CANADIAN PRIVACY LAW REVIEW

Volume 12 • Number 3 February 2015

In This Issue:

Warrantless Searches of Cell Phones upon Arrest Are Lawful in Canada—but Strict Safeguards Apply

Pierre-Christian Collins Hoffman
Lawyer
McMillan LLP

Guy Pinsonnault
Partner
McMillan LLP

Joshua Chad
Lawyer
McMillan LLP

The Supreme Court of Canada has found that under certain circumstances, law enforcement officers may perform a warrantless search of the contents of a lawfully arrested individual's cell phone via their ancillary search powers. This landmark decision in *R. v. Fearon*[1] reached by a 4:3 majority was released on December 11, 2014.

While they differed in their ultimate ruling, both the majority and dissenting justices noted that significant privacy issues arise within the specific context of cell phone search that make this type of search different from the standard search incident to arrest.

The Canadian position on cell phone searches incident to arrest therefore contrasts with that of the United States, where, in the recent case of *Riley v. California*,[2] the U.S. Supreme Court unanimously ruled that police must obtain a warrant to search the cell phone of an arrestee.

Facts

Two robbers (one armed with a handgun) stole jewellery from a merchant as she was loading her vehicle, and fled by car. Shortly thereafter, police officers arrested two suspects, Fearon and Chapman, and located the getaway vehicle.

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

ISBN 0-433-44417-7 ISSN 1708-5446
ISBN 0-433-44418-5 (print & PDF)
ISBN 0-433-44650-1 (PDF)
ISSN 1708-5454 (PDF)

Subscription rates: $280.00 (print or PDF)
$425.00 (print & PDF)

Upon the arrest of the suspects, the police proceeded with the usual pat-down search and found a cell phone on the person of Fearon not protected by password, the contents of which they browsed. The device contained an incriminating draft text message and the picture of a handgun. After obtaining a warrant, the police searched the vehicle and found the handgun depicted in the photo.

The trial judge found that s. 8 of the *Canadian Charter of Rights and Freedoms* (the "Charter"),[3] which entrenches the right to be secure against unreasonable searches and seizures, had not been breached by the warrantless search of the cell phone. Fearon was convicted of armed robbery (among other offences), and he appealed. The Ontario Court of Appeal dismissed the appeal.[4]

Decision of the Supreme Court

Justice Cromwell, writing for the majority, dismissed the appeal and found "that there were important law enforcement objectives to be served by a prompt search of aspects of the phone"[5] but that the officers' evidence with respect to the extent of the search was insufficient, thus making it unreasonable. He explained that Canadian courts to date had provided four different views as to whether the search incident to arrest powers of the police extended to permit the searching of cell phones:

1. Searches of cell phones are permitted.
2. "Cursory" searches of cell phones are permitted.
3. "Data-dump" cell phone searches are not permitted.
4. Searches of cell phones are not permitted, except in exigent circumstances where a "cursory" search may be permissible.

The majority elected to go with none of these approaches as Cromwell J. advocated for setting "meaningful limits" on cell phone searches incident to arrest. For these searches, police must limit the scope of the search, the purposes of the search, and keep detailed notes of what they searched on the phone and why such a search was required as being incident to arrest. In particular, Cromwell J. noted that in general, "only recently sent or drafted emails, texts, photos and the call log may be examined as in most cases only those sorts of items will have the necessary link to the purposes for which prompt examination of the device is permitted [emphasis added]".[6]

The majority judges further affirmed the notion that searching the entire contents of a cell phone is equivalent to searching a computer, and triggers considerable privacy interests, drawing a parallel with the Supreme Court's decision in *R. v. Vu* [*Vu*],[7] where it had held that a specific authorization is required to conduct the search of a computer or a cell phone found during the search of an individual's residence, performed under a warrant issued for the search of the premises.

However, in keeping with the majority's view of the ability to set "meaningful limits" on a search, Cromwell J. highlighted that a targeted cell phone search would not always trigger these extreme privacy interests, as opposed to seizure of bodily samples and strip searches, which are "very great invasions of privacy"[8] no matter how they are conducted.

It is also worth noting that contrary to what the Court of Appeal had concluded, Cromwell J. held that whether or not a phone is password protected should not change an individual's expectation of privacy. The fact that an individual did not protect his cell phone by password does not constitute a waiver of his/her privacy interests. However, it is unclear from the majority decision how police would, in practice, be expected to perform a search incident to arrest on a password-protected phone.

The majority of the Supreme Court summarized as follows the conditions under which a warrantless cell phone search incident to an arrest will not be unconstitutionally unreasonable:

1. The arrest was lawful.
2. The search was truly incidental to the arrest pursuant to valid law enforcements purposes, namely:
   (a) protecting the police, the accused, or the public;
   (b) preserving evidence; or
   (c) discovering evidence (only where the investigation will be stymied or significantly hampered absent such search).
3. The scope and nature of the search is tailored to its purpose.
4. The police have taken detailed notes of their examination and way the device was searched.

The majority ultimately found that the search was conducted in breach of s. 8, but only for want of evidence detailing to what extent, how, and why the device was examined. Nevertheless, the majority refused to exclude the evidence as remedy for the violation of Fearon's rights, reasoning, *inter alia*, that the invasion of privacy of the accused was not particularly serious in the circumstances.

Justice Karakatsanis, writing for the dissent, opined that the police were required to obtain a warrant before searching the cell phone. Specifically, Karakatsanis argued that except in exigent circumstances, a warrant would be required to search a person's phone or other personal digital device, even as part of a search incident to arrest. The dissent was not opposed to searching cell phones but argued that a warrant is required to ensure that individuals' privacy interests are appropriately protected. It noted that "a telewarrant can usually be obtained relatively quickly and with little harm to the investigation"[9] and that the police "were entitled to seize the phone pending an application for a warrant".[10]

Impact on White Collar Crime

The decision of the Supreme Court was rendered in the context of armed robbery, a violent crime, which can be distinguished from economic offences such as fraud, corruption, or criminal competition offences. As Cromwell J. noted, in the particular circumstances of this case, "the police knew a dangerous weapon was on the streets".[11] In such a situation, the incident search of a cell phone appears much more justified and reasonable, given the imminent danger for the safety of the public. Justice Cromwell observed that law enforcement objectives permitting incident searches of cell phones will be "most compelling" in cases of "violence or threats of violence, or that in some other way put public safety at risk [...] or serious property offences that involve readily disposable property, or drug trafficking".[12]

Such circumstances are dissimilar to those where, for instance, the cell phone of an arrestee would be searched on suspicions of participation in financial fraud unless it is apparent that evidence could be lost absent a search incident to the arrest. Where the incident search is conducted for purposes of discovering evidence, "great circumspection" is required: a warrantless examination of the device upon arrest will only be permitted if "the investigation will be stymied or significantly hampered".[13]

In our view, upon the arrest of an individual suspected of having committed an economic offence, searches of cell phone devices would still require a warrant in most cases. Unlike offences such as robbery involving "readily disposable property", white collar crime generally involves no imminent risk of another offence being committed or violence. In other words, there will rarely be an element of urgency, which can, for other types of offences, permit some limited search of a cell phone.

With respect to competition offences, it should be noted that unlike police officers, Competition Bureau agents do not possess incident search powers and must always, save for exceptional circumstances, obtain a warrant to search the contents of a cell phone.

Comments

The Supreme Court attempted to strike a balance between effective law enforcement and the protection of significant privacy interests impacted by cell phone searches. The majority ruled in favour of a system under which police officers may carry out incidental cell phone searches upon arrest, but pursuant to rather stringent safeguards.

Although the Majority in this case permitted the evidence gathered from the warrantless search of a cell phone to be used against the accused, both the dissent and the majority agreed that the search of a cell phone triggers significant privacy interests. Even in the majority's opinion, the type of cell phone review that is permitted and the circumstances when such a review is permitted are very limited. A strong argument can be made that, outside of the search incident to arrest context, a cell phone search would require a warrant that has specifically considered the privacy interests triggered by this type of search.

Despite such safeguards, the ruling of the Supreme Court means that complete trust is given to police officers with respect to the scope and extent of cell phone examinations incident to arrest. As the dissenting justices noted, "it is very difficult—if not impossible—to perform a meaningfully constrained targeted or cursory inspection of a cell phone or other personal digital device".[14] While the police must detail their search of the device, there will generally be no way to confirm that they did not peer into the contents of the device further than stated in their report.

As Cromwell J. previously recognized in *Vu*, protocols limiting the way in which a computer may be searched are not, as a general rule, required for a warrant. The dissent observed that the same reasoning applies to cell phones but did not preclude the development of such protocols, highlighting that in performing a cell phone search, with or without a warrant, the authorities must not extend the search beyond the scope of the grounds permitting it. Grounds to search a cell phone for a specific purpose cannot provide *carte blanche* to roam the person's digital life without restraint.

In the context of economic crimes, authorities should be proactive and suggest to the court, when applying for a warrant to search a cell phone, a protocol to protect the powerful privacy interests entailed by such digital devices, which may contain records of *viva voce* private communications and sometimes be able to track the location where one was while in possession of the device.

As the dissent observed, seizure of the cell phone pending the granting of a warrant may serve to preserve the evidence contained therein, and telewarrants may be obtained within a relatively short period; however, it is worth noting that functions and applications available on smart phones permit the user to remotely erase all data contained on the

device. The approach sustained by the majority will arguably be able to prevent the destruction of evidence using such methods.

Finally, we note that the Supreme Court did not make an observation as to whether an accused could be compelled to provide his or her password to a locked device during an incident search. The Quebec Court of Appeal held in 2010 that a warrant compelling the accused to provide the password to his computer with a view to incriminate him breached the constitutional protection against self-incrimination and rendered the subsequent seizure of data unreasonable under s. 8 of the Charter.[15]

---

1 [2014] S.C.J. No. 77, 2014 SCC 77.
2 573 U.S. ___ (2014).
3 *The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK)*, 1982, c. 11.
4 *R. v. Fearon*, [2013] O.J. No. 704, 2013 ONCA 106.
5 *Supra* note 1, para. 86.
6 *Ibid.*, para. 76.
7 [2013] S.C.J. No. 60, 2013 SCC 60.
8 *Supra* note 1, para. 55.
9 *Ibid*., para. 138.
10 *Ibid*., para. 106.
11 *Ibid*., para. 68.
12 *Ibid*., para. 79.
13 *Ibid*., para. 80.
14 *Ibid*., para. 164.
15 *R. v. Boudreau-Fontaine*, [2010] Q.J. No. 5399, 2010 QCCA 1108.