of assembly, speech and dissent, rights of

---

93 This article went for publication prior to the April 2013 deadline the SCC had imposed for passage of Bill C-55.

94 As just one example, we lack any data on tracking devices for individuals or vehicles. Yet, other authorities argue that geo-location has become one of the most important data elements used when compiling an investigation. See Senator Ron Wyden, "Clear Geolocation Guidelines are Needed to Protect Privacy Rights" *US News and World Report: Debate Club* (25 June 2012) online: <http://www.usnews.com/debate-club/should-probable-cause-be-required-for-police-to-use-cell-phone-location-data/clear-geolocation-guidelines-are-needed-to-protect-privacy-rights>.

association, movement and lawful protest all hinge on how the vast resources of government to register, track, survey and monitor its citizens are restricted. Interpretation of "reasonableness" requires public dialogue to match societal attitudes. Without transparent reporting, interpretation of Section 8 rights becomes the exclusive domain of the investigating body and a judge while the public is completely left out of the conversation.

Particularly in the past ten years, Canada has wrestled with the issue of invasive surveillance in a variety of contexts: airport security measures, the long-form census, the firearms registry, Canada-US "Beyond the Border" perimeter security plans, and other initiatives which all require citizens to lessen their expectation of privacy to some extent. How and when government chooses to intrude upon the lives of citizens can shape the trust and confidence citizens have in its authority and legitimacy. Following fiascos such as the Maher Arar extradition, a Canadian citizen who was arrested by American authorities acting on inaccurate Canadian intelligence and tortured in Syria for eight months, Canadian law enforcement, especially the RCMP, are acutely aware of the repercussions of expanding beyond the parameters set by Parliament and the courts.

For these reasons, Canada needs a detailed and thorough discussion of all types of surveillance practices. However, before this can happen, we need to explore the best research and legal alternatives on how to moderate the invasive powers of the state, oversee the various agencies involved, and enforce accountability from these bodies without needlessly encroaching on their ability to carry out their protective mandates; a task for the more than capable pens of Canadian civil society. However, as indicated in Section 8 of the *Charter*, the onus is upon the watchers — not the watched — to explain and justify the powers they have before Parliament grants further invasive surveillance powers in such bills as the *Investigating and Preventing Criminal Electronic Communications Act* (bill C-30). As noted above, at present, this explanation has not been forthcoming primarily because Parliament has failed to demand a clear accounting based on fact rather than anecdote and ideology.

IV. FURTHER RESEARCH

Mapping out areas for future exploration is not difficult because there are glaring gaps in every single section of our article which must be filled by future research. We have a provisional picture of the landscape at best — filled with edges, valleys and channels devoid of detail. As mentioned throughout, the growing role that CSIS, CSEC and provincial police might play in the overall structure of surveillance in Canada is largely invisible to us — a considerable dark spot in the midst of our map. The Service, CSEC, their review bodies and provincial Attorneys-General all have a role in bringing transparency to the structure. Only these organizations have the statistics, reporting data, and warrant application review processes to fill in the blanks. It is entirely possible that the creation of CSIS (1984), CSEC (created in 1946, but granted a legislative mandate by the *Anti-Terrorism Act* in 2001) and a growing sophistication within provincial and municipal policing has decentralized the use of electronic surveillance. The extent of this shift would require considerable further research.

The costs and effectiveness of surveillance currently reported also requires serious investigation, particularly because Public Safety Canada's Annual Report gets

thinner with each passing year. Compared with reports from the Office of the Solicitor-General in the mid-1990s, current reports are anaemically devoid of explanation. Clearly, this is a seriously under-resourced priority in that Ministry and certainly not what Parliamentarians had in mind when reporting requirements were established in law. Independent researchers with the requisite background in statistics, criminology and legal training could make much of the historical data comparing persons identified through surveillance versus those arrested, charged, brought to trial or successfully prosecuted.

Finally, as others have argued convincingly, we need analysis, or at least educated estimates, of a reasonable sort on all other forms of surveillance mentioned in this article such as production orders — call that the "ocean" that surrounds the map we have set out. The UK and US require detailed public reporting and independent review of many of these forms of surveillance. Without similar evidence and consideration, the Canadian public remains dangerously in the dark. Critical questions about privacy, due process, lawful authority and reasonable surveillance deserve clarity and transparency so that they may be included in the public discourse by legislators, courts and Canadian citizens.