Digital Devices and Eroding Privacy From the Police

Section 8 of the *Canadian Charter of Rights and Freedoms* states, "Everyone has the right to be secure against unreasonable search or seizure."[i] This broad statement began its jurisprudential interpretive journey in the case of *Hunter v Southam* when the Canadian government, under statutory authority, authorized several civil servant investigators to enter the Edmonton Journal newspaper office and conduct a search of the premises.[ii] There were several key developments in the interpretation of section from this case. Some of the most notable include that section 8 is in place to *prevent* unreasonable searches and not to provide a tool *after* a search has occurred; **therefore warrantless searches are considered to be *prima facie* unreasonable**.[iii] However, the Supreme Court of Canada ("the SCC") did not stop there, they also held that the legislation that had 'allowed' the search was defective in two key ways: 1.) The person authorizing the search (i.e. signing the warrant) was not impartial;[iv] and 2.) The legislation in question provided no standard or criteria for when a warrant could be issue therefore the SCC specified that the *minimum* standard for a search to be compliant with section 8 would be that there are, "reasonable and probable grounds, established upon oath, to believe that an offence has been committed…"[v]

These principals from *Hunter* are still important today upholding the standard of search and seizure by not only providing a starting point for assessing warrantless searches which are as mention above, *prima facie* unreasonable but also by providing clear directions on what are the absolute minimums standards for a valid search.[vi]

With that as our backdrop it could be assumed that Canadians have fairly strong search and seizure legislation with the jurisprudential history to back it up. However, it can be argued that there has been a gradual trend towards the weakening of section 8 *Charter* rights through the

introduction of stronger powers of police (or other officials) to search individuals. This is especially so when we look at how technology is affecting the type and amount of information not only that we carry with us, but how the state is able to use technology to search Canadians. This post will give a brief introduction to the types of technology that have been found to be considered as 'fair searches' by the SCC, followed by an assessment of how we are treating searches of technology such as our cellphones or similar devices.

The first case we are looking at is *R v Plant* where the SCC held that individuals do not have a reasonable expectation of privacy regarding electricity records (i.e. your Manitoba Hydro records).[vii] In *Plant*, the police had received an anonymous tip that a home was a marijuana grow-op.[viii] The police pulled up the homes electricity records which indicated that a higher than usual amount of electricity was being used.[ix] The police conducted a warrantless perimeter search and observed activities that might suggest there was a grow-op on the property, and on the basis of this information had a search warrant issued.[x] What is important for the analysis here is not actually the *warrantless* perimeter searches (which the SCC did find violated section 8 of the *Charter*) but actually **the computerized search of the electricity records**.[xi] The SCC concluded that electrical consumption records "reveals little about an individual's lifestyle or private decisions" and therefore these records do not fall within section 8 protections.[xii] In other words, Canadians do not have a reasonable expectation of privacy regarding their electricity records. However, as the dissent suggested, this seems counter-intuitive, because if you consider how and what these records demonstrated for Plant, they actually revealed a ton of information about their lifestyle and private decisions.[xiii]

Next, in *R v Tessling* we see what could be characterized as an even larger jump in how the state can now validly use technology to gain information.[xiv] Similarly to *Plant*, the police had

received tips that there may be a marijuana grow in the home.[xv] However, in this case, when the police pulled the electricity usage records, it did *not* show abnormal usage.[xvi] Still, the police continued their investigation and used what is called FLIR technology which records images of thermal energy or heat radiating from a building which enabled them to identify unusual heat patterns.[xvii] From there, the police got a warrant, the home was search and a grow up was discovered.[xviii]

The SCC held that the image that the FLIR technology took an image of the *exterior* of the home, and although the "home" has traditionally been "accorded the highest degrees of privacy" in this case, the FLIR technology does not "see" into the home, but merely views the exterior walls which is information available to the public.[xix] The SCC stated the following:

> Certainly FLIR imaging generates information about the home but s. 8 protects *people*, not *places*. The information generated by FLIR imaging about the respondent does not touch on "a biographical core of personal information", nor does it "ten[d] to reveal intimate details of [his] lifestyle" (Plant, at p. 293). It shows that some of the activities in the house generate heat. That is not enough to get the respondent over the constitutional threshold. [Emphasis added][xx]

This same concept was applied in *R v Gomboc,* where the police had installed a digital recording ammeter (DRA) which recorded electrical flow in a home and can demonstrate electricity usage that is consistent with a grow op.[xxi] The SCC seemed to equate the information from the DRA with the electricity readings from *Plant* and the FLIR readings in *Tessling* noting *"*Indeed, the nature of the information has not changed nor is what was disclosed by the DRA about private and intimate activities in the home any more revealing than the information at issue

in *Tessling* and *Plant*."[xxii] In *Gomboc*, the SCC actually went as far as saying that it would be "strange" if the police could have access to electrical billing information and *not* to the DRA because the DRA provides better and more accurate information.[xxiii] They argue, that by allowing DRA evidence in they would actually protect more Canadians privacy because it would prevent more "intrusive methods of investigation" by confirming whether or not a grow-op was identified; if the DRA did not show unusual electricity readings they would not proceed with a search.[xxiv] However, this seems to really open up when devices like DRA's, or information similar in type to electricity readings can be used. If the standard has become that the state will be permitted to intrude *just so* they do not have to intrude more, it seems to be setting a risky precedent and unusually low standard.

With this really brief overview the question remains as to why Canadians are not more concerned about this? It may be fair to say that many Canadians have become trite with the protection of their section 8 rights or that many Canadians are in fact supportive of increasing government powers (aka greater police powers). Broadly, Canadians may be willing to pass up some of their "dignity, integrity and autonomy"[xxv] for the assumption that greater police powers reinforce concepts of protecting the greater good or to 'get the bad guy.' Another issue may be that many Canadians do not see themselves as being at risk of being the victim of an intrusion of their privacy *especially* if they are not doing anything wrong. I myself am guilty of this when I blindly agree to Facebook's request for my information because I think *that I have nothing to hide*.

Perhaps using court cases are bad examples of trying to demonstrate why we should ensure we are enforcing section 8 *Charter* rights. Usually the reason these cases end up in court is because the person who was searched was in fact doing something wrong! Perhaps Canadians

have less sympathy for Plant, Tessling or Gomboc's section 8 rights when they are dealing drugs. Further, our justice system has a clear objective to hold people accountable for the illegal things they do and perhaps as Canadians in these contexts it feels like limiting someone's rights is fair.

Maybe a better example is when "normal" or "innocent" people feel unjustly searched. For example, when you are at a border crossing or at an airport. It is clear that as a society we have decided that this is an area where all people have a lower expectation of privacy to ensure security at our borders. However, one of the issues that has crept up regarding these searches is whether they extend to our cell phones or similar devices.

In Canada the power for border guards to search you is found in Section 99(1)(a) of the Customs Act. It states that border offices may "at any time up to the time of release, examine any *goods* that have been imported and *open or cause to be opened any package or container* of imported goods and take samples of imported goods in reasonable amounts."[xxvi] However, if we look at previous SCC decisions regarding cell phones *specifically* it is clear that our devices have not been treated similarly as other goods or other means of storing information because of their unique ability to contain so much of our personal information.[xxvii] In *R v Fearon* the SCC concluded that the search of a cell phone had the potential to a be a much more significant invasion of privacy than a "typical" search.[xxviii] This case might mean that our devices are actually not like all "goods" and perhaps require more protection at the border.

This question has not yet made its way to the SCC and currently, however on the website for the Office of the Privacy Commissioner of Canada it sates the following regarding the current policy on cell phone, tablet, and laptop searches at the Canadian border:

"…The Canadian courts have not yet ruled on whether a border officer can compel a person to

turn over their password and on what grounds, so that their electronic device may be searched at a border crossing. While the law is unsettled, CBSA policy states that examinations of personal devices should not be conducted as a matter of routine; such searches may be conducted only if there are grounds or indications that "evidence of contraventions may be found on the digital device or media." If your laptop or mobile device is searched, it should be searched in line with this policy and, in that context, you will likely be asked to provide your password. If you then refuse to provide your password, your device may be held for further inspection. According to the policy, officers may only examine what is stored within a device, which includes, for example, photos, files, downloaded e-mails and other media. Officers are advised to disable wireless and internet connectivity, limiting access to any data stored external to the device, for instance, on social media or in a cloud…"[xxix]

However, there seems to be anecdotal evidence in the media of people who have been stopped and had their devices searched at the border without the necessary "grounds" to search the device and/or ignoring issues such as client/solicitor privilege. You can read the stories here, here and here.[xxx] Further, civil liberties advocates have questioned whether the *Customs Act* should even apply to cellphones or other devices because the *Customs Act* was enacted we;; before cellphones and similar devices were created and being used like they are today. These advocates argue that the *Customs Act* therefore could not take into account the unique context of cellphones at a border creates.[xxxi]

As mentioned, the SCC has not ruled on the constitutionality of these searches but in Manitoba, one decision did make its way before the courts. The Manitoba court ruled that if border officers are to search phones, they have to abide by the limits defined in *Fearon* therefore the search to be lawful there would have to be a relevant law enforcement purpose for the search,

the search could not be indiscriminate, and officers would be required to take detailed notes on what was searched and how.[xxxii]

In the past, there seems to have been a slow undercutting of our section 8 rights. As we begin to carry technology on us that holds vast amount of information, this may be the impetus needed for Canadians to ensure that these rights are not further eroded. At this point, there has not been sufficient judicial scrutiny to see how courts will assess what level of privacy that our cellphones should receive but it seems reasonable that they should not be considered similarly as other 'goods' and in fact will require a different approach.

This is not an argument for there to be no oversight on what we carry on our phones and computers but rather a review on standard that meets the current (and evolving) technology. At this time this question is unanswered until the SCC has the opportunity to close this jurisprudential gap.

---

i *Canadian Charter of Rights and Freedoms*, s 8, Part 1 of the *Constitution Act, 1982* being Schedule B to the *Canada Act 1982* (UK), 1982, c11 [*Charter*].
ii *Hunter et al v Southam Inc*, [1984] 2 SCR 145, [1984] 6 WWR 577 [*Hunter*]
iii *Hunter* at para 146.
iv *Ibid*.
v *Ibid* at para 147.
vi *Ibid* at paras 146-147.
vii *R v Plant*, [1993] 3 SCR 281 at para 2, [1993] SCJ No 97 [*Plant*].
viii *Plant* at para 2.
ix *Ibid*.
x *Ibid*.
xi *Ibid* at para 22.
xii *Ibid* at para 27.
xiii *Ibid* at paras 49-53.
xiv See Generally *R v Tessling*, 2004 SCC 67 [*Tessling*].
xv *Ibid* at para 4.
xvi *ibid* at paras 2, 5.
xvii *Ibid* at paras 5-6.
xviii *Ibid* at para 6.
xix *Ibid* at paras 45, 47.
xx *Tessling supra* note xiv, citing *Plant* at para 28.

[xxi] *R v Gomboc*, 2010 SCC 55 at paras 61, 63 [*Gomboc*].
[xxii] *Ibid* at para 38.
[xxiii] *Ibid* at para 52.
[xxiv] *Ibid*.
[xxv] *Plant supra* at note vii at para 17.
[xxvi] *Customs Act*, RSC, 1985, c 1 (2nd Supp), s 99(1)(a).
[xxvii] See Generally *R v Vu*, 2013 SCC 60.
[xxviii] See Generally *R v Fearon*, [2013] SCCA No 141, [2013] CSCR no 141 [*Fearon*].
[xxix] https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/your-privacy-at-airports-and-borders/
[xxx] https://www.cbc.ca/news/technology/lawyers-canada-warrantless-smartphone-searches-customs-act-1.4247036; https://www.cbc.ca/news/technology/border-phone-laptop-search-cbsa-canada-cbp-us-1.4002609; https://www.cbc.ca/news/business/cbsa-boarder-security-search-phone-travellers-openmedia-1.5119017
[xxxi] https://www.cbc.ca/news/technology/lawyers-canada-warrantless-smartphone-searches-customs-act-1.4247036.
[xxxii] https://www.cbc.ca/news/technology/lawyers-canada-warrantless-smartphone-searches-customs-act-1.4247036.