TILT LAW & TECHNOLOGY
WORKING PAPER SERIES

Criminal investigation and privacy in Canadian law

Bryce C. Newell and Tom Chokrevski

Tilburg University, TILT
b.c.newell@tilburguniversity.edu

Version 1.0, February 2017

Citation: B.C. Newell and T. Chokrevski, Criminal investigation and privacy in Canadian law, TILT Law & Technology Working Paper Series, version 1.0, February 2017.

Abstract

The law regulating criminal investigation both legitimates the government's use of power and limits it by setting conditions for intrusions on fundamental rights and liberties. Privacy is one of the most prominent issues in establishing and limiting investigation powers. This paper analyses criminal investigation in relation to privacy in Canadian law, with particular focus on privacy-related limitations and safeguards to criminal investigation powers. As part of a large-scale project on privacy protection in the 21st century, together with similar country studies, it will facilitate comparative legal analysis of criminal investigation (a relatively under-researched field), and also help to better understand privacy, as the forms and scope of privacy protection in criminal investigation law tell us something about how legislators conceptualize privacy, and how and to what extent the law protects different types of privacy.

Privacy-related crimes in Canadian law

Version 1.0 (working paper), 28 February 2017

CONTENTS

1. Introduction

This report provides an overview of how privacy is protected through the law of criminal procedure in Canada. This working paper, which is part of a larger and on-going project, provides an overview of (selected) privacy-related aspects of Canadian criminal procedure. We structure our analysis along four types of objects of the right to privacy, as identified in our earlier work: the protection of persons, places, things, and data.[1] Because the overall goal of this project is to generate a better understanding of the concept of privacy and its importance in our contemporary society filled with myriad new forms of surveillance and other privacy intrusions (and to do so from a comparative perspective), we conceptualize privacy broadly and include provisions that relate to the broad theme of protecting aspects of persons and their personal lives (encompassing the various types and dimensions of privacy we present in Koops, et al. (2017)). This conceptualization undoubtedly encompasses a large part of criminal procedure law. The current working version of this draft includes more substantive analysis of particular provisions (those prioritized by our on-going research to date), and additional analysis and analysis of additional provisions will continue to be added as the research progresses.

[1] *See* Koops, et al., *A Typology of Privacy*, 38 U. PA. J. INT'L L. __ (2017) (forthcoming).

Section 2 contains a brief summary of the basic elements of Canadian criminal procedure. Sections 3-5 outline criminal provisions related to protecting places (section 3), persons (both as individuals and in the context of social and/or intimate relationships) (section 4), and things (section 5).

2. Background: Canadian criminal procedure

The protection of privacy in Canadian law has three main sources: common law, federal and provincial legislative statutes, and the Canadian Charter of Rights and Freedoms. Privacy *as such* is not mentioned in the Charter, which instead protects a right to be secure from unreasonable search and seizure (s. 8, Canadian Charter of Rights and Freedoms). The Supreme Court of Canada (SCC) has interpreted privacy protection rules from the Charter in a number of cases over time that are relevant for criminal procedure.

It is emphasized in SCC doctrine that section 8 "protects people, not places."[2] This has resulted in a "hierarchy" of privacy protection[3]: the highest protections attach to privacy of the person, especially privacy protecting bodily integrity (e.g., strip-searches, taking biological samples); second and following bodily privacy is the privacy of the home, followed by the perimeter space around the home. This is then followed in an even more "diluted" level of protection for commercial spaces, then to private cars, privacy at school, and finally even a degree of protection for privacy in prison. At the top of this hierarchy sits the home, and "[t]here is no place on earth where persons can have a greater expectation of privacy than within their 'dwelling-house.'"[4]

3. The protection of places

While there is no direct privacy protection of a place *as such*, there is an indirect relationship that extends from a person to a given place, through the 'reasonable expectation of privacy' concept. This concept is used to operationalize the privacy interest as extending from a person to a place, and varies flexibly depending on the place and the ties it has to the person in question (contrasted with the US property approach). A person's residence or dwelling generally attracts a high level of privacy interest, but the SCC has over time created very specific exceptions to the rule.

3.1. Thermal imaging of a home

In *R. v. Tessling*,[5] the SCC overruled a lower appellate court's ruling and held that an overhead flight and use of a thermal imaging device to measure heat emanating from a private residence did not violate the accused's constitutional right to be free from unreasonable search and seizure. In that case, the RCMP used an airplane equipped with a Forward Looking Infra-Red ("FLIR") camera to overfly properties owned by the accused. FLIR technology records images of thermal energy or heat radiating from a building. It could not determine the nature of the source of heat within the building or "see" through the external surfaces of a building. The RCMP were able to obtain a search warrant for the accused's home based on the results of the

[2] Hunter et al. v. Southam Inc., 2 SCR 145 (1984), *quoting* Katz v. United States, 389 U.S. 347, 351 (1967).
[3] R. v. Tessling, 3 SCR 432 (2004).
[4] R. v. Silveira, 2 S.C.R. 297, at para. 140 (1995) (per Cory J.).
[5] R. v. Tessling, 3 SCR 432 (2004).

FLIR image coupled with information supplied by two informants. In the house, the RCMP found a large quantity of marijuana and several guns. The accused was charged with a variety of drug and weapons offences. At trial, he unsuccessfully argued that the FLIR overflight was a violation of his right to be free from unreasonable search and seizure guaranteed by s. 8 of the Canadian Charter of Rights and Freedoms, and was convicted. The Court of Appeal set aside the convictions. The court found that the use of FLIR technology constituted a search of the accused's home and, since it was done without a warrant, violated his s. 8 right. The appellate court concluded that the evidence ought to have been excluded and the accused was acquitted on all charges.

In overruling the lower court's decision, dismissing Justice Abella's arguments that such thermal imaging gains information about the activities of the person in the home and is therefore intrusive enough to constitute a search, by saying that the information was crude and focused only on the outside of the home, merely hinting at activity that produced heat. Being on the exterior of the home, the person had no reasonable expectation of privacy in those heat signals, and the FLIR overhead flight did not violate the respondent's s.8 right. The heat signatures were "exposed to the public"; despite the use of FLIR technology, the technology itself was not deemed to be sufficiently intrusive for privacy. The SCC notes that similar uses should be decided on a case-by-case basis taking the specific technological capabilities into account every time, but despite this, Kerr et al. later note that the case was taken at face value and applied in subsequent decisions without attention to specific details of technical capabilities.

3.2. Collecting data about home energy and electrical consumption

In *R. v. Gomboc*,[6] the SCC was confronted with a case where the police had requested, without a warrant, that an electric utility company install a digital recording ammeter (DRA) to measure the flow of electricity into a residence suspected of housing a marijuana grow operation. The court was asked to decide whether the occupants of the home could maintain a reasonable expectation of privacy in information collected by the police from the DRA. The SCC held that collecting data from a device like a DRA does not constitute a search under section 8 of the Charter and that the defendant could not claim any objective expectation of privacy in that electrical flow information. In coming to this conclusion, the majority of the justices stated that, "A critical factual consideration, on which much of the disagreement in this case turns, is the degree to which the use of DRA technology reveals private information." However, in answering that question, they held that,

> The DRA is a technique that reveals nothing about the intimate or core personal activities of the occupants. It reveals nothing but one particular piece of information: the consumption of electricity.

The justices concluded that collecting electrical flow data did not disclose any "biographical core data" or "revealing intimate and private information for which individuals rightly expect constitutional privacy protection."

Gomboc built on earlier case law from *R. v. Plant*.[7] In *Plant*, the court was asked to decide whether the warrantless search of computerized electrical consumption data violated section 8 of the Charter. The court held that the police check of computer records on electricity

[6] R. v. Gomboc, [2010] 3 SCR 211 (2010).
[7] R. v. Plant, [1993] 3 SCR 281 (1993).

consumption was not unreasonable and that the accused had no reasonable expectation of privacy in the computer records on electricity consumption, primarily because they "do not reveal intimate details of the accused's life."

3.3. Searches around the perimeter of the home

A number of additional SCC cases are relevant to protecting privacy in certain places surrounding a home. For example, the court has held in multiple cases that perimeter searches of the exterior of a person's house violate section 8 when they are conducted without sufficient "probable grounds" for believing that an offense was taking place inside the home.[8] However, the court has not always found these intrusions significant enough, when weighed against law enforcement interests, to justify the exclusion of evidence.[9]

The SCC has also held, most prominently in *R v. Patrick*,[10] that placing garbage outside the house for pickup by garbage collectors results in a diminished expectation of privacy, on the theory that the garbage has been abandoned. In that case, the majority held reasoned that,

> [the defendant] abandoned his privacy interest in the information when he placed the garbage bags for collection at the back of his property adjacent to the lot line. He had done everything required of him to commit the bags to the municipal collection system. The bags were unprotected and within easy reach of anyone walking by in the public alleyway, including street people, bottle pickers, urban foragers, nosey neighbours and mischievous children, not to mention dogs and assorted wildlife, as well as the garbage collectors and the police. However, until garbage is placed at or within reach of the lot line, the householder retains an element of control over its disposition. It could not be said to have been unequivocally abandoned if it is placed on a porch or in a garage or within the immediate vicinity of a dwelling. Abandonment in this case is a function both of location and [the defendant's] intention.

3.4. Other place-related cases

Other cases have held that the search of a student by a school principle, on school grounds and in the presence of a police officer, was not an unreasonable search because students have diminished expectations of privacy at school,[11] that . For an analysis of the diminished expectations of privacy in vehicles, see the discussion of *R v. Wise*, below at section 4.1.1; however, some searches of vehicles can violate section 8 (at least in regards to the owner, but not in regards to mere passengers), especially when the search exceeds the scope of the officer's probable grounds to believe that evidence will be found (for example, searching closed bags or containers within the vehicle without specific and probable grounds to believe they contained evidence of an offense).[12]

---

[8] *See e.g.*, R. v. Plant, 3 SCR 281 (1993); R. v. Kokesch, 3 SCR 3 (1990).
[9] *See e.g.*, R. v. Kokesch, 3 SCR 3 (1990).
[10] R. v. Patrick, 1 SCR 579 (2009).
[11] R. v. M. (M.R.), 3 SCR 393 (1998).
[12] R. v. Belnavis, 3 SCR 341 (1997); R. v. Mellenthin, 3 SCR 615 (1992).

4. The protection of persons

4.1. Protections for behavioural privacy

4.1.1. Location tracking

In Canada, warrantless location tracking by the police is governed by judicial interpretations of section 8 of the Canadian Charter of Rights and Freedoms, which reads, "Everyone has the right to be secure against unreasonable search and seizure."[13] Location tracking can be authorized, however, by tracking-specific warrants outlined in the Criminal Code, including sections 492.1(1) (*Warrant for tracking device — transactions and things*) and 492.1(2) (*Warrant for tracking device — individuals*).[14] For purposes of a section 492.1 warrant, a *tracking device* is defined as "a device, including a computer program… that may be used to obtain or record tracking data or to transmit it by a means of telecommunication."[15] When such a warrant is granted, it allows a police officer to "to install, activate, use, maintain, monitor and remove the tracking device, including covertly,"[16] subject to any conditions imposed by the judge,[17] but only for a maximum of 60 days from the date the warrant was issued.[18]

These two types of tracking warrants were distinguished in amendments to the Criminal Code in 2014, when Parliament determined that tracking individuals (or things "usually carried or worn by" individuals, such as cell phones) was more privacy-invasive than tracking vehicles or the location of transactions and should be based on a higher standard of proof; namely, "reasonable grounds to *believe*"[19] rather than "reasonable grounds to *suspect* that an offence has been or will be committed… and that tracking [an individual, thing, or transaction] will assist in the investigation of the offence."[20] Either of these warrants can also be combined with an "assistance order"[21] designed to ensure, for example, that a telecommunications provider assist law enforcement in tracking a device such as a cell phone (by providing data or access to data required for such purposes).

The Criminal Code also provides for production orders and preservation demands that cover location tracking data. Section 487.017 (*Production order – tracking data*) allows the police to make *ex parte* applications for court orders requiring third parties to produce documents containing *tracking data*, defined as "data that relates to the location of a transaction, individual or thing."[22] Additionally, preservation demands and preservation orders under sections 487.012 and 487.013, respectfully, can also encompass location tracking data as a form of *computer data*.[23]

---

[13] Canadian Charter of Rights and Freedoms § 8.
[14] For some discussion, see e.g., R. v. Grandison, 2016 BCSC 1712 (BCSC 2016).
[15] CC § 492.1(8).
[16] CC § 492.1(3).
[17] CC § 492.1(4).
[18] CC § 492.1(5).
[19] CC § 492.1(2).
[20] CC §§ 492.1(1) (emphasis added). *See also* R. v. Grandison, 2016 BCSC at para. 34. The text of the bill amending the standard of proof, Bill c-13, R.S. 2014, c. 31, s. 23, is available at http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6830553&File=4.
[21] Canadian Criminal Code § 487.02.
[22] CC § 487.011.
[23] "Computer data" is defined as "representations, including signs, signals or symbols, that are in a form suitable for processing in a computer system." CC § 342.1(2).

The legal goods (interests) protected

Section 8 of the charter protects against *unreasonable* searches and seizures.[24] Put differently, the intent of Section 8 is to "protect individuals from unjustified state intrusions on their privacy."[25] In doing so, the Supreme Court has also determined that Section 8 protects "the underlying values of dignity, integrity and autonomy."[26] The Court has differentiated between three types of privacy protected by Section 8: personal, territorial, and informational. According to the Court in *R. v. Plant*, the Charter protects informational privacy by seeking

> to protect a *biographical core of personal information* which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[27]

In determining whether a search is reasonable, the Supreme Court analyzes whether the contested "police activity invades a reasonable expectation of privacy."[28] In doing so, it examines the totality of the circumstances, including a two-step test for determining whether subjective expectations of privacy are objectively reasonable, fashioned after the test proposed by Justice Harlan of the United States Supreme Court in *Katz v. United States*.[29] All warrantless searches are prima facie unreasonable.[30]

Types of location tracking

Visual observation

Visual observation, including video surveillance, by the police constitutes an unreasonable search only when it intrudes upon a person's reasonable expectation of privacy.[31] However, visual surveillance conducted in public places (e.g., on a public road) for the purpose of tracking a suspect is generally not unreasonable, because—as one Quebec court put it—such a suspect cannot expect any privacy or intimacy in such a place ("ne pouvait prétendre à aucun droit d'intimité").[32] This conclusion is supported by lower court decisions holding that no reasonable expectation of privacy exists in the entrance lobby of an apartment building[33] or in the public areas of public bathroom.[34] However, a reasonable expectation of privacy does exist in a closed bathroom stall in such a public bathroom[35]—at least unless the suspect exposes himself under the dividing wall so that he is visible from the public areas (in which case, any subjective expectation of privacy becomes unreasonable).[36]

---

[24] Hunter v. Southam Inc., 2 S.C.R. 145, 159 (1984); R. v. Tessling, 3 SCR 432, para. 19 (2004).
[25] STEPHEN COUGHLAN, CRIMINAL PROCEDURE 62 (Toronto: Irwin Law, 2008).
[26] R. v. Plant, 3 S.C.R. 281, 293 (1993).
[27] R. v. Plant, 3 S.C.R. 281, 293 (1993) (emphasis added).
[28] R. v. Wise, 1 SCR 527 (1992).
[29] R. v. Edwards, 1 S.C.R. 128, para. 45 (1996); *see also* R. v. Tessling, 3 SCR 432, para. 19 (2004)..
[30] COUGHLAN, *supra* note 25 at 81.
[31] R. v. Wong, 3 SCR 36 (1990).
[32] R. v. Joyal, 43 CR (4th) 317 (1995) (no reasonable expectation of privacy in the entrance lobby of an apartment building).
[33] R. v. Silva, 1995 CanLII 7242 (ON SC), <http://canlii.ca/t/1w0tx>, retrieved on 2017-01-13.
[34] R. v. LeBeau, 1988 CanLII 3271 (ON CA), <http://canlii.ca/t/22kn3>, retrieved on 2017-01-13.
[35]
[36] R. v. LeBeau, 1988 CanLII 3271 (ON CA), <http://canlii.ca/t/22kn3>, retrieved on 2017-01-13.

GPS or other tracking devices[37]

There are very few cases examining the application of Section 8 to location tracking by the police, particularly warrantless tracking. In some cases, defendants have argued (unsuccessfully) that the standards for obtaining tracking warrants are insufficient to pass constitutional muster under the Charter.[38] However, in only once case has the Supreme Court specifically addressed the constitutionality of warrantless location tracking—and only in a case arising from tracking that took place in 1987. In *R. v. Wise*,[39] the Supreme Court decided that the installation and use of a beeper ("a low power radio transmitter") that assisted officers in determining the location of the defendant's vehicle constituted an unreasonable search because it violated his reasonable expectation of privacy in the location and movements of his vehicle and because it was installed after the expiration of a valid warrant.[40] However, the Court also held that the search was "only minimally intrusive" and that the tracking evidence should not be excluded from the prosecution.[41] In coming to that conclusion, the court explained that motor vehicles were subject to a lower expectation of privacy than other places (e.g., homes, offices) and placed significant weight on the argument that the beeper was a rudimentary device that did not reveal details about the vehicle's movements. According to the Court:

> It must be remembered that the tracking device used in this case was unsophisticated and indeed simplistic. It did not provide a visual record of the movement or position of the vehicle. Nor was it able to pick up and record conversations in the vehicle. Rather, it was capable of giving only a very rough idea of the vehicle's location. Certainly, it could not be said that the device was capable of tracking the location of a vehicle at all times.

As such, police use of more detailed (and contemporary) GPS-based or cellphone tracking techniques may not benefit much from the *Wise* rationale. It seems clear that such methods would constitute unreasonable searches, and more likely that the more detailed evidence would be excluded, but the courts have not yet decided these specific questions.[42]

5. The protection of things

5.1. Computers and cell phones

A number of SCC cases have dealt with the search and seizure of computers or cell phones.

In *R v. Vu*,[43] the court held that a search warrant for a home cannot extend to searching computers inside the home (if not specified in the warrant) on the traditional theory that receptacles (e.g., cupboards and drawers) could be searched, because personal computers should be "treated… as a separate place" to be searched, and should require a separate warrant.

---

[37] Transit driver objects to use of technology (MDT and GPS) on company vehicle, 2009 CanLII 74728 (PCC), <http://canlii.ca/t/27gk8>, retrieved on 2016-12-08.
[38] *See, e.g.,* R. v. Grandison, 2016 BCSC 1712 (2016); R. v. Edwards and Brown, 2014 ONSC 6323 (2014).
[39] R. v. Wise, 1 S.C.R. 527 (1992).
[40] *Id.*
[41] *Id.*
[42] In one lower court in British Columbia, a judge decided that location data collected by the RCMP while tracking a ship with a satellite tracking device (installed on the ship by Greek authorities, unlawfully, in Greece) should not be excluded from trial because it would not "irremediably taint the fairness of the trial itself." R. v. Guilbride, 2003 BCPC 44 (CanLII), <http://canlii.ca/t/5cs5>, retrieved on 2017-01-13.
[43] R. v. Vu, 3 SCR 657 (2013).

In *R v. Fearon*,[44] the SCC held that the search of a cell phone incident to arrest must be conducted in a particular way, due to the intrusiveness of such a search. Specifically, the court held that, to be permissible under section 8, a search of a cell phone incident to arrest must meet the following conditions:

> First, the arrest must be lawful.
>
> Second, the search must be truly incidental to the arrest. This requirement should be strictly applied to permit searches that must be done promptly upon arrest in order to effectively serve the law enforcement purposes….
>
> Third, the nature and the extent of the search must be tailored to its purpose. In practice, this will mean that only recently sent or drafted emails, texts, photos and the call log will, generally, be available, although other searches may, in some circumstances, be justified.
>
> Finally, the police must take detailed notes of what they have examined on the device and how they examined it. The notes should generally include the applications searched, the extent of the search, the time of the search, its purpose and its duration.

Other relevant cases have found limited (but still existent) expectations of privacy in IP addresses (at least in cases involving serious offences)[45] and in work-issued computers.[46]

[44] R. v. Fearon, [2014] 3 SCR 621.
[45] R. v. Spencer, [2014] 2 SCR 212.
[46] R. v. Cole, [2012] 3 SCR 34.