Canadian Journal of Law and Technology

Volume 16 | Number 2 Article 8

1-1-2016

Digital Evidence and the Adversarial System

Colton Fehr
PhD Candidate, University of Alberta

Digital Evidence and the Adversarial System: A Recipe for Disaster?

Colton Fehr*

Abstract

Scholars have observed that the adversarial system tends to provide courts with only a "small snapshot of the technological whole," which in turn forms the record upon which broader legal pronouncements occur. As a result, they contend that legislatures should be more proactive in making rules governing complex and rapidly advancing technologies, and that courts must show deference to these rules. Other scholars retort that, in practice, legislatures often fail to update obviously flawed and outdated privacy provisions. Whether due to special interest influence, majoritarian dislike of criminal suspects, or other institutional constraints, legislative responses have been wanting. As such, courts must often play a pivotal role in governing novel technologies. To help courts bear their burden more effectively, I make two general proposals. First, when courts must make or decide on the constitutionality of a rule, I suggest that the legislature should utilize the reference procedure, which is not inhibited by traditional trial constraints. Second, to aid courts in applying existing rules, I recommend tasking an independent institution with providing up-to-date reports of the current state of technologies expected to come before the courts. Counsel may use such complex and timely research to address gaps in technological evidence at trial.

INTRODUCTION

In the digital age, the capabilities of new and often complex digital technologies[1] change substantially over short periods of time. As digital evidence appears in courtrooms at an ever-increasing rate, judicial decisions concerning the legality of digital device searches and seizures have exposed weaknesses in the adversarial system of judicial decision making. As various scholars have concluded, the adversarial system tends to provide courts with only a "small snapshot of the technological whole."[2] In other words, judges are often forced to

---

* BA (Saskatchewan), JD (Saskatchewan), LLM (Toronto), PhD Candidate (Alberta). I would like to thank Professor Steven Penney and the external reviewer for their invaluable insights on previous drafts of this article. I would also like to acknowledge the generous support of the Social Sciences and Humanities Research Council of Canada for funding this and related work.

1 Throughout this article I use the term "digital" to describe anything which incorporates computer technologies.

2 See Daniel Scanlan, "Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times" (2012) 16 Can Crim L Rev 301 at 302; Steven Penney,

decide digital legal issues based on inadequate evidentiary records. Judges operating within the adversarial process are therefore disadvantaged when attempting to create clear rules or when interpreting legislation which governs the searches and seizures of digital technologies.[3]

Despite the existence of cogent examples of these problems,[4] scholars have considered few means to alleviate these issues related to the treatment of digital evidence. In this article, I make two recommendations. First, when courts must make or decide on the constitutionality of a rule in a case involving digital technologies,[5] I suggest that the legislature should utilize the reference procedure, which is not inhibited by traditional trial constraints. Second, to aid courts in applying existing rules that govern the treatment of digital technologies, I suggest that legislatures should task a body of neutral and impartial experts with informing the legal community of the current state of technology and its likely direction in the foreseeable future. Counsel may use such complex and timely research — which many overworked criminal lawyers cannot feasibly be expected to undertake[6] — to further their cases at trial. I contend that both recommendations will permit courts to make better informed and timelier decisions with respect to digital technologies.

The article unfolds as follows. I begin in Part I with an overview of the literature discussing the difficulties that judges encounter when creating and applying rules with respect to digital technologies. Although many scholars contend that these issues lead to the conclusion that courts should show significant deference to legislatures when deciding issues related to digital evidence, others have provided cogent reasons to reject this solution. In Part II, I provide a detailed example of the types of difficulties that courts have faced with respect to digital evidence by outlining the development of the law concerning the constitutionality of searching cell phones incident to arrest. In Part III, I discuss the aforementioned recommendations in further detail. In so doing, I use the discussion in Part II to test the feasibility of the suggestions offered.

"The Digitization of Section 8 of the *Charter*: Reform or Revolution?" (2014) 67 SCLR 505 at 530; Stephen Breyer, "Our Democratic Constitution" (2002) 77 NYU L Rev 245 at 261-63; Graham Mayeda, "My Neighbour's Kid Just Bought a Drone . . . New Paradigms for Privacy Law in Canada" (2015) 35 NJCL 59 at 79-81; Jordan Fine, "Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smart Phone Data Granted in *R v Fearon*" (2015) 13 CJLT 171 at 177-181.

3 See Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Mich L Rev 801 at 858-859, 869.

4 Examples will be discussed below.

5 As I discuss below, the jurisprudence with respect to searching cell phones incident to arrest provides a clear example.

6 See David Paciocco, "Proof and Progress: Coping with the Law of Evidence in a Technological Age" (2013) 11:2 CJLT 181 at 185.

I. DIGITAL TECHNOLOGIES AND THE ADVERSARIAL SYSTEM

It is common knowledge that judges operating within the adversarial system are generally required to base their decisions on written factums and oral arguments submitted by opposing parties. When dealing with rapidly evolving technologies, the evidentiary records upon which these arguments are made are often insufficient. This is because there is no guarantee that either party has sufficient technological knowledge to identify cases in which it is necessary to call upon expert witnesses to explain the intricacies of a particular technology.[7] Even if a party has sufficient financial resources, the party may not be motivated to call such evidence if it does not benefit his or her position in the case.[8] Also aggravating these difficulties is the fact that judges are limited by time and resource constraints.[9] Consequently, judges are often left to deliver legal pronouncements in an environment that scholars and judges have recognized as being "unusually complex."[10]

As cases reach higher courts, greater safeguards exist to catch technological mistakes made in lower courts. Not only do appellate courts employ more law clerks to research issues,[11] but cases at higher courts also tend to attract interveners who are frequently allowed to make submissions.[12] Nevertheless, scholars have observed that the inherent lag time between the introduction of new technologies and their eventual consideration by trial and appellate courts often renders judicial decisions of "historical interest only."[13] It may take many years before technologies used by suspects or police are legally challenged in a criminal trial.[14] Moreover, if one of the parties appeals, there would be further delay in waiting for an intermediate appellate court to decide the case.[15] Finally, if a case is one of the few to be heard by the Supreme Court of Canada (S.C.C.), the Court's decision would come many years after the initial search or seizure took place.[16]

---

7 See Kerr, *supra* note 3 at 875.

8 *Ibid.*

9 *Ibid* citing Henry Hart Jr., "Foreword: The Time Chart of Justices" (1959) 73 Harv L Rev 84 at 99-100.

10 Breyer, *supra* note 2 at 261; Kerr, *supra* note 3 at 877.

11 For instance, the Supreme Court of Canada permits three clerks per judge. See Supreme Court of Canada, "Law Clerk Program," online: < www.scc-csc.ca/about-apropos/empl/lc-aj-eng.aspx > .

12 For instance, in *R. v. Vu*, 2013 SCC 60, 2013 CarswellBC 3342, 2013 CarswellBC 3343, [2013] 3 S.C.R. 657, [2013] S.C.J. No. 60, at paras 43-44 [*Vu*], the Court relied upon an academic article as well as submissions by the Canadian Civil Liberties Association in rejecting a number of ill-suited metaphors used to justify searches of computers that were not specifically authorized in a warrant.

13 See Scanlan, "Issues in Digital Evidence," *supra* note 2 at 312; Kerr, *supra* note 3 at 868-869.

14 See Kerr, *supra* note 3 at 868.

15 *Ibid.*

Judges facing these problems are often aware of their limitations and, as a result, tend to craft broad rules that provide future courts adequate flexibility in assessing novel circumstances.[17] The result, however, is that judicial rules governing novel technological devices are often highly indeterminate. Law enforcement officers tasked with implementing such rules will generally favour *ex post* judicial determination of the legality of their conduct as they are generally less concerned with upholding constitutional rights, and more preoccupied with ensuring crime is detected and thoroughly investigated.[18] This leads to frequent litigation that perpetuates the challenges involved with creating expedient and informed decisions.

In comparison to courts, scholars contend that legislatures are institutionally better equipped to govern complex and rapidly changing technologies. One reason for this is that they are in theory able to move more quickly to address evolving technologies, even in some cases legislating before technologies are in mainstream use.[19] Tracing the extensive American history of privacy protections for a variety of novel technologies, scholars have concluded that "[c]ongress rather than the courts has shown the most serious interest in protecting privacy [in] new technologies."[20] Although the Canadian literature is sparse, similar assertions have been made with respect to Canadian legislatures.[21]

A second advantage of legislative over judicial regulation is the former's superior informational capacity and responsiveness to citizens' preferences.[22] Legislatures commonly hear from a diverse array of groups, ranging from independent commissions to special interest organizations.[23] Even if the

---

[16] *Ibid*. For an excellent example, see the Supreme Court of Canada's decision in *R. v. Fearon*, 2014 SCC 77, 2014 CarswellOnt 17202, 2014 CarswellOnt 17203, [2014] S.C.J. No. 77, [2014] 3 S.C.R. 621 [*Fearon*], dealing with the constitutionality of searching cell phones incident to arrest. In the American context, Professor Kerr provides a number of examples in his article *supra* note 3 at 869-870.

[17] For an excellent example, see *Fearon*, *supra* note 16 at paras 83-84.

[18] See Kerr, *supra* note 3 at 869-870; James Stribopoulos, "In Search of Dialogue: The Supreme Court, Police Powers, and the *Charter*" (2005) 31 Queen's LJ 1 at 48-50 citing Jerome Skolnick, *Justice Without Trial: Law Enforcement in Democratic Society* (New York: MacMillan, 1994) at 12.

[19] See *Riley v. California*, 134 S. Ct. 2473 (2014) [*Riley*] (opinion of Justice Alito) at 6 [*Riley*]; Kerr, *supra* note 3 at 870-871.

[20] See Kerr, *supra* note 3 at 857 and Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Mich L Rev 485 at 535-536.

[21] The leading example is found in Steven Penney's article "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 J Crim L & Crim 477 at 504-505.

[22] *Ibid* at 501. See also Kerr, *supra* note 3 at 875; *Breyer*, *supra* note 2 at 261-264; Penney, "The Digitization of Section 8," *supra* note 2 at 531; Marc Blitz, "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Trades Image and Identity" (2004) 82 Texs L Rev 1349 at 1421.

legislative process does not initially strike an appropriate balance of interests, democratic discourse will tend to result in legislatures abandoning rules which provide insufficient privacy or security protections.[24] As discussed above, the ability of courts to access such information is constrained by the scope of the judicial function within the adversarial system.

Other scholars argue, however, that courts are better suited to govern privacy interests in digital technologies.[25] They assert that courts are more independent and therefore less susceptible to special interest influence or majoritarian dislike of criminal suspects, who are disproportionately members of disadvantaged minorities.[26] Indeed, scholars in the United States and Canada have found that law enforcement agencies and corporations play an outsized role in shaping privacy policy given their "clear and constant voice in the political process."[27]

These scholars have also found that legislatures are often unable or unwilling to update "obviously flawed and outdated provisions."[28] Legislative responses to privacy issues are instead "largely reactive, targeting industries on a case by case basis, and often responding only after extreme instances of privacy infringement."[29] Other American studies show that the degree of protection

---

[23] See Penney, "Reasonable Expectations," *supra* note 21 at 501.

[24] See Kerr, *supra* note 3 at 881.

[25] See Blitz, *supra* note 22 at 1363; Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006) at 222-223; Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007) at 201; William Fenrich, "Common Law Protection of Individuals' Rights in Personal Information" (1996) 65 Fordham L Rev 951 at 958; Daniel Solove, *Nothing to Hide: The False Trade-off Between Privacy and Security* (New Haven: Yale University Press, 2011) at ch 17; Daniel Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" (2005) 74 Fordham L Rev 747 at 761; David Sklansky, "Two More Ways Not to Think about Privacy and the Fourth Amendment" (2015) 82 U Chicago L Rev 223 at 224.

[26] See Lessig, *supra* note 25 at 216-22; Sklansky, *supra* note 25 at 227; Murphy, *supra* note 20 at 535-536; Penney, "Reasonable Expectations," *supra* note 21 at 505-506. See also Kent Roach, *Due Process and Victims' Rights: The New Law and Politics of Criminal Justice* (Toronto: University of Toronto Press, 1999).

[27] See Murphy, *supra* note 20 at 533-535; Donald Dripps, "Constitutional Theory for Criminal Procedure: *Dickerson*, *Miranda*, and the Continuing Quest for Broad-but-Shallow" (2001) 43 Wm & Mary L Rev 1 at 46; Solove, "Fourth Amendment Codification," *supra* note 25 at 763-767; Solove, *Nothing to Hide*, *supra* note 25 at 165-167; Sklansky, *supra* note 25 at 227; Fenrich, *supra* note 25 at 958, 966. Professor Penney has warned of similar dangers in the Canadian context. See Penney "Reasonable Expectations," *supra* note 21 at 502-506. It is notable that Kerr, *supra* note 3 at 859 suggests that legislatures are not lobbied in the criminal law context. His reasons for this assertion are, however, contradicted by the extensive study of Murphy, *supra* note 20. Her conclusions are summarized at 535-536.

[28] *Ibid.*

[29] See Fenrich, *supra* note 25 at 966. See also Murphy, *supra* note 20 at 498, 500-501; Solove, "Fourth Amendment Codification," *supra* note 25 at 771.

provided by federal statutes is much more likely to turn on whether the information sought is useful to investigations than on widely shared notions of the degree of privacy expected in whichever property is searched.[30] For instance, access to one's driving, email, health, and personal credit records are disclosable upon administrative request, while video and cable records demand significantly heightened evidentiary requirements.[31]

Scholars have also observed that case-by-case adjudication allows litigants to force rule-making even in the absence of legislative action.[32] In support of this observation, scholars have identified many instances where legislatures have been found to be woefully inefficient in enacting privacy laws.[33] Even though judges often create broad and indeterminate rules, judicial rule-making at least guarantees the incremental, evolutionary development of policy in response to changing technological and social circumstances.[34]

Given the above review, it would be imprudent to downplay the role played by courts in governing digital privacy. Instead, it appears that both courts and legislatures have pivotal roles to play, as each institution brings different benefits to governing privacy in the digital age.[35] As such, it is prudent to think of ways to help judges operating within the adversarial system bear their burden more effectively. Before considering such options, however, it will prove useful to provide a more detailed example of the problems faced by courts when governing digital devices. A review of the judicial development of the law with respect to searches of cell phones incident to arrest will serve this purpose. Not only will this example bring the above issues into better focus, it will also provide a factual basis to test the recommendations discussed below in Part III.

II. CELL PHONE SEARCHES INCIDENT TO ARREST

As the capacity and use of modern cell phones increases, police have taken greater interest in searching cell phones as part of the common law power to search incident to arrest.[36] As the S.C.C. had previously prohibited,[37] or

---

30 See Murphy, *supra* note 20 at 506 citing Slobogin, *supra* note 25 at 184.

31 *Ibid*.

32 See Sklansky, *supra* note 25 at 227; Murphy, *supra* note 20 at 535.

33 *Ibid*. The *Privacy Act*, R.S.C. 1985, c. P-21 provides an excellent Canadian example, as it has not been substantially updated since 1983. See Jennifer Stoddart, "Letter to the Editor from Privacy Commissioner Jennifer Stoddart regarding proposed lawful access legislation," Letter to the Editor, *Office of the Privacy Commissioner of Canada* (12 November 2012).

34 See Sklansky, *supra* note 25 at 227; Murphy, *supra* note 20 at 535.

35 Murphy, *supra* note 20 at 490, 537-538 makes a similar point.

36 For the requirements of a valid search incident to arrest, see *R. v. Caslake*, 1998 CarswellMan 1, 1998 CarswellMan 2, [1998] 1 S.C.R. 51, [1998] S.C.J. No. 3, 121 C.C.C. (3d) 97 [*Caslake*].

37 See *R. v. Stillman*, 1997 CarswellNB 107, 1997 CarswellNB 108, [1997] 1 S.C.R. 607, 1997

modified,[38] the legal framework for conducting particularly invasive searches incident to arrest, a variety of courts have heard argument that cell phone searches ought to be prohibited as unjustifiable violations of s. 8 of the *Canadian Charter of Rights and Freedoms* (*Charter*), which protects the rights of all Canadians to be free from unreasonable searches and seizures.[39] In *R. v. Fearon*, the Court accepted the Crown's argument that conducting such searches was necessary for three reasons. First, public safety required searching phones to ensure suspects were not calling criminal backup.[40] Second, searching a cell phone will sometimes be necessary to preserve evidence due to the threat of remote deletion.[41] Third, searching phones may lead police to new evidence which would otherwise be lost.[42] Many technological arguments have been advanced to both undermine and support these points.

A. Passwords and Biometric Identification

Most cases concerning the scope of cell phone searches incident to arrest arose before the prevalence of smartphones.[43] As a cursory review of the jurisprudence reveals, many of the "dumb" phones[44] at issue were not password protected.[45] With the advancement of smartphone technology, however, users became more protective of the information in their phones. This likely explains why password protection has become ubiquitous among cell phone users.[46] Yet, as Daniel Scanlan posited long before the S.C.C.'s decision in *Fearon*: "[t]here is no mechanism at law to force an accused to disclose a password and, if any such measures were created, they would not likely survive constitutional scrutiny."[47]

S.C.J. No. 34, 144 D.L.R. (4th) 193 [*Stillman*] where the Court concluded that bodily samples could not be taken incident to arrest. See also *R. v. Godoy*, 1998 CarswellOnt 5223, 1998 CarswellOnt 5224, [1999] 1 S.C.R. 311, [1998] S.C.J. No. 85 [*Godoy*] where it was concluded that houses could not be searched incident to arrest.

38 See *R. v. Golden*, 2001 S.C.C. 83, 2001 CarswellOnt 4253, 2004 CarswellOnt 4301, [2001] 3 S.C.R. 679 [*Golden*] where the Court required a higher threshold for conducting strip searches incident to arrest.

39 Part I of the *Constitution Act, 1982* being schedule B to the *Canada Act 1982* (UK), 1982, c. 11.

40 See *Fearon*, *supra* note 16 at para 48.

41 *Ibid* at para 49.

42 *Ibid* at para 46.

43 See Peter Svensson, "Smartphones now Outsell 'Dumb' Phones," *Newshub* (28 April 2013), online: < www.newshub.co.nz/technology/smartphones-now-outsell-dumb-phones-2013042912 > .

44 "Dumb" phones are those which can only receive calls and text messages.

45 *R. v. Giles*, 2007 BCSC 1147, 2007 CarswellBC 3299, [2007] B.C.J. No. 2918, 77 W.C.B. (2d) 469 (B.C.S.C.) [*Giles*] is the only pre-*Fearon* decision involving a locked phone.

46 See Colton Fehr, "Cell Phone Searches Incident to Lawful Arrest: A Case Comment on the Ontario Court of Appeal's Decision in *R. v. Fearon*," case comment on *R. v. Fearon* (2014) 60 Crim LQ 343 at 356.

Subsequent to the *Fearon* decision, Jared Biden and I expanded on this view.[48] We asserted that the Court in *Fearon* failed to undertake a full constitutional analysis due to the lack of password protection and biometric identification evidence submitted in the case.[49] If an accused is required to provide a password, we argued that the accused's self-incrimination rights are unjustifiably violated.[50] Similarly, requiring an accused to speak into a phone arguably violates the right to silence.[51] Finally, conscripting fingerprints or retina scans constitutes a warrantless seizure which raises s. 8 constitutionality issues which were not considered by the Courts.[52] Although these considerations are arguably less intrusive compared to the warrantless search of a cell phone, conscripting passwords or biometric information adds to the severity of the overall intrusion.[53]

If there is merit to the argument that police cannot demand password or biometric evidence,[54] then the Crown's arguments in *Fearon* are significantly undermined. The desire to preserve evidence from remote deletion, to inquire as to whether criminal backup is being requested, or to discover evidence which is temporally vulnerable is only possible if the police have "prompt" access to the phone.[55] Yet, modern smartphones can thwart such access. Only in rare instances, such as through use of the pairing method,[56] can police enter a password-locked phone quickly. Otherwise, police will generally have to rely

---

47 See Daniel Scanlan, *Digital Evidence in Criminal Law* (Aurora: Canada Law Book, 2011) at 214 citing *R. v. Beauchamp*, 2008 CarswellOnt 2756, [2008] O.J. No. 1347, 58 C.R. (6th) 177, 171 C.R.R. (2d) 358 (Ont. S.C.J.) at paras 18, 66.

48 See Colton Fehr & Jared Biden, "Divorced from (Technological) Reality: A Response to the Supreme Court of Canada's Reasons in *R v Fearon*" (2015) 20 Can Crim L Rev 93. For an interesting discussion (and similar conclusion) in the border context, see Robert J. Currie, "Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?" (2016) 14 CJLT 289 at 314-317.

49 See Fehr & Biden, *supra* note 48 at 95. The phone in *Fearon* was not password protected and did not require biometric identification to enter the phone.

50 *Ibid* at 103.

51 *Ibid.*

52 *Ibid* at 104-105.

53 *Ibid.*

54 For an opposing view see Steven Penney, "'Mere Evidence'? Why Customs Searches of Digital Devices Violate Section 8 of the *Charter*" (2016) 49:2 UBC L Rev 485 at 517 (see note 152 and the sources cited therein).

55 See *Fearon*, *supra* note 16 at paras 49, 59, 66.

56 As we observe *supra* note 48 at 101-102, "if police have access to a computer which the iPhone has previously been connected to, they will be able to bypass the security function . . . Even if the police have access to an iPhone, [however] the user may prevent searches of this sort as 'users [can] encrypt their hard drives to protect their pairing record.'" We cite in support of this view technology expert Andy Greenberg's article "Despite Apple's Privacy Pledge, Cops Can Still Pull Data Off a Locked IPhone," *Wired* (18 September 2014), online: <www.wired.com/2014/09/apple-iphone-security/>.

upon the "brute force" method, which involves a machine rapidly inputting passwords until it finds the correct code.[57] Yet, even with basic four-digit passwords, this process can take many hours.[58] Moreover, a program can be installed to shut down the phone after a certain amount of attempts.[59] This is precisely the type of technology which significantly restrained the FBI's ability to enter into the San Bernardino shooter's smartphone.[60] These and similar security technologies are also currently preventing Canadian police from searching cell phones in numerous criminal investigations.[61]

Despite the above-mentioned barriers to entering cell phones "promptly," the state of the technology has hardly been considered in the jurisprudence.[62] Although the Crown *may* be able to justify any breach arising from demanding a password or biometric identifier, it is the fact that these obvious issues were not considered by courts that illustrates the general problem with courts deciding cases that involve digital evidence issues.[63] At best, the constitutionality of searching locked cell phones incident to arrest — the majority of cell phones today[64] — remains ambiguous post-*Fearon*. At worst, the Court's decision in *Fearon* became inapplicable to most cell phone searches incident to arrest the moment it was rendered.

---

[57] See Fehr & Biden, *supra* note 48 at 102.

[58] *Ibid* citing Adam Rouse, "Apple and Google Make the Next Generation of Smartphones More Secure," (17 November 2014), online: < blogs.kentlaw.iit.edu/islat/2014/11/17/apple-and-google-make-the-next-generation-of-smartphones-more-secure/ > .

[59] *Ibid*.

[60] See, "FBI Breaks into iphone of San Bernardino Shooter without Apple's Help," *CBC News* (28 March 2016), online: < www.cbc.ca/news/technology/fbi-san-bernardino-iphone-break-1.3509899 > . The 2015 San Bernardino shooting was a terrorist attack in San Bernardino, California. The FBI seized the accused's cell phone but, upon attempting to search it, were obstructed by a variety of security features on the cell phone.

[61] See Daniel Seglins, Robert Cribb & Chelsea Gomez, "RCMP Want New Powers to Bypass Digital Roadblocks in Terrorism, Major Crimes Cases," *CBC News* (15 November 2016), online: < www.cbc.ca/news/investigates/rcmp-digital-roadblocks-1.3850018 > .

[62] The Ontario Court of Appeal's decision in *R. v. Fearon*, 2013 ONCA 106, 2013 CarswellOnt 1703, [2013] O.J. No. 704, 114 O.R. (3d) 81, 296 C.C.C. (3d) 331 (Ont. C.A.), affd 2017 SCC 77, [2014] 3 S.C.R. 621 at para 75 [*Fearon ONCA*] arguably makes this suggestion when it concluded that a warrant was required for locked phones, but not unlocked phones. It is unclear if the Court was considering whether the accused's expectation of privacy was higher as a result, or if the Court realized the difficulties officers would have in entering a phone.

[63] I feel comfortable making this claim as the basic arguments (detailed more thoroughly in the article *supra* note 48) were published in a peer-reviewed journal.

[64] See Svensson, *supra* note 43.

B. Battery Removal

With respect to the rationale regarding the preservation of evidence, numerous courts,[65] as well as academic commentators,[66] have asserted that any deletion of cell phone data could be prevented if an officer removes a battery from a cell phone. As I explain elsewhere, cell phone content cannot be deleted when a phone is turned off.[67] As long as the officer reboots the phone within an area that is isolated from the phone's cellular network, any remote-control deletion attempts will be thwarted.[68] As such, it is arguable that any concern about remote destruction of evidence on a phone — which was forcefully argued by the Crown in *Fearon* — is without merit.

The issue that judges and commentators have failed to address concerns the way in which computers store data. Computers store a significant amount of data permanently on a hard drive.[69] However, not all data is stored on the hard drive. Random Access Memory (R.A.M.) stores frequently used program information in a temporary manner.[70] The benefit of using R.A.M. is that it significantly increases the speed of a device.[71] Removing the battery from a computer or phone, however, risks losing memory stored on the R.A.M.[72] As such, removing the battery does not provide a perfect solution as it risks losing potentially incriminating evidence. Although computer developers have, subsequent to *Fearon*, made significant progress with respect to making R.A.M. less volatile,[73] the technology was much less capable when lower courts began deciding whether cell phone searches incident to arrest were constitutional.[74]

---

65 See the dissenting reasons in *Fearon*, *supra* note 16 at para 144; *R. v. Liew*, 2012 ONSC 1826, 2012 CarswellOnt 3686, [2012] O.J. No. 1365, 100 W.C.B. (2d) 256 (Ont. S.C.J.) at para 144; *R. v. Hiscoe*, 2011 NSPC 84, 2011 CarswellNS 852, 310 N.S.R. (2d) 142, [2011] N.S.J. No. 615 (N.S. Prov. Ct.), affd 2013 NSCA 48, 297 C.C.C. (3d) 35, 1 C.R. (7th) 350 (C.A.) at para. 15 [*Hiscoe* N.S.P.C.]; *R. v. Cater*, 2012 NSPC 2, 2012 CarswellNS 37, 312 N.S.R. (2d) 242, [2012] N.S.J. No. 22 (N.S. Prov. Ct.) at para 32 [*Cater*].

66 See Fehr, *supra* note 46 at 352-353.

67 *Ibid.*

68 *Ibid.*

69 See Scanlan, *Digital Evidence*, *supra* note 47 at 159-167.

70 *Ibid.*

71 *Ibid.*

72 *Ibid* at 160. See also Tim Schiesser, "Guide to Smartphone Hardware: Memory and Storage," *Neowin* (12 March 2012), online: <www.neowin.net/news/guide-to-smart-phone-hardware-37-memory-and-storage>.

73 See Sean Gallagher, "Memory that Never Forgets: Non-Volatile DIMMs Hit the Market," *Arstechnica* (4 April 2013), online: <arstechnica.com/information-technology/2013/04/memory-that-never-forgets-non-volatile-dimms-hit-the-market/>.

74 *Ibid.* The issue was first decided in *Giles*, *supra* note 45 in 2007.

C. Faraday Bags

A number of courts and scholars have also suggested that placing a phone in a Faraday bag would prevent any risk of remote control deletion.[75] Faraday bags are designed to prevent a phone from receiving any signals when powered on, and are relatively inexpensive.[76] As such, it was argued that a police officer could simply place a phone into one of these bags to prevent remote control deletion.[77] However, as Daniel Scanlan observes, "these bags are not always completely effective at blocking transmissions."[78] Moreover, Faraday bags do not prevent "logic bombs" from operating.[79] A logic bomb is designed to overwrite information if a triggering event (such as entering a particular code) does not occur within a period of time.[80] Again, in the context of the adversarial trial, many courts were not presented with evidence of the existence of Faraday bags, let alone evidence explaining its frailties. Regardless of the lack of evidence, even the narrow minority in *Fearon* accepted without question the feasibility of battery removal and Faraday bags preventing destruction of evidence.[81]

D. Smartphones vs "Dumb" Phones

In *Fearon*, the majority concluded that courts "should not differentiate among different cellular devices based on their particular capacities when setting the general framework for the search power."[82] In failing to draw a distinction between the device and its data, courts have been criticized for missing an opportunity to distinguish smartphones from less sophisticated "burner" or "dumb" phones.[83] The latter generally have fewer features, significantly lesser capacity, and are much more difficult to trace as they are not connected to G.P.S. technology.[84] As one author observes, the two types of phones are "too distinct to bear any categorical similarities besides the capacity for emailing, photographing, and making and receiving calls."[85] Yet, the Court's governing framework failed to give appropriate weight to these basic technological

---

[75] Most notably see the dissenting reasons in *Fearon*, *supra* note 16 at para 144. See also Fehr, *supra* note 46 at 352-353.

[76] *Ibid.*

[77] See for instance *Fearon*, *supra* note 16 at para 144. Post-*Fearon*, this argument still has some traction. See *R. v. Jones*, 2015 SKPC 29, 2015 CarswellSask 106, 468 Sask. R. 264, [2015] S.J. No. 89, 119 W.C.B. (2d) 563 (Sask. Prov. Ct.) at para 69 [*Jones*].

[78] See Scanlan, *Digital Evidence*, *supra* note 47 at 160.

[79] See Eamon Doherty, "The Need for a Faraday Bag," *ForensicMag* (21 February 2014), online: < www.forensicmag.com/article/2014/02/need-faraday-bag > .

[80] *Ibid.*

[81] See *Fearon*, *supra* note 16 at para 144.

[82] *Ibid* at para 52.

[83] See Fine, *supra* note 2 at 179.

[84] *Ibid.*

[85] *Ibid.*

differences. As a result, the Court's framework has been criticized for risking serious privacy intrusions, as smartphones provide a vast portal into intimate personal details, while dumb phones do not.[86] This is not to say that distinguishing between smart and dumb phones is simple. However, ignoring the significant differences between the privacy interests in each type of phone is hardly more palatable.

Of equal concern is the assumption that officers searching a smartphone will be able to conduct the nuanced types of searches allowed by the Court. The Court permitted searching "only recently sent or drafted emails, texts, photos and the call log."[87] As such, the intrusiveness of a cell phone search appears to be low. Yet, as Jordan Fine observes, conducting such searches on modern smartphones is much more complex:

> Unless law enforcement has been given precise testimony as to where in a device discoverable evidence can be found, *an indefinite search through data will have to be made*. Even if police received a tip that photographic evidence existed on a phone, its location would be a mystery. Would it be in Instagram, a photo sharing application, or is it hidden on the SD card? If the evidence is a text message, is it in a common messaging platform like WhatsApp, or encrypted inside TextSecure?[88]

In rejecting a pre-*Fearon* rule developed in *R. v. Polius*,[89] which permitted police to conduct a "cursory" search of a cell phone incident to arrest, Professor Steven Penney made a similar observation:

> 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.[90]

Given the fundamental differences between searches of smartphones and dumb phones, it is unlikely that these courts had the evidence necessary to fully appreciate the way each type of phone would be searched. As the courts were likely conscious of this evidentiary lacuna, it was only reasonable for the majority in *Fearon* to have developed a vague rule, as it gave future courts flexibility in deciding cases with more robust factual records.[91]

---

86 See *Fearon*, *supra* note 16 at para 131.

87 *Ibid* at para 76.

88 See Fine, *supra* note 2 at 180-181 [emphasis added].

89 2009 CarswellOnt 4213, [2009] O.J. No. 3074, 196 C.R.R. (2d) 288, 84 W.C.B. (2d) 343 (Ont. S.C.J.) [*Polius*].

90 See Steven Penney, "Searches of Digital Devices Incident to Arrest: R v Fearon" (2014) 23 Const Forum Const 1 at 3.

91 For an excellent explanation of the inherent indeterminacy of the rule in *Fearon*, see Tim Quigley, "*R. v. Fearon*: A Problematic Decision" (2015) 15 C.R. (7th) 281.

E. Cell Phone Capacities

A number of lower court decisions failed to focus on the technological facts addressed above. Instead, these decisions focused primarily on the degree of privacy that an accused had in his or her cell phone.[92] In so doing, judges frequently employed questionable metaphors in deciding that cell phone searches were permissible incident to arrest. By comparing digital storage devices to filing cabinets, briefcases, and cupboards, appellate courts, as well as a multitude of trial courts, relied on precedents that permitted such physical searches in upholding the lawfulness of cell phone searches incident to arrest.[93]

By relying upon such metaphors, however, the courts overlooked both qualitative and quantitative differences with respect to modern smartphones.[94] These phones contain substantially more information (much of which is private), store records of every action taken on the device, retain information even after users believe the evidence is destroyed, and permit access to information not "in" the cell phone itself.[95] Given the lack of consideration of these differences, a surprising number of lower courts significantly downplayed the privacy interests that an individual has in his or her modern cell phone.[96]

One plausible explanation for the reliance by courts on illogical analogies lies in the adversarial system's tendency to focus on the narrow facts of a case. In the cases dealing with dumb phones, the capacity of the phone at issue was significantly less than any smartphone. An analogy to a briefcase or an address book makes much more sense in this context. At least one court explicitly stated that it was relying exclusively on the technological capabilities of the dumb phone at issue when relying on such a metaphor.[97] However, this also reveals a different problem: the failure of the adversarial system to consider a complete picture of available and foreseeable technology. When making rules within this

---

92 *Hiscoe NSPC*, *supra* note 65 and *Cater*, *supra* note 65 are good examples.

93 Although in a different digital case, see *Vu*, *supra* note 12 at para 43, revg 2011 BCCA 536, 2011 CarswellBC 3551, 285 C.C.C. (3d) 160, for use of such a metaphor. See also *R. v. Beauchamp*, 2008 CarswellOnt 2756, [2008] O.J. No. 1347, 58 C.R. (6th) 177, 171 C.R.R. (2d) 358 (Ont. S.C.J.) at para 40; *R. v. Fearon*, 2010 ONCJ 645, 2010 CarswellOnt 10077, [2010] O.J. No. 5745, 92 W.C.B. (2d) 116 (Ont. S.C.J.), affd 2013 ONCA 106, 2013 CarswellOnt 1703, 296 C.C.C. (3d) 331 (C.A.) at para 51 [*Fearon* O.N.C.J.]; *Giles*, *supra* note 45 at paras 56, 63; *Polius*, *supra* note 89 at para 45; *Cater*, *supra* note 65 at para 54 (though the judge restricted his comments to "dumb" phones). Some courts found otherwise. See *Hiscoe* N.S.P.C., *supra* note 65 at paras 40-43, affd 2013 NSCA 48, 2013 CarswellNS 242 at para 75 [*Hiscoe* N.S.C.A.]. See also Kerr, *supra* note 3 at 875 for some American examples.

94 See *Fearon*, *supra* note 16 at paras 125-134. See also *Vu*, *supra* note 12 at para 47.

95 See *Vu*, *supra* note 12 at paras 41-44. When a file on a personal computer is uploaded to the cloud, it may be synchronized with one's cell phone. See Brian Chen, *Always On: How the iPhone Unlocked the Anything-Anytime-Anywhere Future—and Locked Us In* (Boston: Da Capo Press, 2012) at 130-143.

96 See *supra*, note 93.

97 See *Cater*, *supra* note 65 at para 54.

environment, it is unlikely that the common law will keep pace with the privacy interests implicated by searches of modern digital devices.

III. MODIFYING THE ADVERSARIAL FRAMEWORK

Given the evidentiary shortcomings that tend to arise when courts decide issues relating to complex digital technologies, it is necessary to consider options that better equip courts to decide future cases. In my view, legislatures should aid courts in deciding these types of cases in two primary ways. First, legislatures should utilize the reference procedure when requiring courts to make or decide on the constitutionality of a rule concerning a complex digital technology. Second, legislatures should make accessible to counsel up-to-date and independent expert reports describing technologies that are expected to come before courts. The merits of each recommendation are explained in turn.

A. Reference Procedure

The federal government may refer to the S.C.C. virtually any question of law pursuant to s. 53 of the *Supreme Court Act*.[98] The provinces are to be notified of any question in which they have a "special interest," and are entitled to make submissions before the S.C.C.[99] The Court also has jurisdiction to notify any "interested parties" of the proceedings and allow those parties to make submissions.[100] The Court may even direct that specific counsel argue the case brought before the Court.[101] Finally, the Court may bring forward any "papers or other proceedings had or taken before any court, judge or justice of the peace, and that are considered necessary with a view to any inquiry, appeal or other proceeding had or to be had before the Court."[102]

Utilizing the reference procedure in cases where courts are tasked with making or deciding on the constitutionality of a rule with respect to complex digital technologies has several benefits. First, the reference procedure avoids the adversarial system's tendency to hear insufficient evidence from limited parties.[103] In the context of a reference, the Court may hear from any party or take evidence from any proceedings. The Court may even call on parties to argue a particular legal issue. This procedure therefore allows the Court to build the best possible evidentiary record for deciding a question of law. Though courts deciding whether a search of a cell phone incident to arrest was constitutional would sometimes hear from an expert, the vast majority of courts did not have

---

98 R.S.C. 1985, c S-26, s. 53(1)-(3) [*Supreme Court Act*].

99 *Ibid*, s. 53(5).

100 *Ibid*, s. 53(6).

101 *Ibid*, s. 53(7).

102 *Ibid*, s. 55.

103 See Centre for Constitutional Studies, "The Reference Procedure: The Government's Ability to Ask the Court's Opinion," online: < ualawccsprod.srv.ualberta.ca/ > .

the benefit of expert testimony.[104] One might speculate that the costs of hiring an expert were at least partially responsible for the lack of expert evidence submitted in these cases. Given the academic criticism of the Court's decision in *Fearon*, it appears that intervener submissions also failed to adequately update the evidentiary record. Use of the reference procedure, however, would have allowed the Court to address this informational deficit by calling its own experts.

Second, a reference can ensure that courts deciding issues pertaining to novel search technologies do not render decisions of "historical interest only."[105] Bypassing first instance trials and provincial appeals helps ensure that rules concerning novel search technologies are made within a reasonable amount of time. This benefit is again exemplified by observing the judicial development of the law of cell phone searches incident to arrest. The first judicial decision to address this issue arose in 2005.[106] Although the technology of cell phones improved dramatically between 2005 and 2014, when the S.C.C. rendered its reasons in *Fearon*, it was certainly possible to foresee by the mid-2000s that cell phones would come to have basic features, such as password and biometric protection, which would make prompt access difficult without help from the user. As such, a reference to the S.C.C. in the mid-2000s could have resulted in an informed legal opinion that fully canvassed cell phone technology and would have remained relatively current even today.

Finally, the reference procedure ensures that privacy issues are considered by a neutral arbiter. As discussed earlier, several scholars have observed that courts are better suited than legislatures to govern privacy with respect to disadvantaged minorities such as criminal accused.[107] However, scholars have also contended that this concern is counterbalanced by the fact that courts are institutionally less capable of developing an informed evidentiary record.[108] By utilizing the reference procedure, however, these concerns are assuaged. Not only does the court ensure that the issue is considered by a neutral third party, it is also provided with significantly more information than typically provided by the adversarial system.

Despite the above benefits, it may be retorted that utilizing the reference procedure to develop rules with respect to digital technologies is problematic. The fact that the S.C.C.'s answer to a reference question is not binding on lower courts arguably means that the reference process will not affect how lower courts approach digital evidence cases, as they may simply ignore reference opinions and decide the issue based on the factual record before them.[109] However, this

---

[104] *Infra* note 116.

[105] See Scanlan, *supra* note 2 at 312; Kerr, *supra* note 3 at 868-869.

[106] See *Giles*, *supra* note 45.

[107] See Lessig, *supra* note 25 at 216-222; Sklansky, *supra* note 25 at 227; Murphy, *supra* note 20 at 535-536; Roach, *supra* note 26.

[108] See Penney, "Reasonable Expectations," *supra* note 21 at 501; Kerr, *supra* note 3 at 875; *Breyer*, *supra* note 2 at 261-264; Penney, "The Digitization of Section 8," *supra* note 2 at 531; Blitz, *supra* note 22 at 1421.

criticism ignores the S.C.C.'s conclusion that reference opinions are "of highly persuasive weight."[110] In fact, no lower court has ever exercised its discretion to ignore a reference opinion.[111] As such, it is reasonable to conclude that such opinions would be followed by lower courts unless the technology at issue changed in a legally relevant way.

It may also be argued that use of the reference procedure unduly sacrifices the benefit of having multiple courts opine upon the legality of searching a digital device. This criticism, however, is of limited merit. First, as discussed in Parts I and II, courts tend to make their decisions with respect to the legality of searching a digital device in an inadequately informed evidentiary environment. Any rules developed in this context are therefore of limited utility. Second, the reference procedure permits the court to draw upon a variety of perspectives. Not only will the Crown raise arguments, but interveners may also apply to, or be solicited by, the court to make submissions, and experts may be called to provide relevant testimony. Therefore, the benefits of having multiple lower court opinions are significantly offset. Third, requiring that resources be concentrated in one hearing is more efficient than bringing arguments (some of which are bound to overlap) before multiple courts. As such, the benefits of utilizing the reference procedure when courts must make or decide on the constitutionality of a rule with respect to complex technologies likely outweigh any costs.

Finally, it may be argued that there are political obstacles that make this proposal unlikely to work in practice. In other words, it may be difficult to convince legislatures to send such issues to the courts via the reference procedure. True as this may be, the reference procedure still provides a neutral process wherein the government can defend its preferred method for governing a digital technology. As such, a responsible legislature should view the reference process as more pragmatic than expending significant resources on multiple trials wherein a rule will be subject to constitutional challenge and/or developed with inadequate evidence.

B. External Aid

As cases are appealed, intervener briefs are sometimes cited by high courts to help correct factual assumptions.[112] Yet, as seen in Part II, intervener briefs were

---

[109] See *Reference re Remuneration of Judges of the Provincial Court (P.E.I.)*, 1998 CarswellNat 114, 1998 CarswellNat 79, [1998] 1 S.C.R. 3, 155 D.L.R. (4th) 1 (*sub nom R. v. Campbell*) (S.C.C.) at para 10 [*Remuneration*].

[110] *Ibid.*

[111] See Peter Hogg, *Constitutional Law of Canada* (Toronto: Thomson Reuters Canada, 2009) at 8.6(d). Although it is notable that courts have utilized different constitutional principles, or significantly changed facts, to avoid following a prior Supreme Court of Canada precedent. See generally *Canada (Attorney General) v. Bedford*, 2013 SCC 72, 2013 CarswellOnt 17681, 2013 CarswellOnt 17682, [2013] 3 S.C.R. 1101 [2013] S.C.J. No. 72 [*Bedford*].

[112] This phenomenon has been well documented. See Kerr, *supra* note 3 at 877-79 citing *Bach*

incapable of filling the informational lacuna during the development of the law regarding searching cell phones incident to arrest. As Professor Murphy explains, this is likely because institutions that defend privacy, such as civil liberties associations, are not able to expend necessary resources due to limited funding which is divided between numerous civil rights issues.[113] As such, there should be a more reliable means for courts and counsel to become informed of relevant digital evidence. This is necessary, as the vast majority of digital cases will not involve making or deciding on the constitutionality of a rule, rendering the reference process of limited utility. Instead, courts will need assistance applying established rules to often complex digital facts.

One way of addressing this issue is to provide counsel with independent, up-to-date, and readily available information about digital technologies expected to come before the courts. This proposal is obviously vague, and raises at least two general questions. First, what types of questions would the courts need answered? Second, who would counsel turn to for independent advice?

The jurisprudence concerning whether searching cell phones incident to arrest is constitutional is illustrative of the types of questions courts need answered. Determining how such a search takes place, when the search may be thwarted, and the nature of the privacy interests implicated by the search were all integral to deciding the constitutional issues related to cell phone searches. As technologies are generally in development long before they are released, these questions could have been answered at an early stage. For instance, as the first smartphone was developed in 1992,[114] it is reasonable to conclude that those in the industry could have predicted the mass adoption of smartphones by the time the courts first decided the issue in 2007.[115] Likewise, password and biometric security features have long been available to computer users. Given the increased privacy interests implicated by modern cell phones, it was reasonable to assume by the mid-2000s that the technology would continue developing in a manner that would make it increasingly difficult for police to promptly enter cell phones or prevent the destruction of evidence.

Although experts can be called at trial to serve a similar function, the adversarial system provides no guarantee that the Crown or defence will call such evidence. Indeed, of the eight main cases ruling on the constitutionality of cell

---

v. United States, No Crim 01-221, 2001 1690055 (Minnesota, 2001) revd 310 F3d 1063 (8th Circuit 2002) [*Bach*] among other cases. For a good Canadian example, see *Vu*, *supra* note 12 at paras 43-44 where the Court relied upon an academic article as well as submissions by the Canadian Civil Liberties Association in rejecting the various ill-suited metaphors discussed above.

[113] See Murphy, *supra* note 20 at 505-506.

[114] The first smartphone was developed 15 years before the first iPhone was released. See Steven Tweedie, "The World's First Smartphone, Simon, was Created 15 Years before the IPhone" *Tech Insider* (14 June 2015), online: < www.businessinsider.com/worlds-first-smartphone-simon-launched-before-iphone-2015-6 > .

[115] See *Giles*, *supra* note 45, which was the first case to decide the issue.

phone searches incident to arrest, the trial judge relied on expert testimony in only one of them.[116] This is especially problematic as courts operating within the Canadian adversarial model are not permitted to call their own experts, as is possible in some civil[117] and common law[118] jurisdictions. Even if Canadian courts could call their own experts, this sort of aid may not be desirable from an economic standpoint. Frequent resort to experts would be expensive. Given the increased frequency with which judicial decisions can be expected to implicate complex digital evidence, it is desirable to consider less costly ways for courts to avail themselves of necessary information.

To this end, it may be prudent for Parliament to task an independent institution with providing detailed and up-to-date overviews of technologies which are expected to come before the courts. Counsel could then choose whether to rely on this evidence during a trial. An institution that would be suitable for providing such advice would be the Office of the Privacy Commissioner of Canada (O.P.C.), or other similar provincial bodies.[119] The O.P.C. operates independently from government,[120] and its purpose is to "protect and promote the privacy rights of individuals."[121] Although its mandate is currently restricted to overseeing compliance with Canada's main privacy acts,[122] their office could be tasked with providing detailed overviews of technologies which are expected to arise in the jurisprudence.[123] Indeed, the O.P.C. would be well-suited to such a role, given its expertise in issues relating to

---

[116] In *Cater*, *supra* note 65 the court relied on expert evidence. The courts in *Fearon ONCJ*, *supra* note 93; *Hiscoe NSPC*, *supra* note 65; *Liew*, *supra* note 65; *Polius*, *supra* note 89; *R. v. Manley*, 2011 ONCA 128, 2011 CarswellOnt 803, [2011] O.J. No. 642, 269 C.C.C. (3d) 40 (Ont. C.A.) [*Manley*]; *R. v. Finnikin*, 2009 CarswellOnt 8955, [2009] O.J. No. 6016, 87 W.C.B. (2d) 902 (Ont. S.C.J.); *R. v. Otchere-Badu*, 2010 ONSC 1059, 2010 CarswellOnt 1295, 87 W.C.B. (2d) 29 (Ont. S.C.J.) [*Otchere-Badu*] did not rely on expert evidence.

[117] For instance, see *German Code of Civil Procedure* (5 December 2005), s. 404.

[118] For instance, see U.S. Fed. R. Civ. P. 53. The appointment of law and technology expert Lawrence Lessig as a "special master" (who serves effectively as an expert witness) proved useful in the landmark digital case of *United States v. Microsoft Corporation*, 253 F 3d 34 (2001).

[119] In Alberta, for instance, see "Office of the Information and Privacy Commissioner of Alberta," online: < www.oipc.ab.ca/ > . I do not mean to suggest that the various offices of privacy commissioners would be the only suitable institution. The now disbanded Law Reform Commission of Canada would also have been a suitable candidate. As it is no longer in existence, however, I will not entertain this potential avenue for addressing the problems raised by digital evidence and the adversarial system.

[120] Office of the Privacy Commissioner of Canada (OPC), "Who we are," online: < www.priv.gc.ca/en/about-the-opc/who-we-are/ > .

[121] *Ibid.*

[122] *Ibid.* The OPC particularly oversees the *Privacy Act*, R.S.C. 1985, c. P-21 [*Privacy Act*] and *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*].

[123] For an example of what such a report would look like, see Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You" (May 2013),

privacy which, in today's day and age, it is reasonable to assume includes an in-depth knowledge of complex digital technologies.

Two main criticisms of this proposal merit comment. First, as the O.P.C. has a mandate of *protecting* privacy, it may be perceived as biased against legitimate security interests. Either explicitly or implicitly, those researching the relevant digital technologies may conduct research that they believe tends to bolster privacy-based arguments. This problem could, however, be offset in two ways. First, Parliament could explicitly require that the O.P.C. conduct this research in a neutral manner. Second, even if the research tended to support privacy interests, the Crown could still call its own experts in reply. As the Crown has relatively significant resources to expend, it does not seem overly burdensome to require it to call rebuttal evidence if it has reason to believe that the work of the O.P.C. is inadequate.

Second, it may be asked whether such a proposal would serve the main purpose of s. 8 of the *Charter*: namely *preventing* unreasonable searches and seizures.[124] Many digital law issues come before courts *ex parte* as warrant applications. As defence counsel is not present on such applications, courts would suffer from the same informational deficit as currently exists. True as this may be, the proposal here at least better ensures that *ex post* review will be conducted with an adequate factual basis. Moreover, if a judge was aware of an independent report that raised concerns with a warrant application, I see no reason why the judge could not dismiss or modify a Crown's application on that basis. In this way, my proposal at least has the potential to prevent some unreasonable searches, even if its main function will be to ensure laws are properly applied *ex post*.

CONCLUSION

Judges operating within the adversarial system are generally unable to build an adequate factual record due to the unusually complex and rapidly changing nature of digital evidence. As such, some commentators have suggested that courts defer to legislatures to create rules governing digital technologies. However, other scholars have demonstrated that the "leave it to the legislature" argument is no panacea. Although legislatures are, in theory, able to respond in an informed and diligent manner, they often fail to do so, thereby leaving it to the courts to create new rules or apply ambiguous legislative rules to complex digital facts. Scholars have also observed that legislatures often downplay the privacy interests of individuals, especially those of disadvantaged minorities such as criminal accused. Given the increasing relevance of digital

---

online: <www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/>.

[124] See *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, 1984 CarswellAlta 121, 1984 CarswellAlta 415, [1984] S.C.J. No. 36, 11 D.L.R. (4th) 641 at 160.

technologies to privacy, it may be preferable to have neutral parties decide digital evidence issues, especially in the criminal law context.

To ensure courts are institutionally equipped to play this role, it is necessary to develop means for courts to receive adequate evidence with respect to digital technologies. I have offered two recommendations to address this issue. First, in controversial cases where a court must make or decide on the constitutionality of a rule, I maintain that best practice would involve sending the issue as a reference question to the S.C.C. Not only does this permit courts to develop a rule expeditiously, thereby avoiding any eventual judicial decision being of "historical interest only," it also allows the S.C.C. to solicit a fully informed evidentiary record upon which to develop the law. Second, when a court must apply an existing rule to a complex digital issue, I suggest that the O.P.C. or a similar government institution should aid counsel in understanding digital technologies by providing detailed and impartial overviews of digital technologies expected to come before the courts. By relying on such reports, counsel can ensure judges are better equipped to decide digital legal issues.

Devising better ways to govern privacy in the digital age is among the most pressing challenges facing the modern nation state. As Justice Karakatsanis recognized in *Fearon*, "[when] technology changes, our law must also evolve so that modern mobile devices do not become the telescreens of George Orwell's *1984*."[125] In other words, effective governance of privacy is necessary to preserve fundamental rights and freedoms. At the same time, effective surveillance is necessary to ensure state security. Regardless of one's opinion on how this balance is best struck, it is necessary that the institutions governing privacy be working to their strengths, not their weaknesses.

---

[125] See *Fearon*, *supra* note 16 at para 102.