Searches of Digital Devices Incident to Arrest: R v Fearon

Steven Penney*

On May 23, 2014, the Supreme Court of Canada is scheduled to hear the appeal in *R v Fearon*.[1] *Fearon* raises the questions of whether, and under what circumstances, police may conduct warrantless searches of digital devices seized under their common law power to search incident to arrest. Against the weight of the jurisprudence, I argue in this comment that, absent exigent circumstances, such searches violate section 8 of the *Canadian Charter of Rights and Freedoms (Charter)*.[2]

In *Fearon*, police arrested the accused for armed robbery, performed a pat down search, and found a mobile phone on his person. The arresting officer examined the phone's contents and found incriminating photographs and text messages.[3] At trial, the accused sought the exclusion of this evidence under section 24(2) of the *Charter* on the basis that the warrantless search of the phone violated his section 8 right to be secure against unreasonable searches and seizures. The trial judge found that there was no infringement and the Ontario Court of Appeal unanimously affirmed, concluding that the examination of the phone was a lawful incidental search and rejecting calls by the accused and interveners to impose strict, *ex ante* limits on incidental searches of digital devices.

The power to search incident to arrest is a longstanding common law police power.[4] Briefly, it allows police to search an arrestee's person and belongings, as well as the immediate vicinity of the arrest,[5] when there has been a lawful arrest[6] and the search is aimed at uncovering weapons or evidence relating to the offence arrested for.[7] Police do not need probable grounds, however, to believe that they will find weapons or evidence.[8] Instead, the justification for the search stems from the probable grounds required for arrest[9] and the need for police to have a reasonable belief that the search may uncover weapons or evidence.[10]

Applying this framework in *Fearon*, the Court concluded that police had a reasonable belief that they might find incriminating texts or photographs by looking at the phone and that this kind of "cursory look" fell inside the ambit of the search incident to arrest power.[11] It intimated, however, that the subsequent searches at the police station may have exceeded the limits of the power.[12] But since the trial judge found that these searches were still connected to the immediate investigation, and since no evidence was found, the Court concluded that section 8 was not violated.[13]

The Court also declined the accused's and interveners' invitations to carve out an exception to the search incident to arrest power for electronic devices.[14] But following the approach first set out in *R v Polius*,[15] it indicated that incidental searches of digital devices should be limited to "cursory" examinations of unlocked material.[16] More thorough, technical examinations (including any required to defeat password protection) would require a warrant.[17] Most courts have come to similar conclusions.[18]

But why require warrants to search digital devices when they are not needed to search other belongings containing potentially sensitive personal information? In answering this question, it is helpful to understand why warrants are generally not required for incidental searches. While the doctrine has not received a thorough justification, the Supreme Court of Canada has noted that incidental searches are "relatively non-intrusive"[19] and that a warrant requirement would risk both officer safety and the loss of evidence.[20]

Given that arrest entails a substantial deprivation of liberty and creates a significant risk of discriminatory profiling,[21] it is arguable that police should have to obtain warrants to arrest when feasible.[22] Warrantless arrest powers, however, have been around for a long time[23] and have withstood *Charter* scrutiny.[24] So the question is whether incidental searches conducted without warrants or probable grounds to believe that evidence will be found are reasonable under section 8 of the *Charter*.

As a general matter the answer should be "yes."[25] Requiring warrants or evidence-based probable grounds would do little to protect privacy or liberty, but the costs to law enforcement would be substantial. Consider the case where police have probable grounds to arrest but turn out to be mistaken, *i.e.*, the arrest is lawful but the suspect innocent. Such a person will be often be manhandled,[26] handcuffed,[27] questioned, detained for a lengthy period,[28] fingerprinted, and photographed.[29] Permitting police to frisk and search belongings and immediate surroundings in these circumstances causes little additional harm. If police were required to apply for a warrant or develop evidence-related probable grounds, in contrast, valuable evidence would often be lost.

The situation is different for mobile digital devices, however. These technologies enable access to staggering amounts of information about both the arrestee and third parties, with many of the latter being unconnected to suspected criminal activity.[30] It is therefore sensible to treat digital devices differently than bags, suitcases, or purses.[31]

Indeed, in its recent decision in *R v Vu*, the Supreme Court of Canada strongly hinted that it would not permit unrestrained searches of digital devices incident to arrest. There, it concluded that a warrant to search a residence (and any documents found therein) could not authorize the search of computers or cell phones found during the execution of the search, even if those devices might reasonably contain relevant documents. Highlighting their enormous storage capacities, Justice Cromwell concluded for a unanimous Court that section 8 requires police to have specific authorization to search digital devices.[32] If they find one while executing a warrant that lacks such an authorization, they may seize it if they reasonably believe it contains evidence related to an offence.[33] But they may not search it unless they first obtain a warrant to do so.[34] Though Justice Cromwell warned that his reasons should not be interpreted to "disturb the law that applies when a computer or cellular phone is searched incident to arrest,"[35] his logic points strongly to a rule forbidding unrestricted access to digital devices during such searches.

Requiring prior judicial authorization before non-cursory searches would help ensure that such searches are justified by probable grounds and restricted (so far as feasible) to examinations of potentially relevant data.[36] As judges[37] and commentators[38] have recognized, requiring a warrant is much more effective in preventing unjustified searches than requiring probable grounds without a warrant. In carrying out their crime control and public safety mandates, police have strong incentives to invade people's privacy. Without *ex ante* constraints on their discretion, police will systematically favour these mandates over privacy.[39] While the possibility of *ex post* review (and the prospect of evidentiary exclusion) provides some incentive to adhere to *Charter* norms,[40] compliance is strengthened by requiring prior authorization by a neutral arbiter.[41] Police are unlikely to spend time applying for warrants, moreover, unless those applications are likely to succeed.[42] Searches authorized by warrants are therefore more likely to uncover evidence of crime than warrantless searches.[43]

So it makes sense to constrain the ability of police to conduct warrantless searches of digital devices incident to arrest. The next question is whether the *Polius* model – permitting only "cursory" searches without a warrant – strikes the right balance. In my view, it does not. The problem is the indeterminacy of "cursory". Depending on the nature of the device and its operating system, quantity and type of information contained in it, sophistication of the police examining it, and other factors, the intrusiveness of a cursory search may vary greatly. A cursory search conducted by an inexperienced or technically naïve officer, moreover, could inadvertently result in the loss of valuable evidence.[44]

The Supreme Court of Canada should therefore adopt a bright-line rule forbidding incidental searches of digital devices absent a warrant or exigent circumstances.[45] Unlike the concept of a "cursory" search, exigency is a well understood standard that police should be able to apply reasonably accurately. Where police reasonably believe that applying for a warrant would risk the loss of evidence, warrantless searches are reasonable under section 8 of the *Charter*.[46] This approach provides maximum protection for privacy without significantly compromising the ability of police to obtain relevant evidence from digital devices.

Notes

* Professor, Faculty of Law, University of Alberta

1 2013 ONCA 106 [*Fearon*], leave to appeal to SCC granted, [2013] SCCA No 141.

2 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

3 Police conducted further searches of the phone at the police station, but no additional evidence was uncovered. *Fearon*, *supra* note 1 at para 16.

4 See generally Steven Penney, Vincenzo Rondinelli & James Stribopoulos, *Criminal Procedure in Canada* (Markham, ON: LexisNexis, 2011) at paras 3.275-3.304 [Penney].

5 See *Cloutier v Langlois*, [1990] 1 SCR 158 at 186, [1990] SCJ No 10 [*Cloutier*].

6 See *ibid* at 180-81; *R v Stillman*, [1997] 1 SCR 607 at para 27, [1997] SCJ No 34 [*Stillman*]. Police may not, however, take bodily samples or search bodily cavities. *Stillman, ibid* at paras 41-43, 87. See also *R v Simmons*, [1988] 2 SCR 495 at 517, [1988] SCJ No 86; *R v Greffe*, [1990] 1 SCR 755, [1990] SCJ No 32. And they may conduct strip searches only under very limited circumstances. See *R v Golden*, [2001] 2 SCR 679, [2001] SCJ No 81.

7 *Cloutier*, *supra* note 5 at 186; *R v Caslake*, [1998] 1 SCR 51 at para 22, [1998] SCJ No 3 [*Caslake*].

8 *Cloutier*, *supra* note 5 at 179-81.

9 See *Caslake*, *supra* note 7 at para 13; *R v Nolet*, 2010 SCC 24, [2010] 1 SCR 851 at para 51; *Cloutier*, *supra* note 5 at 179-81.

10 *Caslake, ibid* at paras 19-20.

11 *Fearon*, *supra* note 1 at para 57. The court also noted that the phone "was not password protected or otherwise 'locked'." *Ibid*.

12 *Ibid* at para 58.

13 *Ibid* at paras 58-59.

14 *Ibid* at para 64.

15 [2009] OJ No 3074, 196 CRR (2d) 288 at paras 52-57 (Ont Sup Ct) [*Polius*].

16 *Fearon*, *supra* note 1 at para 73.

17 *Ibid* at paras 73-75.

18 See e.g. *R v Hiscoe*, 2013 NSCA 48 at paras 69-78, 297 CCC (3d) 35 [*Hiscoe*]; *R v Finnikin*, [2009] OJ No 6016 (available on CanLII), (Ont Sup Ct); *R v McBean*, 2011 ONSC 878, 228 CRR (2d) 11; *R v Little*, [2009] OJ No 3278 (available on CanLII), (Ont Sup Ct); *R v D'Annunzio*, [2010] OJ No 4333, 224 CRR (2d) 221 (Ont Sup Ct). See also *R v Manley*, 2011 ONCA 128 at para 39; 228 CRR (2d) 45 (suggesting, without deciding, that the *Polius* approach is correct).

19 *Cloutier*, *supra* note 5 at 185.

20 *Stillman*, *supra* note 6 at para 33.

21 See Penney, *supra* note 4 at para 2.154.

22 See *Criminal Code*, RSC 1985, c C-46 ss 494-95 (setting out warrantless arrest powers).

23 See *Criminal Code, 1892*, SC 1892, c 29 s 552.

24 See generally *R v Feeney*, [1997] 2 SCR 13; [1997] SCJ No 49 (warrants only constitutionally required for residential arrests in non-exigent circumstances).

25 See Steven Penney, "Unreasonable Search and Seizure and Section 8 of the Charter: Cost-benefit Analysis in Constitutional Interpretation" in Errol Mendes & Stéphane Beaulac, eds, *Canadian Charter of Rights and Freedoms* (Toronto: LexisNexis, 2013) 751 at 785-86.

26 See *Criminal Code*, s 25(4) (authorizing use of reasonable force).

27 See *Fraser v Soy*, [1918] NSJ No 5, 30 CCC 367 (NSSC); *Hamilton v Massie*, [1889] OJ No 143, 18 OR 585 (Ont H Ct J).

28 See *Criminal Code*, s 503(1)(a) ("where a justice is available within a period of twenty-four hours after the person has been arrested ... the person shall be taken before a justice without unreasonable delay and in any event within that period"); Penney, *supra* note 4 at paras 5.41-5.47.

29 See *Identification of Criminals Act*, RSC 1985, c I-1. Also see *R v Beare; R v Higgins*, [1988] 2 SCR 387, [1987] SCJ No 92 (upholding constitutionality of legislation).

30 See *R v Vu*, 2013 SCC 60 at para 38, [2013] SCJ No 60 [*Vu*] ("[a] lthough historically cellular phones were far more restricted than computers in terms of the amount and kind of information that they could store, present day phones have capacities that are, for our purposes, equivalent to those of computers"). See also Adam M Gershowitz, "Why *Arizona v Gant* Is the Wrong Solution to the Warrantless Cell Phone Search Problem" 94 BUL Rev [forthcoming in 2014]; Orin S Kerr, "Foreword: Accounting for Technological Change" (2013) 36 Harv JL & Pub Pol'y 404 at 404-05.

31 See *Hiscoe*, *supra* note 18 at para 75.

32 *Ibid* at paras 40-48.

33 *Vu*, *supra* note 30 at para 49.

34 *Ibid*.

35 *Ibid* at para 63.

36 This might include conditions minimizing intrusions on the privacy of third parties. See *R v Thompson*, [1990] 2 SCR 1111; [1990] SCJ No 104.

37 See *Hunter v Southam Inc*, [1984] 2 SCR 145 at 160, [1983] SCCA No 408 (section 8's purpose is to prevent unjustified searches "before they happen;" not to simply decide, after the fact, "whether they ought to have occurred").

38 See Max Minzner, "Putting Probability Back into Probable Cause" (2009) 87 Texas L Rev 913.

39 See generally Ric Simmons, "Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment" (2013) 36 Harv JL & Pub Pol'y 449 at 567 (police "overly sympathetic" to intrusive surveillance because the "privacy cost of these methods is externalized (that is, the privacy cost is not borne directly by the law enforcement agency and is therefore not a part of their internalized cost-benefit analysis)").

40 See Steven Penney, "Taking Deterrence Seriously: Excluding Unconstitutionally Obtained Evidence Under Section 24(2) of the *Charter*" (2004) 49 McGill LJ 105 at 125.

41 See *Hunter*, *supra* note 38 at 161-62 ("[t]he purpose of a requirement of prior authorization is to provide an opportunity, before the event, for the conflicting interests of the state and the individual to be assessed, so that the individual's right to privacy will be breached only where the appropriate standard has been met, and the interests of the state are thus demonstrably superior").

42 See Donald Dripps, "Living With *Leon*" (1986) 95 Yale LJ 906 at 926.

43 See William J Stuntz, "Warrants and Fourth Amendment Remedies" (1991) 77 Va L Rev 881 at 908, 920-25, 927; H Richard Uviller, *Tempered Zeal: A Columbia Law Professor's Year on the Streets with the New York City Police* (Chicago: Contemporary Books, 1988) at 25.

44 See *R v Cater*, 2012 NSPC 2 at para 57, 312 NSR (2d) 242 [*Cater*] .

45 See e.g. *R v Liew,* 2012 ONSC 1826 at paras 137ff, [2012] OJ No 1365.

46 See *R v Grant*, [1993] 3 SCR 223 at 242-43, [1993] SCJ No. 98. In deciding whether exigent circumstances existed, however, police and courts should be cognizant of the ability of tele-warrants. They should also be aware of inexpensive technologies available to prevent the remote manipulation of digital data after seizure. See Adam Gershowitz, "Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem" 22 Wm & Mary Bill Rts J (forthcoming in 2014), online: Social Science Research Network <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2313911>.