The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference

Volume 71 Article 17

2015

A Step Forward or Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age

Nader R. Hasan

Citation Information

Hasan, Nader R.. "A Step Forward or Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age." *The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference* 71. (2015).
DOI: https://doi.org/10.60082/2563-8505.1319
https://digitalcommons.osgoode.yorku.ca/sclr/vol71/iss1/17

A Step Forward or Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age

Nader R. Hasan[*]

I. INTRODUCTION

It is a cliché to write that computers and cell phones are ubiquitous.[1] These devices and the digital technologies that make them work have been a part of our lives for so long now that taking note of this fact seems as quaint as extolling the wonders of airplanes or pasteurization. These technologies are not new.

The laws responding to digital technologies, however, are new — particularly as they relate to our privacy rights and the protections afforded under section 8 of the *Canadian Charter of Rights and Freedoms*.[2] Over the past five years, the Supreme Court of Canada has issued a series of decisions meant to bring section 8 of the Charter into the Digital Age. These decisions acknowledged the unique privacy interests that people have in the information stored on their digital devices. In *R. v. Morelli*, the Court held that "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the

---

[*] Counsel, STOCKWOODS LLP (NaderH@stockwoods.ca). The author is grateful to Frederick Schumann, Annamaria Enanajor, Penelope Ng and the anonymous reviewers for their comments on an earlier draft of this article. The author also thanks Gerald Chan, who was co-counsel with him in their representation of the British Columbia Civil Liberties Association in *R. v. Vu* and *R. v. Fearon*, two of the cases discussed at length in this article.

[1] In this article, I refer to "computers", "cell phones" and "digital devices", but the distinction between these items is increasingly meaningless. See *R. v. Fearon*, [2014] S.C.J. No. 77, [2014] 3 S.C.R. 621, at para. 51 (S.C.C.) [hereinafter "*Fearon*"]; see also *R. v. Vu*, [2013] S.C.J. No. 60, [2013] 3 S.C.R. 657, at para. 38 (S.C.C.) [hereinafter "*Vu* (S.C.C.)"] ("Although historically cellular telephones 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.").

[2] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [hereinafter "Charter"], s. 8.

search and seizure of a personal computer."[3] In *R. v. Cole*, it held that because of the "highly revealing" and "meaningful information" about an individual's personal life that is stored on a computer, we enjoy a reasonable expectation of privacy even on work-issued computers that do not belong to us.[4] In *R. v. TELUS Communications Co.*, a plurality of the Court declared that "[t]echnical differences inherent in new technology should not determine the scope of protection afforded to private communications", and held that the *Criminal Code*'s wiretap authorization provisions apply to the prospective interception of text messages.[5] In *Vu*, the Court held that a search warrant may only be relied on to search the contents of a computer where the warrant specifically authorizes a computer search; a warrant that only authorizes the search of a residence in which a computer happens to be found is inadequate.[6] In *R. v. Spencer*, the Court held that section 8 protects a right to online anonymity.[7] And most recently, in *Fearon*, the Court established a framework for regulating warrantless searches of cell phones under the search-incident-to-arrest exception.[8]

In each of these decisions, the Court acknowledged that digital technologies have fundamentally changed the game, and that the prophylactic rules that protect our privacy rights from the State must evolve to keep pace. Through these judgments, the Court demonstrated an awareness of how these technologies work. It has also taken note of their potential to eviscerate privacy if law enforcement is simply permitted to apply the old Analog World rules in a Digital Age.

While the Court has recognized the unprecedented challenge to privacy posed by the search and seizure of digital devices, it has stopped short of creating bright-line rules to protect our privacy rights. In *Vu*, despite the urging of civil liberties groups, the Court declined to impose a constitutional requirement that computer search warrants include "search protocols" to limit the invasiveness of a computer search. This leaves

---

[3] *R. v. Morelli*, [2010] S.C.J. No. 8, [2010] 1 S.C.R. 253, at para. 2 (S.C.C.) [hereinafter "*Morelli*"].

[4] *R. v. Cole*, [2012] S.C.J. No. 53, [2012] 3 S.C.R. 34, at paras. 39-58 (S.C.C.) [hereinafter "*Cole*"].

[5] *R. v. TELUS Communications Co*., [2013] S.C.J. No. 16, [2013] 2 S.C.R. 3, at paras. 5, 43-45 (S.C.C.) [hereinafter "*TELUS*"].

[6] *Vu* (S.C.C.), *supra*, note 1, at paras. 3, 22.

[7] *R. v. Spencer*, [2014] S.C.J. No. 43, [2014] 2 S.C.R. 212, at para. 47 (S.C.C.) [hereinafter "*Spencer*"].

[8] *Fearon*, *supra*, note 1, at paras. 82-83.

open the possibility that, once police are armed with a computer warrant, they can conduct a dragnet search into our entire digital lives — consisting potentially of millions of photographs, videos, e-mails, diaries and private medical and banking documents. And in *Fearon* — despite acknowledging that a cell phone is a miniature computer containing a treasure trove of personal information about an individual — a majority of the Court held that the police had a limited right to conduct *warrantless* searches of a cell phone as a search incident to arrest.

The cynical way to read *Vu* and *Fearon* is that privacy matters but only to the extent that it does not fetter law enforcement, which is to say, it does not matter at all. Constitutional rights are meaningful only if they limit State power. If these six decisions on digital search and seizure have not succeeded in requiring more of law enforcement where our core privacy rights are at stake, they have not succeeded in protecting privacy at all.

The less cynical way to read these cases is that the law of digital search and seizure remains a work in progress. The task for lawyers and the trial courts will be to reconcile the Supreme Court's pro-privacy language with the actual holdings in *Vu* and *Fearon*. That task is the goal of this article. I suggest that the apparent tension between the Court's pro-privacy language and the holdings in *Vu* and *Fearon* can be reconciled by insisting on rigorous *ex post* review of police searches of computers and cell phones. While the Supreme Court in *Vu* did not impose a requirement of "search protocols" as a constitutional imperative in all cases, I suggest that in many cases the only way to achieve the appropriate balance between law enforcement needs and privacy rights is for issuing justices to impose a set of search protocols that constrain and limit the scope of the computer search. In the context of searches of cell phones incident to arrest, I suggest that the only way to achieve meaningful after-the-fact review is to require that police electronically record all warrantless cell phone searches.

Part 1 of this article will summarize the key lessons from the Supreme Court of Canada's six digital-search-and-seizure decisions from 2010 to 2014. Part 2 will focus on two of the most recent of those decisions, *Vu* and *Fearon*, and explain the apparent tension that exists between the pro-privacy language in *Morelli*, *Cole*, *TELUS*, *Vu* and *Spencer* and the actual holdings in *Vu* and *Fearon*. Part 3 will suggest that the only way to reconcile this tension is to insist on rigorous manner-of-search review, including a requirement of search protocols in the case of warranted searches, and a requirement that police video-record all warrantless cell phone searches.

1. Supreme Court of Canada Jurisprudence on Digital Search and Seizure

(a) Morelli (2010) and Cole (2011)

Morelli marked a technological awakening of the Supreme Court of Canada. The Court, for the first time, turned its mind to the highly intrusive nature of a search of one's personal computer. In *Morelli*, a computer technician had arrived at the accused's house to install a high-speed Internet connection. He noticed, among other things, Internet links to adult and child pornography in the browser taskbar's favourites list. The technician contacted a social worker, who informed the RCMP, which subsequently obtained a warrant to search the accused's computer. The ensuing search revealed evidence of child pornography. The Supreme Court held that the search violated section 8 of the Charter. The warrant should not have issued because statements contained in the ITO were misleading and erroneous.

The important part of the judgment for the purposes of this article, however, is the Court's analysis under section 24(2) of the Charter. The Court excluded the improperly obtained evidence under section 24(2) because of the highly invasive nature of a search of one's personal computer. Justice Fish wrote:

> It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer.
>
> First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created. The police scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet — generally by design, but sometimes by accident.
>
> .....
>
> Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.

> It is therefore difficult to conceive a s. 8 breach with a greater impact on the *Charter*-protected privacy interests of the accused than occurred in this case.[9]

The logic of *Morelli* drove the analysis in the Supreme Court's subsequent computer-privacy decisions. In *Cole*, the accused, a high school teacher, was permitted to use his work-issued and school board-owned laptop for incidental personal purposes. He browsed the Internet and stored personal information on his hard-drive. When a school technician found a hidden folder containing nude photographs of a female student on the accused's computer, he notified the principal. The principal copied the photographs onto a CD and seized the laptop, both of which were handed over to the police, who, without a warrant, reviewed their contents and created a mirror image of the hard drive for forensic purposes. The accused did not own the computer hardware but he did own the personal and private information stored on it — private information that "falls at the very heart of the 'biographical core' protected by s. 8 of the *Charter*".[10] Accordingly, the Supreme Court held that the accused had a reasonable expectation of privacy in his work-issued computer, and that the warrantless search of the computer had violated section 8.

(b) TELUS (2013)

The Court was confronted with a different technology-based challenge in *TELUS*, but like *Morelli* and *Cole*, the new realities created by digital technologies drove the Court's analysis. The police in *TELUS* obtained a general warrant and related assistance order under sections 487.01 and 487.02 of the *Criminal Code*,[11] requiring Telus to provide the police with copies of any stored text messages sent or received by two Telus subscribers. Telus applied to quash the general warrant arguing that the prospective, daily acquisition of text messages from their computer database constituted an interception of private communications and therefore required authorization under the wiretap authorization provisions in Part VI of the *Criminal Code*.

---

9 *Morelli*, *supra*, note 3, at paras. 2-3, 105-106.

10 *Cole*, *supra*, note 4, at para. 48.

11 R.S.C. 1985, c. C-46.

Part VI of the *Criminal Code* is Parliament's response to the dangers of allowing the State unfettered discretion to listen to and record our private telephone conversations. The need to prevent unnecessary state intrusions into our private lives is essential not just for privacy, but also for expressive freedom. As Harlan J. famously noted, "Were third-party bugging a prevalent practice, it might well smother that spontaneity — reflected in frivolous, impetuous, sacrilegious, and defiant discourse — that liberates daily life."[12]

These dangers moved Parliament in 1974 to enact what is now Part VI of the *Criminal Code*. The purpose of Part VI is to provide a "higher degree of protection … for private communications".[13] Its requirements are stricter than those of the other warrant provisions in the *Criminal Code* to reflect the heightened privacy interests at stake.[14] For example, unlike any other warrant provisions in the *Criminal Code*, a Part VI authorization can only be obtained where the judge is satisfied under section 186(1)(b) "that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures" (*i.e.*, investigative necessity).[15]

The issue in *TELUS* was whether Part VI — traditionally concerned with interception of telephonic *voice* communications — applied to the prospective acquisition of cell phone *text* messages. Taking a purposive approach, the plurality held that Part VI applied to the prospective acquisition of text messages. "Text messaging", wrote Abella J., "is, in essence, an electronic conversation. The only practical difference between text messaging and the traditional voice communications is the transmission process".[16]

The plurality's purposive approach was supported by the broad definition of "intercept" in the *Criminal Code*, which was not limited to traditional wiretapping (involving "bugging" a telephone line and

---

[12] *United States v. White*, 91 S. Ct. 1122, 401 U.S. 745 (1971), at 787-89 [hereinafter "*White*"], as quoted in *R. v. Duarte*, [1990] S.C.J. No. 2, [1990] 1 S.C.R. 30, at 54 (S.C.C.) [hereinafter "*Duarte*"].

[13] *TELUS*, *supra*, note 5, at para. 31, *per* Abella J.

[14] *Id.*, at para. 27, *per* Abella J.

[15] *Criminal Code*, *supra*, note 11, s. 186(1)(b). It should be noted that under s. 186(1.1) there are exceptions to the "investigative necessity" requirement where the wiretap relates to criminal organizations or terrorism offences.

[16] *TELUS*, *supra*, note 5, at para. 5.

listening to the conversation), but was defined to include, "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof"[17] — terms that could apply equally to the acquisition of text messages. Accordingly, the plurality concluded, Part VI should apply to the prospective acquisition of text messages.[18] "Technical differences inherent in new technology should not determine the scope of protection afforded to private communications."[19]

(c) R. v. Vu (2013)

The Court in *Vu* picked up where it left off in *Morelli* and *Cole*. The accused was charged with several drug-related offences, including theft of electricity. The police obtained a warrant authorizing the search of a residence for evidence of theft of electricity, including documentation identifying the owners and/or occupants of the residence. The Information to Obtain a Search Warrant ("ITO") indicated that the police intended to search for, among other things, "computer generated notes", but the warrant did not specifically authorize the search of computers. In the course of their search of the residence, police discovered two computers and a cellular telephone, which they searched without obtaining a new warrant. These searches led to evidence that Vu was the occupant of the residence.[20]

At trial, the accused claimed that these searches violated his rights under section 8 of the Charter because the search warrant did not specifically authorize the police to search the computers or the cellular phone. The trial judge accepted this argument and excluded most of the evidence found as a result of these searches and acquitted the accused of the drug charges.[21]

---

17 *Criminal Code*, *supra*, note 11, s. 183.

18 While the issue in *TELUS* concerned the applicability of Part VI to *prospective* interception of text messages (*i.e.*, *ex ante* authorization to intercept a future message), the reasoning in *TELUS* also supports an argument that Part VI should apply to the *retroactive* interception of text messages and e-mails (*i.e.*, any search of private electronic communications) on a cell phone or computer. See Factum of the BCCLA, *Fearon v. Her Majesty the Queen*, SCC Case No. 35298, online: <http://www.scc-csc.gc.ca/WebDocuments-DocumentsWeb/35298/FM060_Intervener_British-Columbia- Civil-Liberties-Association.pdf>. That discussion, however, is beyond the scope of this article.

19 *TELUS*, *supra*, note 5, at para. 5.

20 *Vu* (S.C.C.), *supra*, note 1, at para. 4.

21 *R. v. Vu*, [2010] B.C.J. No. 1777, 218 C.R.R. (2d) 98, at paras. 60-69 (B.C.S.C.).

The British Columbia Court of Appeal set aside the acquittal and ordered a new trial. It held that a computer was no different than "a four-drawer filing cabinet" when it came to search and seizure law.[22] The general rule when it came to physical objects, according to the Court of Appeal, is that a warrant authorizing a search of a specific location for specific things confers on those executing that warrant the authority to conduct a reasonable examination of anything at that location within which the specified things might be found. "Just as it cannot be said that a warrant to search for documentary evidence relating to a fraudulent scheme would not apply to a four-drawer filing cabinet …", the B.C. Court of Appeal wrote, "neither can it be said that such a warrant would not apply to a computer, the existence of which the police learn of after entering a residence".[23]

The Supreme Court of Canada disagreed. Its decision in *Vu* lays to rest the quaint notion that computers are no different from physical-world receptacles like filing cabinets, drawers and briefcases. It held that the police violated Vu's rights against unreasonable search and seizure under section 8 of the Charter when they searched the three electronic devices found on the premises. It rejected the B.C. Court of Appeal's holding that a computer is no different from a physical container. "Computers differ in important ways from the receptacles governed by the traditional framework," wrote Cromwell J. for a unanimous Court, "and computer searches give rise to particular privacy concerns that are not sufficiently addressed by that approach".[24] Specific, prior authorization to search a computer was necessary to comply with section 8 of the Charter.

The outcome in *Vu* is not surprising. The writing had been on the touch-screen since *Morelli*.[25] Nevertheless, before *Vu*, the approach of the British Columbia Court of Appeal had been accepted by learned trial and appellate courts across the country, which routinely compared computers to containers, briefcases,[26] "sealed box[es]",[27] "logbook[s],

---

[22] *R. v. Vu*, [2011] B.C.J. No. 2487, 250 C.R.R. (2d) 108, at para. 63 (B.C.C.A.) [hereinafter "*Vu* (B.C.C.A.)"].

[23] *Id*.

[24] *Vu* (S.C.C.), *supra*, note 1, at para. 2.

[25] *Morelli*, *supra*, note 3, at paras. 2, 105 ("[I]t is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer".)

[26] *R. v. Polius*, [2009] O.J. No. 3074, 196 C.R.R. (2d) 288, at para. 47 (Ont. S.C.J.) ("[a] cell phone is the functional equivalent of a locked briefcase …").

[27] *R. v. Burchell*, [2011] O.J. No. 4723, 246 C.R.R. (2d) 74, at para. 55 (Ont. S.C.J.).

diar[ies] or notebook[s]",[28] and "four-drawer filing cabinets".[29] *Vu* rejected these analogies and held what was implied but not explicitly stated in *Morelli* and *Cole*: that the old rules that protected privacy in an Analog World are insufficient in the Digital Age. Modern computers, cell phones and personal digital assistants are not analogous to the traditional "receptacles" found in the course of search and seizure.[30]

What makes computers and computer technology so different? The Court in *Vu* catalogued a number of important ways in which computers are qualitatively different from physical world receptacles and explained how these unique features affect digital privacy.

First, the *quantity* of the information stored on computers is unlike anything in the physical world.[31] For less than $100, anyone can purchase a computer hard drive with storage capacity of 1 terabyte (1,000 GB),[32] which is roughly equivalent to 500 million pages of text — or about the amount of information contained in all of the books on 12 floors of an academic library.[33] Given this "massive storage capacity", the Supreme Court noted, there is a significant difference between the search of a computer and the search of a briefcase or filing cabinet found in the same location.[34]

Second, the type of information stored on a computer is often intimate and private, thereby "fall[ing] at the very heart of the 'biographical core' protected by s. 8 of the *Charter*".[35] As the Court previously noted, virtually every aspect of one's private life is

---

[28] *R. v. Giles*, [2007] B.C.J. No. 2918, 2007 BCSC 1147, at para. 56 (B.C.S.C.).

[29] *Vu* (B.C.C.A.), *supra*, note 22, at para. 63.

[30] *Vu* (S.C.C.), *supra*, note 1, at para. 24 ("The privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets.").

[31] *Id*. ("Computers potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search.")

[32] See Best Buy Canada, online: Bestbuy.ca <http://www.bestbuy.ca/Search/SearchResults.aspx?path=ca77b9b4beca91fe414314b86bb581f8en20&query=hard+drive+external> (last visited October 26, 2015); "Hard Drives", online: PC Mag.com <http://www.pcmag.com/reviews/hard-drives> (last visited October 2, 2015).

[33] Orin S. Kerr, "Searches and Seizures in a Digital World" (2006) 119 Harv. L. Rev. 531 [hereinafter "Kerr"], at 542; see also Marc Palumbo, "How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment" (2009) 36 Fordham Urb. L.J. 977 [hereinafter "Palumbo"], at 995.

[34] *Vu* (S.C.C.), *supra*, note 1, at para. 41.

[35] *Id*., at para. 40; *Cole*, *supra*, note 4, at para. 48 (S.C.C.).

consolidated into one's computer, including "our most intimate correspondence", "details of our financial, medical, and personal situations", and "our specific interests, likes, and propensities" as revealed through the records of what we "seek out and read, watch, or listen to on the Internet".[36] People today use computers as photo albums, stereos, telephones, desktops, filing cabinets, waste paper baskets, televisions, postal services, playgrounds, jukeboxes, dating services, movie theaters, shopping malls, personal secretaries, virtual diaries and more.[37] Your computer may reveal to the world more about you than your spouse, family members or close friends ever could.

Third, the computer is a "fastidious record keeper".[38] Computers contain information that is automatically generated, often unbeknownst to the user. This computer-generated "meta-data" tracks information about who created a document on what date or who visited a given website at a particular time. It can reveal significant private information about the user's interests, habits and identity.[39]

Fourth, a computer retains files and data even after users think they have destroyed them.[40] When a user "deletes" a file, the operating system simply marks the disk clusters occupied by that particular file as available for future use by other files. If the operating system does not reuse that cluster for another file by the time the computer is searched, the file marked for deletion will be available for forensic examination.[41] Even if another file has been assigned to that cluster, a large amount of that data can be forensically recovered from the computer's "slack space", *i.e.*, space within the cluster left temporarily unused.[42] In an era where hard drive data storage now exceeds multiple terabytes, this means

---

[36] *Morelli*, *supra*, note 3, at paras. 3, 105; *Cole*, *supra*, note 4, at para. 47.

[37] Kerr, *supra*, note 33, at 569. See also Lesley Ciaruula Taylor, "The astonishing amount of personal data police can extract from your smartphone" (February 27, 2013), The Star.com, online: <www.thestar.com/news/world/2013/02/27/the_astonishing_amount_of_personal_ data_police_ can_extract_from_your_smartphone.print.html> (where a police search of a smart phone revealed 104 call logs, eight passwords, 422 text messages, six wireless networks, and 10,149 files of audio, pictures, text and videos — 378 of which were deleted).

[38] *Vu* (S.C.C.), *supra*, note 1, at para. 42.

[39] *Id*.

[40] *Id*., at para. 43.

[41] Edward T.M. Garland & Donald F. Samuel, "The Fourth Amendment and Computers: Is a Computer Just Another Container or Are New Rules Required to Reflect New Technologies?" (2009) 10 Ga. B.J. 14, at 16; Kerr, *supra*, note 33, at 542; *R. v. Little*, [2009] O.J. No. 3278, at para. 96 (Ont. S.C.J.) [hereinafter "*Little*"].

[42] *Vu* (S.C.C.), *supra*, note 1, at para. 43 (citing Kerr, *supra*, note 33, at 542).

that many of us unwittingly retain massive amounts of data we attempted to delete. Your computer's "delete" key thus is more appropriately described as the "hide" button — it hides files from the casual user but preserves them for the future forensic examiner.

Finally, a computer is rarely a stand-alone, self-contained entity. A computer that is connected to a network or to the Internet is a portal to a world exponentially larger than the computer itself.[43] A search of a computer for which the police have lawful authority to access will potentially give police access to other users' information stored on other devices and for which the police have no lawful authority to search.

These unique factors "call for distinctive treatment under s. 8 of the *Charter*".[44] The old bricks-and-mortar approach to section 8 cannot be applied haphazardly to computers. The "markedly different" privacy interests flowing from computers call for a rule requiring specific, prior authorization before the police can search a computer.[45]

(d) R. v. Spencer (2014)

Whereas *Morelli*, *Cole*, *TELUS* and *Vu* concerned privacy in data stored on digital devices, *Spencer* concerned privacy in one's virtual life. In *Spencer*, an officer of the Saskatoon Police Service was engaged in a child pornography investigation. Using the publicly available Limewire file-sharing software, he searched for users sharing child pornography. Limewire also permitted him to see the Internet Protocol ("IP") addresses associated with each user. He ran a list of IP addresses against a database with approximate locations and found that one of the IP addresses had an approximate location of Saskatoon, with Shaw Communications Inc. ("Shaw") as the Internet Service Provider.[46]

What he lacked, however, was a precise knowledge of where exactly the computer was and who was using it. He therefore made a request to Shaw under section 7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act*,[47] requesting the subscriber information

---

[43] *Vu* (S.C.C.), *supra*, note 1, at para. 44.

[44] *Id.*, at para. 45.

[45] *Id.*, at paras. 46-49.

[46] *Spencer*, *supra*, note 7, at paras. 7-12.

[47] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [hereinafter "PIPEDA"].

associated with the IP address. No warrant was obtained. Shaw complied with the request and provided their customer's name, address and telephone number.

The question on appeal was whether section 8 demands that a warrant be sought and obtained to access Internet subscriber information. The Crown argued that section 8 protects informational privacy only where the user has a reasonable expectation of privacy. In *Morelli* and *Cole*, the data searched involved information going to the accused's core biographical information. In *Spencer*, however, the information sought — the name, address and telephone number matching a publicly available IP address — did "not touch on the core of Mr. Spencer's biographical information".[48] There is no privacy in a name and address.

The Supreme Court disagreed. What was being sought was not simply generic biographical information; "it was the identity of an Internet subscriber which corresponded to particular Internet usage".[49] Knowing both the IP address, and associated user activity, combined with identifying information, would tell you a great deal about that individual's biographic core. Accordingly, the accused did have a reasonable expectation of privacy in the identifying information.[50]

The logic of the Court's reasoning is compelling when we understand privacy as anonymity. Privacy is often associated with the right to control personal information about oneself. But to think of privacy only as the "right to control information" obscures the equally important right to anonymity.[51]

Anonymity permits individuals to act in the public sphere but to preserve freedom from identification and surveillance.[52] An analogy with the physical world is helpful. We enjoy a degree of anonymity as we go about our daily lives. We may go to the office, the gym, the bar, the shopping mall, the medical clinic, the place of worship, or maybe even the swingers' club. These are all (to varying degrees) public places where we are no doubt seen by others. But we might feel more inhibited going

---

[48] *Spencer*, *supra*, note 7, at para. 25.

[49] *Id.*, at para. 32.

[50] *Id.*, at para. 45.

[51] See *id.*, at paras. 38-51; A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) 7; *Duarte*, *supra*, note 12, at 46; *R. v. Dyment*, [1988] S.C.J. No. 82, [1988] 2 S.C.R. 417, at 429 (S.C.C.); Andrea Slane & Lisa M. Austin, "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" (2011) 57 Crim. L.Q. 486 [hereinafter "Slane & Austin"].

[52] *Spencer*, *supra*, note 7, at para. 43 (citing Slane & Austin, *id.*, at 31-32).

to these places if there were a life-size nametag hanging over our heads everywhere we went. That inhibition might in turn stymie the creativity and spontaneity that are necessary for individuals to thrive in a free and democratic society.[53] "The mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a person may not be able to control who observes him or her in public."[54]

The Court cited *R. v. Wise*, a physical world case involving privacy as anonymity. The Court in *Wise* held that the ongoing monitoring of a vehicle's whereabouts on public highways using a tracking device amounted to a violation of the suspect's reasonable expectation of privacy.[55] It could have been argued that the suspect was driving his car in public areas for all the world to see, and therefore, did not have a reasonable expectation of privacy, but even the Crown conceded in *Wise* that ongoing beeper monitoring violates the suspect's reasonable expectation of privacy.[56]

Browsing the Internet is the digital world equivalent of driving around town. We drive from website to website — to shop, to visit our virtual worlds, to do our banking and to satisfy our quirky curiosities — in full view of each website we visit and our Internet service provider. Through the use of "cookies" and other devices, Internet search engines like Google and social networking sites like Facebook gather information about our likes, interests and shopping habits. Only "by guarding the link between the information and the identity of the person to whom it relates" can the user be assured that Internet activity remains private.[57]

---

[53] *White*, *supra*, note 12, at 787-89, as quoted in *Duarte*, *supra*, note 12, at 54; see also *R. v. Ward*, [2012] O.J. No. 4587, 2012 ONCA 660, at para. 48 (Ont. C.A.).

[54] *Spencer*, *supra*, note 7, at para. 44.

[55] *R. v. Wise*, [1992] S.C.J. No. 16, [1992] 1 S.C.R. 527, at 538 (S.C.C.).

[56] *Id*. It should be noted that *Wise* was decided at a time when the police were limited to fixing (now seemingly ancient "beepers" onto cars — technology that is now obsolete owing to GPS tracking devices). In *United States v. Jones*, 132 S. Ct. 945 (2012), the United States Supreme Court reached a similar result as in *Wise* in the context of modern GPS tracking devices, and in *Torrey Dale Grady v. North Carolina*, 135 S. Ct. 1368 at 1370 (2015), it clarified that its holding in *Jones* applies equally to tracking people as it does to vehicles.

[57] *Spencer*, *supra*, note 7, at para. 46.

(e) R. v. Fearon (2014)

The Court's first five digital-search-and-seizure decisions arguably expanded the ambit of our section 8 privacy rights and imposed new requirements on police seeking to search our digital devices. *Fearon* took an (unexpected) opposite turn. In a narrow 4-3 decision, the Supreme Court in *Fearon* held that law enforcement has the power — albeit a limited one — to conduct a warrantless search of a cell phone under the common law search-incident-to-arrest power.

Fearon was arrested following an armed robbery of a jewellery merchant at a Toronto flea market. Upon arrest, a pat-down search revealed Fearon's cell phone, which police accessed both at that moment and again later at the station. Scrolling through Fearon's photographs, the police found an incriminating draft text message referring to jewellery and opening with the words, "We did it…". They also found a photograph of a handgun. Police subsequently recovered the handgun during a search of the getaway vehicle. The trial judge found that the handgun used in the robbery was the same as the one in the photograph and found in the getaway vehicle.[58]

At trial and on appeal, Fearon argued that both searches violated his section 8 Charter rights and sought to have the inculpatory text message and photograph excluded under section 24(2) of the Charter. In response, the Crown argued that the searches were mere applications of the common law police power to search a suspect incident to arrest, and therefore reasonable under section 8 of the Charter.

A warrantless search is presumptively unreasonable.[59] But the common law in Canada has long recognized the search-incident-to-arrest power as a narrow exception to the presumptive rule.[60] For more than two decades, the search-incident-to-arrest exception has remained a limited exception because it has been tightly tied to its purposes. First, the arrest itself must be lawful. Second, the search must aim at a valid search-incident-to-arrest purpose, such as (1) police safety; (2) safeguarding evidence; or (3) discovering evidence.[61]

---

[58] *Fearon*, *supra*, note 1, at paras. 5-9.

[59] *R. v. Nolet*, [2010] S.C.J. No. 24, [2010] 1 S.C.R. 851, at para. 21 (S.C.C.) [hereinafter "*Nolet*"]; *Hunter v. Southam Inc*., [1984] S.C.J. No. 36, [1984] 2 S.C.R. 145, at 161 (S.C.C.) [hereinafter "*Hunter*"].

[60] See *Cloutier v. Langlois*, [1990] S.C.J. No. 10, [1990] 1 S.C.R. 158, at 181-82 (S.C.C.); *R. v. Caslake*, [1998] S.C.J. No. 3, [1998] 1 S.C.R. 51, at para. 17 (S.C.C.) [hereinafter "*Caslake*"].

[61] *Caslake*, *id.*, at para. 25.

The question in *Fearon* was whether the warrantless search of a suspect's cell phone falls within this exception. Justice Cromwell, writing for the majority, held that it should. He noted that cell phones, like computers, are quantitatively and qualitatively different from physical world storage devices — both because of their immense storage capacity and the intimate, personal nature of the information stored on them — but held that to exclude them from the search-incident-to-arrest exception would upset the balance between privacy interests and law enforcement's needs. Justice Cromwell held that the appropriate balance can be struck by permitting but circumscribing the search of cell phones incident to arrest. This would be accomplished by ensuring that the search is truly incidental to the arrest in that it promotes at least one of the valid law enforcement purposes — *i.e.*, protecting the police, the accused or the public; preserving evidence; or discovering evidence, "including locating additional suspects, in situations in which the investigation will be stymied or significantly hampered absent the ability to promptly search the cell phone incident to arrest".[62]

To help ensure that searches incident to arrest of cell phones remained tightly moored to these legitimate purposes, after-the-fact review is especially important. Accordingly, Cromwell J. wrote, officers must make "detailed notes" of what they have examined on the cell phone.[63] A careful record is essential to ensuring meaningful after-the-fact review.[64]

2. Digital Privacy: A Step Forward or Just a Sidestep?

(a) The Problem with Fearon

Until *Fearon*, it appeared that the Supreme Court was marching along a teleological path to greater privacy protections in the Digital Age. *Fearon* arguably undermines that inference. Whereas the *Morelli/ Cole/TELUS/Vu/Spencer* line of cases focused on bringing section 8 Charter rights into the Digital Age, *Fearon* appears to try to squeeze a Digital Age problem back into an Analog World box.

---

62 *Fearon*, *supra*, note 1, at para. 83.
63 *Id.*, at paras. 82-83.
64 *Id.*, at para. 82.

The search-incident-to-arrest rules were devised at a time when people carried only their wallet, keys and maybe a pack of cigarettes[65] on their person. In 1998, when *Caslake* — the Supreme Court's leading search-incident-to-arrest case — was decided, it would have seemed far-fetched to imagine people carrying around miniature computer-phones containing copies of all of their private correspondence, their scheduling calendars, as well as their Internet browsing history and information stored on any number of mobile phone "apps". As the unanimous United States Supreme Court observed in its decision on warrantless cell phone searches in *Riley v. California*, "[a] decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary … Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives — from the mundane to the intimate."[66]

A search of a cell phone can reveal as much about its user as a search of that person's laptop or desktop computer — and then some. Canadians increasingly engage in private text-based communications using their cell phones. More than any other computing device, cell phones contain massive amounts of private communications. In 2008, 44 per cent of Canadians said that text messaging was the most common activity they performed on their cell phone aside from voice calls; 11 per cent said e-mailing; and 6 per cent said instant messaging.[67] Since 2008, Canadians' use of text messaging has more than quadrupled. In 2012, the total text messages sent in Canada numbered 96.5 billion.[68] As MacKenzie J. observed in *R. v. Giles*, "the explosion of e-mail and other text-based modes of instantaneous communication has meant that much of our communication that was once exclusively verbal is now by electronic text".[69] Nearly all of these communications can be retrieved

---

[65] See, *e.g.*, *United States v. Robinson*, 414 U.S. 218 (1973).

[66] *Riley v. California*, 134 S. Ct. 2473 (2014), at 2490 (U.S. Sup. Ct.) [hereinafter "*Riley*"].

[67] 2008 Wireless Attitudes Study Conducted on behalf of the Canadian Wireless Telecommunications Association, at 13, September 12, 2008, available online: <http://www.cwta.ca/CWTASite/english/pdf/DecimaStudy_2008.pdf>.

[68] Canadian Wireless Telecommunications Association, "Mobile Originated Text Messages in Canada Yearly (2002-2012)", online: <http://www.cwta.ca/blog/2013/05/06/canadians-sent-96-5-billion-text-messages-in-2012/>.

[69] *R. v. Giles*, [2007] B.C.J. No. 2918, 2007 BCSC 1147, at para. 43 (B.C.S.C.) [hereinafter "*Giles*"]; *R. v. Belcourt*, [2012] B.C.J. No. 2636, 296 C.C.C. (3d) 163, at para. 9 (B.C.S.C.).

from a cell phone — including those that the user has deleted.[70] Thus, the police often search cell phones for the primary purpose of retrieving private communications.[71] That type of search — the acquisition of private communications — has traditionally garnered a higher (not lower) degree of protection in the form of protections under Part VI of the *Criminal Code*.

In addition, cell phones — unlike our larger computing devices — are invariably on our person at any given time. As the United States Supreme Court noted in *Riley*, cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy".[72] Cell phones also keep invisible records of every cellular tower and every WiFi network the user has ever logged into.[73] Given that most of us carry our cell phones everywhere, these records give law enforcement access to what is essentially a retroactive tracking device, with which they can retrace all of the user's movements, beginning from when the user first purchased the phone.[74] Thus, the vast repository of highly personal data

---

[70] Extraction Report in *In the Matter of the Search of an Apple I-Phone model A1332 with IC#_____*, online: <https://www.aclu.org/files/assets/iphone-forensics-report_redacted.pdf> [hereinafter "Extraction Report"]; American Civil Liberties Union, "New Document Sheds Light on Government's Ability to Search iPhones", February 26, 2013, online: <https://www.aclu.org/blog/technology-and-liberty-criminal-law-reform-immigrants-rights/new-document-sheds-light>. See also *R. v. Vye*, [2014] B.C.J. No. 98, 301 C.R.R. (2d) 180, at para. 5 (B.C.S.C.) [hereinafter "*Vye*"]; *Giles*, *supra*, note 69, at paras. 18-19; *Vu* (S.C.C.), *supra*, note 1, at para. 43. The cell phone in *Giles* could store 10,000 messages, and the storage capacity of cell phones has grown by more than 4,000 times since *Giles*. See *Apple – iPhone 6 – Technical Specifications*, online: <https://www.apple.com/ca/iphone-6/specs/>.

[71] In *Vye*, *supra*, note, 70, at para. 5, the police retrieved 633 text messages from the accused's phone over a six-month period, including deleted messages; in *R. v. Hiscoe*, [2013] N.S.J. No. 188, 328 N.S.R. (2d) 381, at paras. 5-8 (N.S.C.A.), the police reviewed a number of text messages in the accused's cell phone at the arrest scene before downloading the contents of the entire phone to a DVD; in *R. v. Liew*, [2012] O.J. No. 1365, 2012 ONSC 1826, at para. 26 (Ont. S.C.J.) [hereinafter "*Liew*"], the police conducted a "fairly extensive search" of the text messages in the accused's cell phone at the police detachment; and in *Giles*, *supra*, note, 69, at para. 13, the police retrieved 164 e-mail messages from the co-accused's cell phone.

[72] *Riley*, *supra*, note 66, at 2484.

[73] Extraction Report, *supra*, note 70.

[74] See, *e.g.*, *United States v. Davis*, No. 12-12928 (slip opinion), at *76 (11 Cir. May 5, 2015), *per* Martin J., dissenting. In *Davis*, the government obtained 67 days of cell site location data disclosing the suspect's location every time he made or received a call. During that 67-day period, the suspect received 5,803 phone calls, so the prosecution had 11,606 data points about his location.

that the Court was concerned about protecting in *Morelli* and *Vu* is arguably even more at risk in the *Fearon* search-incident-to-arrest context than in the home computer context.

The majority's ruling in *Fearon* also creates another curious tension with *Vu*. If the police find your cell phone or computer in your home pursuant to a valid warrant, they cannot search your device (unless the warrant specifically allows it),[75] but if they arrest you without a warrant with those same devices, they have the right to search them.[76]

That distinction might have made more sense in a pre-Digital Age. In earlier times, no search of a place was more invasive than the search of one's home.[77] This is no longer true. As the United States Supreme Court wrote in *Riley*:

> In 1926, Learned Hand observed … that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form — unless the phone is.[78]

Given the privacy interests at stake in *Fearon*, one would think that the law enforcement interests must be particularly strong to justify the warrantless search. Curiously, however, they appear more attenuated than even the ordinary search-incident-to-arrest context.

The *Fearon* majority identified three legitimate purposes of the search incident to arrest of cell phones: (1) police and public safety; (2) safeguarding the evidence; or (3) discovering evidence. It is difficult to see how any of these goals would be undermined by a warrant requirement.

---

[75] *Vu* (S.C.C.), *supra*, note 1, at paras. 46-49.

[76] *Fearon*, *supra*, note 1, at paras. 82-83.

[77] *Weeks v. United States*, 232 U.S. 383 at 390 (1914) (discussing the "a man's house is his castle" doctrine); see also *R. v. Tessling*, [2004] S.C.J. No. 63, [2004] 3 S.C.R. 432, at para. 22 (S.C.C.) (individuals are entitled to a high expectation of privacy in the home because it is "the place where our most intimate and private activities are most likely to take place").

[78] *Riley*, *supra*, note 66, at 2490-91 (citing *United States v. Kirschenblatt*, 16 F. 2d 202, 203 (2d Cir.)).

It is uncontroversial that the police have the lawful authority to seize the phone, provided that they have a reasonable basis to believe that the phone may contain evidence of the alleged offence.[79] So there is no real concern that the phone will be used as a physical weapon. If the concern, on the other hand, is the risk that the suspect has summoned his confederates via text or voice communication to come to his aid and ambush the police, then, as Karakatsanis J. noted in dissent, the "exigent circumstances" exception can ably deal with this Hollywood scenario (provided that the police have reasonable grounds to believe that the suspect has summoned his accomplices to his aid).[80] Indeed, the exigent circumstances exception is a well-established common-law exception to the warrant requirement, which permits police to search or seize property where there is a "risk of imminent loss or destruction of the evidence or contraband" and "where there is a concern for public or police safety".[81] Parliament codified the exigent circumstances exception under section 487.11 of the *Criminal Code*, providing that police may exercise powers of search and seizure "without a warrant if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant".[82]

The other goals identified by the *Fearon* majority as justifying a limited warrantless search — the preservation of evidence and discovery of evidence — are both valid goals, but it is difficult to see how these goals would be frustrated if the police were to seize the cell phone at the scene but wait to search it until they had obtained a warrant.[83] As the dissenting judges observed, "[t]he text messages and photographs

---

[79] For distinction between the right to seize and right to search, see *Cole*, *supra*, note 4, at para. 65 ("The police may well have been authorized to take physical control of the laptop and CD temporarily, *and for the limited purpose of safeguarding potential evidence of a crime until a search warrant could be obtained*."); see also *R. v. Butters*, [2014] O.J. No. 2159, 309 C.R.R. (2d) 299, at para. 36 (Ont. C.J.) ("If the police can ameliorate the risks of further criminality … by taking physical control over a computer tower without putting the material privacy interest at risk by delaying inspection until a warrant is obtained, the law should and in my view does accommodate it."); *R. v. Seguin*, [2015] O.J. No. 1424, 2015 ONSC 1908, at para. 35 (Ont. S.C.J.) (noting that "[t]here is a distinction to be drawn between seizing a computer for the purpose of searching it and actually searching it").

[80] *Fearon*, *supra*, note 1, at paras. 139-140, *per* Karakatsanis J., dissenting; see also *Riley*, *supra*, note 66, at 2484-85.

[81] *R. v. Kelsy*, [2011] O.J. No. 4159, 283 O.A.C. 201, at para. 24 (Ont. C.A.).

[82] *Criminal Code*, *supra*, note 11, s. 487.11.

[83] *Liew*, *supra*, note 71, at para. 124 ("The seizure of the phone goes a long way towards achieving the objective of ensuring that evidence against the accused is secured.")

discovered in this case … generally would not disappear if police wait to acquire a warrant."[84]

The Crown raised the concern that if the phone were not searched immediately, then the suspect's confederates could remotely delete the data on that device. Even assuming a highly sophisticated group of criminals, this problem is not without a relatively easy solution. The police could simply remove the cell phone's battery thus disconnecting it from any remote or cellular networks, or they could place the phone in a "Faraday bag", an inexpensive aluminum bag that blocks wireless communications.[85] Given the incredibly high privacy interests at stake in a cell phone (potentially millions of e-mails, texts and personal photographs) and the attenuated law enforcement interest (nothing they can get at the scene cannot be retrieved after a warrant is obtained) the balance struck in *Fearon* appears off-kilter.

(b) Morelli/Vu: The Unfinished Business of Setting Limits on Searches of Digital Devices

While the *Morelli*/*Vu* line of cases appears to offer more to individual privacy than *Fearon*, its impact is potentially modest. The lesson for law enforcement from *Morelli*, *Cole*, *TELUS*, *Vu* and *Spencer* is clear: If you want to search someone's computer or other digital device, get a warrant and get the proper warrant. But if this is the only lesson, then these cases will have been a Pyrrhic victory for digital privacy.

Vu demands that the warrant specifically authorize the search of digital devices. Obtaining such a warrant, however, is not a tough task for law enforcement. Going forward, the police must establish in the Information to Obtain that there are reasonable grounds to believe that any computers they discover will contain the evidence for which they are looking.[86] This is not a high hurdle. Most people alive today own multiple computer devices and use them constantly. Given the ubiquitousness of computer use, there is a good chance that, if a crime has been committed, there will be some evidence on a computer. Unless we develop additional rules constraining the *manner* of a computer search, there is a danger that *Vu* will simply become a lesson to police to

---

84 *Fearon*, *supra*, note 1, at para. 146, *per* Karakatsanis J. dissenting.

85 *Id*., at para. 144.

86 *Vu* (S.C.C.), *supra*, note 1, at para. 48.

include computer-related terms in their ITO boilerplate. The question thus becomes: Once the police have grounds to obtain a computer warrant, what sensible limitations should be applied to limit the manner of search?

This question has traditionally been a key concern of section 8. Our section 8 rights are protected primarily by two rules. First, police must obtain judicial authorization (usually a search warrant) for the search before they conduct it.[87] The warrant requirement ensures that before a search is conducted, an impartial judicial officer (*i.e.*, the issuing justice) turns her mind to the state's interest in conducting the search and the individual's privacy interest in being left alone. Second, even where a warrant has been issued, the search must be conducted in a reasonable manner.[88] This second prophylactic rule ensures that the search is no more intrusive than is reasonably necessary to achieve law enforcement's objectives.

The *Morelli*/*Vu* line of cases deal with section 8's prior authorization requirement. They do not speak directly to section 8's *reasonable manner* requirement. And it is the reasonable manner requirement that is especially vexing when it comes to computers and digital information.[89]

This problem flows from a computer's unique features. First, the search and seizure process is inverted when it comes to digital devices. In the physical world, one is entitled to a high reasonable expectation of privacy in one's home, for example. As such, the search of one's home is seen as particularly invasive.[90] Search warrants grant police permission to search a dwelling usually for only limited periods of time (often only one day). Items are then seized. The search-and-seizure process with respect to computers is inverted. After seizing the computer during the initial search, the police may take months (or even years) to conduct a full forensic search of the device. This inversion means that the time limits which would apply in the classic search-and-then-seizure sequence are meaningless. Related to the inversion of the search/seizure process is

---

87 *Hunter v. Southam Inc.*, *supra*, note 59, at 160.

88 *R. v. Collins*, [1987] S.C.J. No. 15, [1987] 1 S.C.R. 265, at 278 (S.C.C.).

89 See Gerald Chan, "Life after *Vu*: Manner of Computer Searches and Search Protocols" in J. Cameron, B.L. Berger & S. Lawrence, eds., *Constitutional Cases 2013* (2014) 67 S.C.L.R. (2d) 433 (for extended commentary on manner-of-search issues) [hereinafter "Chan"].

90 *R. v. Tessling*, [2004] S.C.J. No. 63, [2004] 3 S.C.R. 432, at para. 22 (S.C.C.) (individuals are entitled to a high expectation of privacy in the home because it is "the place where our most intimate and private activities are most likely to take place").

the problem of overseizure. Because the computer is seized first and searched later, the police are necessarily seizing the haystack to search for the needle.

If we are to take seriously *Morelli*'s holding that there are few searches more intrusive than the computer search, then these lengthy computer searches are the privacy equivalent of having one's home open to the police for months on end — for them to come and go as they please as new case leads develop — without any need to go back before a judicial officer to get a new warrant.

Second, as noted above, a computer is rarely a stand-alone, self-contained entity. Thus, even where there are reasonable grounds to believe that a computer contains documents evidencing crime, there is a strong likelihood that this evidence is intermingled with private information on other computers that the government has no reasonable grounds to search or seize.[91]

The problem of intermingling is particularly acute in the digital world. In the physical world, the physical location specified in the warrant necessarily narrows the ambit of the search. If the warrant gives the police the authority to search "1000 Elm Street", then there is little danger that the police, acting in good faith, will stray into the neighbours' houses.

Not so with computers. The digital world is different, particularly in settings where data is shared between multiple users or where data is stored on common hardware because the boundaries between one computer and the next are amorphous. For example, the police may have reasonable grounds to believe that a suspect has accessed child pornography from the computer in his living room. But what if that computer is a shared computer, used by the suspect's spouse and two adolescent children? Each of these individuals has a reasonable expectation of privacy in data stored on the computer. The police have no business seizing or searching data belonging to those third parties, but their data is intermingled with data for which they do have grounds to seize. Let us further assume that the spouse is a physician who sometimes uses the home computer to correspond with patients. Each of those patients also has a privacy interest in that correspondence stored on

---

[91] See, *e.g.*, *Cole*, *supra*, note 4, at para. 88 (illegal photographs intermingled with photographs of the accused's wife); *In the Matter of the Search of 3817 W. West End*, 321 F. Supp. 2d 953, at 958 (N.D. Ill. 2004) [hereinafter "*3817*"]; *United States v. Otero*, 563 F.3d 1127, at 1132 (10th Cir. 2009).

the computer, raising the specter of potentially limitless innocent third party privacy interests commingled with the data that the police have grounds to seize.[92]

The challenges may be even more complex in the workplace. The typical workplace computer does not exist in a silo. In many companies and institutions, multiple computers are connected to each other across cities, countries and continents via company network servers. It is not unusual for thousands of users to store their work product on a common or shared server. Each one of those users potentially has privacy interests in data stored on that network. And if the information stored on the computer includes private (or privileged) client information, then each one of those clients may have an expectation of privacy in data stored on the company network.

The problem of intermingling will only be exacerbated as users continue to shift data storage from devices to the "cloud". Cloud computing refers to the capacity of Internet-connected devices to display and edit data stored on remote servers.[93] Often users may not even know whether particular information is stored on the device or in the cloud. But where data is stored in the cloud, it will be intermingled with the data of potentially millions of other users — all of whom have unique privacy interests.

Further, doctrines that limit the invasiveness of physical searches do not map easily — or at all — onto computer searches. The ambit of a physical-world search warrant is limited by the realities of the physical world, which prevent the typical search from becoming limitless, dragnet searches. In United States Fourth Amendment parlance, this is sometimes known as the "elephant-in-a-matchbox" doctrine (*i.e.*, if the warrant authorizes police to search only for an elephant, then they have no business looking in a matchbox).[94] Likewise, the plain-view doctrine, which authorizes the seizure of unanticipated evidence inadvertently discovered where the officer is lawfully in the premises,[95] is

---

[92] See *United States v. Comprehensive Drug Testing Inc*., 621 F3d 1162 at 1176-77 (9th Cir. 2010) (*en banc*), modifying 579 F.3d 989 (9th Cir. 2009) (*en banc*) [hereinafter "*Comprehensive Drug Testing Inc.*"].

[93] *Riley*, *supra*, note 66, at 2491.

[94] See *Vu* (B.C.C.A.), *supra*, note 22, at para. 47; see also *Jackson v. Florida*, 18 So. 3d 1016, at 1028, 1029 (Fla. Sup. Ct., 2009), cert. denied 130 S. Ct. 1144 (2010).

[95] *R. v. Buhay*, [2003] S.C.J. No. 30, [2003] 1 S.C.R. 631, at para. 37 (S.C.C.).

circumscribed in the physical world. To qualify for plain view treatment, the items seized must be found within the area being searched and they must be conspicuous.[96]

These concepts do not translate into the digital world. What is in plain view on the computer or cell phone? This question has been the subject of much academic discussion, but yields no easy answer.[97] In the digital world, the plain view exception has the potential to swallow up a virtually limitless space. As long as the investigator is making a good faith effort to search only for evidence specified in the warrant, then anything discovered on the computer is potentially captured under the plain view doctrine. Law enforcement will also argue vigorously that once given permission to access a computer, they must be able to search every file and folder — at least in cursory fashion — because the suspect may be adept at hiding or concealing files in difficult-to-find places. This gives breadth to the plain view exception that is unfathomable in the physical world context.

3. The Way Forward: Rigorous Manner-of-Search Review

In light of these challenges, manner-of-search review is the next frontier in digital-search-and-seizure litigation. *Vu* and *Fearon* each raise distinct challenges to privacy, but the solution to both is to insist on rigorous manner-of-search review.

In the search warrant context, judges and justices of the peace should insist that police seeking a computer search warrant propose "search protocols" as a means to restrict the invasiveness of a computer search. These protocols will help constrain and limit the invasiveness of a computer search, and will foster meaningful after-the-fact review.

In the search-incident-to-arrest context in *Fearon*, there is no opportunity to impose judicially-sanctioned, *ex ante* search restrictions because the *Fearon* exception is, by definition, warrantless. This makes after-the-fact review especially important (which the majority acknowledged in *Fearon*).[98] Rigorous after-the-fact review is essential to ensure that cell phone searches incident to arrest do not become

---

[96] *Id*.

[97] See Ray Ming Chang, "Why the Plain View Doctrine Should Not Apply to Digital Evidence" (2007) 12 Suffolk J. Trial & App. Adv. 31, at 33; Lisa Jorgenson, "In Plain View: R v Jones and the Challenge of Protecting Privacy Rights in an Era of Computer Search" (2013) 46 U.B.C. L. Rev. 791, at 798-18.

[98] *Fearon*, *supra*, note 1, at paras. 82-83.

fishing expeditions. And to enable that rigorous review, police will need to make complete and accurate records of their cell phone search, which will require that they video-record or otherwise digitally log their searches.

(a) Ex Ante Rules and Search Protocols (Where a Warrant Is Required)[99]

"Search protocols" refer to *ex ante* rules, proposed by the police and approved by the issuing justice, that specify how the police will conduct a computer search. The point of a search protocol is to ensure that the search is "conducted in a reasonable manner", as section 8 of the Charter requires.

Search protocols can involve myriad possibilities. They can define, and thereby constrain, the search for specified keywords, file types and date ranges; they can limit the search to text files or graphics files; and they can focus on certain software programs.[100] They can also prescribe the use of more sophisticated search tools based on constantly evolving forensic technologies that allow law enforcement to conduct computer searches without opening files by searching based on "file headers"[101] or "hash values".[102] Some of those programs, such as Guidance Software's

---

[99] I have written about the importance of search protocols in an earlier article. See Nader Hasan, "*R. v. Vu*: The Right to Digital Privacy and the Need for Search Protocols" (2014) 35:1 *For the Defence* 6 [hereinafter "Hasan"]. See also Chan, *supra*, note 89.

[100] *3817*, *supra*, note 91, at 959.

[101] A "file header" is an internal computer file identifier that tells the computer about the file. Even if someone tries to disguise an image file by giving it a name and extension that makes it look like a word processing document, the computer and forensic software will not be fooled because the file header will reveal the true nature of the file. See Christina M. Schuck, "A Search for the Caselaw to Support the Computer Search Guidance in *United States v. Comprehensive Drug Testing*" (2012) 16 Lewis & Clark L. Rev. 741, at 750 [hereinafter "Schuck"].

[102] A "hash value" for a file is an identifier that characterizes a data set. The relationship between a hash value and its data set compares roughly to the relationship between an organism and its DNA sequence or fingerprint. See *R. v. Braudy*, [2009] O.J. No. 347, at para. 21 (Ont. S.C.J.) [hereinafter "*Braudy*"], *per* Stinson J. (explaining that the hash value "is an unique number [of a digital file] that could only be the product of applying the same formula to an identical file: it is a so-called 'digital finger print'"); see also Lily Robinton, "Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence" (2010) 12 Yale J. L. & Tech 311, at 326-27 [hereinafter "Robinton"]; Kerr, *supra*, note 33, at 544-46.

"EnCase Forensic Toolkit", are already used by law enforcement throughout Canada and other jurisdictions.[103]

Vu should not be read as closing the door on search protocols. In *Vu*, the Court declined to mandate search protocols as a matter of constitutional imperative, but made it clear that it was not "foreclos[ing] the possibility that our developing understanding of computer searches and changes in technology may make it appropriate to impose search protocols in a broader range of cases in the future".[104] The Court noted that as the case law develops, "after-the-fact review may lead courts to set out specific rules according to which searches must be conducted", which can then be imported into search protocols.[105] In particular, the Court wrote that issuing justices may find it "necessary and practical" to impose search protocols in cases involving "confidential intellectual property or potentially privileged information".[106] In those cases, protocols could be imposed when police first request authorization to search the computer. Alternatively, issuing justices may prefer a "two-stage approach" where they would first issue a warrant authorizing the *seizure* of the computer and then have police return for an additional authorization to search the seized device, which would include a protocol that would limit the scope of the search.[107]

(i) Search Protocols Help Address the Unique Problems Posed by Computers' Unique Features

As discussed above, the unique features of computers — the highly personal nature of computer data, the vastness of their storage capacity and their interconnectedness — make properly limited computer searches more challenging. Only carefully tailored search protocols can address the unique manner-of-search issues posed by computers and digital technologies.

Where police are going into a situation where there is likely to be intermingling of data — *i.e.*, if the computer is found in a multi-person dwelling unit or is the server of a large company — the police should be

---

[103] See Palumbo, *supra*, note 33, at 1001; see also *Little*, *supra*, note 41, at para. 27, *per* Fuerst J. (describing officer's testimony regarding EnCase forensic software).

[104] *Vu* (S.C.C.), *supra*, note 1, at para. 62.

[105] *Id.*, at para. 55.

[106] *Id.*, at para. 62.

[107] *Id.*

able to articulate in the ITO what innocent third party privacy interests exist, and what measures they will take to minimize the intrusion. The issuing justice should, in turn, scrutinize those measures and issue a warrant that adequately protects those third-party interests as well as the suspect's residual privacy interests. Police should bear the onus of proving what search protocols will permit them to strike the appropriate balance between privacy and the needs of law enforcement because they "have available to them the necessary software, technology and expertise to enable them to tailor their searches in a fashion that will generate the information they seek, if it exists, while at the same time minimizing the intrusion on the computer user's privacy rights in other information stored on the computer".[108]

While search protocols entail infinite possibilities and will be highly case-specific, they may include:[109]

- Where the search involves a shared network or shared hard-drive, the protocols should specify that the police may not search any part of hard-drive or server that the suspect did not access.
- If the search involves a shared network or shared hard-drive, the protocols should specify that the police should not examine files created prior to when the suspect first gained access to those shared devices.
- Date-range and keyword search restrictions will be appropriate in many cases.[110]
- Where applicable, the protocols should specify that police must work with third parties to ensure that safeguards are put in place to protect privileged, private and commercially sensitive information.[111]

---

[108] *R. v. Jones*, [2011] O.J. No. 4388, 107 O.R. (3d) 241, at para. 50 (Ont. C.A.).

[109] Hasan, *supra*, note 99, at 8.

[110] See *R. v. Cross*, [2007] O.J. No. 5384, at paras. 21-27 (Ont. S.C.J.) (search warrant contained a protocol that the police shall "limit search to information concerning e-mail of August 6, 2005…").

[111] See *Lavallee, Rackel & Heintz v. Canada (Attorney General)*, [2002] S.C.J. No. 61, [2002] 3 S.C.R. 209, at para. 49 (S.C.C.) ("In the interim, I will articulate the general principles that govern the legality of searches of law offices as a matter of common law until Parliament, if it sees fit, re-enacts legislation on the issue."); *supra*, note 92, at 1175-77 (9th Cir. 2010) (*en banc*), modifying 579 F.3d 989, at 1166-76 (9th Cir. 2009) (*en banc*).

- In certain investigations, specific file types ought to be excluded from the search because of the unlikelihood that incriminatory information will be found in such files. For example, investment advisers engaged in inside trading are unlikely to snap "selfies" of their unlawful trades, so there is a strong case for excluding image and video files from the search in such a case.

- Police currently have access to certain forensic software programs that have the potential to limit the invasiveness of the computer search.[112] As noted above, forensic software currently available to police allows analysts to conduct searches based on "file headers" or "hash values". The police can then, for example, compare hash values found in the computer files against databases of hash values known to be child pornography.[113] In many cases, it will be reasonable to insist that the police perform hash-value or file-header search before embarking on a more intrusive file-by-file review of the entire computer.

- Where police intend to use particular forensic programs to search the computer, those programs should be listed in the search protocols.

- The protocols should specify an end date of the search. If the police want to extend the search beyond the end date, then they ought to go back before the issuing justice and persuade her why they need ongoing access to someone's computer.

(ii) Search Protocols Foster Reviewability

Section 8 is concerned with preventing unreasonable searches from occurring — not merely with punishing unreasonable searches after the fact.[114] An advantage of search protocols is that there will be fewer unreasonable searches because the police will know the rules of the game before they conduct the search.

And when the defence does challenge the reasonableness of the search, the search protocols will provide judges with an objective

---

[112] See Palumbo, *supra*, note 33, at 1001; see also *Little*, *supra*, note 41, at para. 27, *per* Fuerst J. (describing officer's testimony regarding EnCase forensic software).

[113] *Braudy*, *supra*, note 102, at paras. 21-23.

[114] *Vu* (S.C.C.), *supra*, note 1, at para. 51.

baseline against which to assess the reasonableness of the police search. If the police failed to adhere to the search protocols, then the search is *prima facie* unreasonable. If the police did adhere to the search protocols, then defence counsel would have to show why these protocols were unreasonable.

Without that objective baseline, the section 8 *voir dire* will become a battle of experts conducted in a vacuum. The police will explain why they could not have conducted the computer search any other way. The defence computer expert will testify that there were many ways as to how the search could have been conducted in a less intrusive way. Search protocols would give judges an objective baseline against which to assess these arguments.

(iii) Search Protocols Will Ensure the Integrity of Evidence

Search protocols can also help law enforcement ensure the integrity of evidence by requiring that computer searches to be done in controlled laboratory settings by technically trained officers. Computers are sophisticated devices. Improper handling — or even manual computer searches done outside of the laboratory setting — can damage or destroy evidence.[115] Simply opening a file or turning on a computer can overwrite data, and may alter the "meta-data", which show when the suspect created or last accessed a file.[116]

The manual search of a computer is the equivalent of walking into a murder scene with muddy boots and removing bare-handed a knife from the victim and dropping it in one's coat pocket. Search protocols can help law enforcement address these risks. In both *Vu* and in *Fearon*, for example, the officers performed a manual search on the suspect's digital devices.[117] If the time that the device was accessed had been at issue in those cases, the officer likely would have compromised that evidence simply by accessing the device.

---

115 Schuck, *supra*, note 101, at 751.

116 Robinton, *supra*, note 102, at 324-25.

117 *Vu* (B.C.C.A.), *supra*, note 22, at para. 18.

(b) Ex Post Review and the Importance of Record-Keeping (Warrantless Context)

The Charter's default position is that the State needs a warrant to search a place or thing,[118] including — or rather, especially — digital devices. The carve-out in *Fearon* is exceptional. But to ensure that the *Fearon* exception does not swallow the general rule, courts must insist on rigorous *ex post* manner-of-search review of searches and seizures of digital devices.

The majority in *Fearon* was alive to this concern, noting that "[a]fter-the-fact judicial review is especially important where, as in the case of searches incident to arrest, there is no prior authorization."[119] Going forward, the courts will have to devise ways to ensure meaningful after-the-fact review of warrantless cell phone searches. This challenge is unique from the warranted context, where the manner of search can be constrained *ex ante* by search protocols attached to the warrant.

Meaningful after-the-fact reasonableness review involves scrutinizing the police conduct to determine whether the police search was more far-reaching than necessary, with regard to the objectives of the search; the nature of the offence for which the police have reasonable grounds to believe has been committed; the grounds for believing that the device will afford evidence of the offence; and the means at law enforcement's disposal to narrow the parameters of the search.

As outlined above, the imposition of search protocols constraining the warranted search will foster meaningful review and it will help prevent overbroad searches before they happen. But *Vu* makes it clear that regardless of whether the issuing justice imposes *ex ante* restrictions, the police do not have the licence to rummage indiscriminately through all of the data on the device:

> By now it should be clear that my finding that a search protocol was not constitutionally required in this case does not mean that once police had the warrant in hand, they had a licence to scour the devices indiscriminately. They were bound, in their search, to adhere to the rule that the manner of the search must be reasonable. Thus, if, in the course of their search, the officers realized that there was in fact no reason to

---

[118] Where a search is carried out without a warrant, it is presumptively unreasonable. *Nolet*, *supra*, note 59, at para. 21; *Hunter*, *supra*, note 59, at 161.

[119] *Fearon*, *supra*, note 1, at para. 82.

> search a particular program or file on the device, the law of search and seizure would require them not to do so.[120]

Trial-level decisions have taken up this concept and the principles they have developed can be applied to the *Fearon* context and help foster meaningful review. First, in *R. v. Sop*, the accused was charged with two offences relating to child pornography.[121] The police had obtained a warrant to seize and search the suspect's electronic devices. There were no search protocols attached to the warrant.[122] The police went on to scour 40 terabytes of data on multiple computers (which the court found was equivalent to an amount of paper that would "fill 14,000 pickup trucks").[123] The accused argued that the search was overbroad; the trial judge agreed and held that this approach violated the accused's section 8 rights. Although the warrant did not specify any search restrictions, the police were still bound by the reasonable manner requirement of section 8 of the Charter. The police knew the file names and hash values of the child pornography files for which they were looking. But rather than begin the search using a targeted keyword search or a hash value search, the police manually combed through *all* of the data.[124] They did so despite having the technological tools available to perform targeted searches. The Court wrote:

> There is no evidence before me that the police first tried to search by name, date or hash values. Depending on what the police found after these searches, they may have to apply different search techniques or apply for a new search warrant.
>
> Rather than try this approach the police combed through 40 TB of data which contained in addition to the alleged child pornography, adult pornography, lifestyle choices, sexual orientation, business travel, personal affairs and business affairs all of which would have been extremely private and sensitive information to the Applicant.
>
> .....
>
> Still from a search procedure point of view, one would have thought the police would have used the parameters they knew to try to narrow their

---

120 *Vu* (S.C.C.), *supra*, note 1, at para. 61.

121 *R. v. Sop*, [2014] O.J. No. 3666, 317 C.R.R. (2d) 1 (Ont. S.C.J.) [hereinafter "*Sop*"].

122 *Id.*, at para. 105.

123 *Id.*, at para. 146.

124 *Id.*, at para. 143.

> search and if they were unsuccessful they would have likely been justified doing a more invasive search. From the number of hours the police spent doing this search, it is almost unbelievable they wouldn't have tried to use the specific information they had to their advantage.
>
> If the police had been unable to locate the movies and photographs they knew about by doing different parameter searches they would have been authorized to continue looking by other methods … without further authorization. However, it appears to this court that the police simply wanted to do a general search of all 40 TB of storage space. Perhaps because of the amount of storage space they seized they thought they may have stumbled onto something much larger than the 11 videos and 380 pictures that they knew had been downloaded.[125]

The Court went on to exclude the unlawfully obtained evidence under section 24(2) of the Charter because the decision to "search every and each file in the accused's vast computer system when they had very specific information about what they were looking for" was "unwarranted and somewhat egregious".[126]

In *R. v. Nurse*, two co-accused were charged with murder.[127] The Crown's theory was that Nurse hired the co-accused Plummer to carry out the killing. The police had grounds to believe that the two co-accused communicated with each other about their plot using their Blackberry devices. The OPP sent the devices to the RCMP to conduct a full "data dump" and analysis of every file on the devices. The Court held that this manner of search was unduly overbroad and a violation of section 8 of the Charter. The officers "should have realized that there was no reason to search all programs and files on the devices".[128] Because the relevant evidence consisted of recent communications between Nurse and Plummer, the search should have been limited to "BBM chats, SMS (texts), emails, notes, and call logs".[129] Searching the web browsing history, photographs and Internet cookies was unreasonable under the circumstances.

Meaningful *ex post* manner-of-search review was possible in *Sop* and *Nurse* because there was a record detailing the extent of the search. The need for a comprehensive record of the search was top-of-mind for

---

125 *Id*., at paras. 143-144, 147-148.
126 *Id*., at para. 163.
127 *R. v. Nurse*, [2014] O.J. No. 4932, 322 C.R.R. (2d) 262 (Ont. S.C.J.).
128 *Id*., at para. 24.
129 *Id*., at para. 34.

the *Fearon* majority. Justice Cromwell suggested that one way to ensure meaningful review in the warrantless context is to require that officers "make detailed notes of what they have examined on the cell phone".[130] Indeed, the majority writes that a requirement of detailed note-taking "should be imposed as a matter of constitutional imperative" because the *Fearon* exception involves an "extraordinary search power that requires neither a warrant nor reasonable and probable grounds".[131]

The majority includes only a single sentence explaining what "detailed notes" means in this context. These notes should "generally" include: (1) applications searched, (2) the extent of the search, (3) the time of the search and (4) its purpose and duration.[132]

It will be necessary for the lower courts to flesh out these requirements. A bare requirement that officers "take detailed notes" pertaining to these four broad categories will not foster meaningful review.[133] As any criminal lawyer can attest, a given officer's idea of "detailed notes" will vary with the length of the police officer's foot. Meaningful after-the-fact review in the warrantless search context requires more than "detailed notes". It requires meticulously accurate and thoroughly complete records. Given the privacy interests at stake — and the attendant risks that the police's searches could easily drift into fishing expeditions — the police should be able to account for every button they press and every keystroke they make on the digital device. Anything short of such a complete and accurate record will frustrate meaningful after-the-fact review.

It would, of course, be cumbersome for police officers to manually record in their notebooks every keystroke they make while conducting the search. Many of these warrantless searches will take place on-scene — either roadside, as in Mr. Fearon's case, or in some other inconvenient circumstance. Accordingly, unless and until the technology becomes available to create a digital log of the officer's roadside search, courts ought to insist that officers make a video record of the search.

---

130 *Id.*; see also *Fearon*, *supra*, note 1, at para. 82.

131 *Fearon*, *id.*

132 *Id.*

133 See *contra R. v. Jones*, [2015] S.J. No. 89, 329 C.R.R. (2d) 320, at paras. 63-65 (Sask. Prov. Ct.) (where the Court held that the officer's transcription of the two text messages he purported to have reviewed satisfied *Fearon*'s "detailed notes" requirement).

Electronic video recording will create a complete and accurate record and foster meaningful after-the-fact review. Knowing that defence counsel will have a video recording of their search will help to ensure that officers take seriously the requirement that warrantless searches be narrowly tailored and truly incidental to the arrest. It would have the desired effect of "helping police officers focus on the question of whether their conduct in relation to the phone falls squarely within the parameters of a lawful search incident to arrest".[134] The video recording requirement is also much less cumbersome and less time-consuming than requiring officers to capture the same information in their notes.

The video recording of evidence is not a novel concept. In many jurisdictions, videography is routinely used to record crime scenes. It is also increasingly common for police to video record the execution of a search of a dwelling conducted pursuant to a warrant.[135] It is also now routine for the police to electronically record interviews of suspects and witnesses.[136] And increasingly, citizens and groups are calling for police officers' entire interactions with members of the public to be video recorded (despite the impact on privacy).[137] The Innocence Project identifies the video recording of interrogations as a key safeguard against false confessions.[138] Video recording reduces the incidence of police misconduct. If interrogators know that their acts are being monitored, it is less likely that they will employ tactics that overstep their lawful authority. It will also make instances of misconduct easier to identify.

In those situations, having an unassailable record of what happened — including the precise sequence of events — is invaluable. These same rationales for video recording evidence in the above-mentioned contexts apply with equal vigour to video recording of cell phone searches. Rifling through a suspect's cell phone is a tempting proposition because it is so easy to do and because there are no witnesses. It is less tempting if

---

134 *Fearon*, *supra*, note 1, at para. 82.

135 See *R. v. Allan*, [2010] O.J. No. 1740, 211 C.R.R. (2d) 244, at para. 88 (Ont. S.C.J.) (drawing an adverse inference from the officers' failure to record the execution of the warranted search).

136 See, *e.g.*, *R. v. Khelawon*, [2006] S.C.J. No. 57, [2006] 2 S.C.R. 787 (S.C.C.).

137 See, *e.g.*, CBC News, "Police body cameras flagged by privacy commissioners" (February 18, 2015), online: <http://www.cbc.ca/news/technology/police-body-cameras-flagged-by-privacy-commissioners-1.2962041>.

138 Innocence Project, "False Confessions & Recording of Custodial Interrogations" (August 12, 2015), online: <http://www.innocenceproject.org/free-innocent/improve-the-law/fact-sheets/false-confessions-recording-of-custodial-interrogations> (last visited October 26, 2015).

the officer knows that the search is being recorded. The knowledge that each keystroke is being electronically recorded will force the officer to carefully turn his mind to the legitimate goals of the search incident to arrest.

A video record will help establish that the officer's search remained moored to its purpose and did not stray into a fishing expedition. If the officer legitimately feared that the suspect had summoned his confederates for assistance (a scenario the *Fearon* majority contemplated), then reviewing the most recent text messages or e-mails or numbers dialed on the call log is arguably a reasonable search. Rummaging through older e-mails or reviewing the Internet browser history is not tailored to the purpose of ensuring officer safety.

Still photography and screen shots of the cell phone search can be selective, but a video is an all-encompassing record of the search. Videography would capture not only the entire scope of the search, but also its sequence. Sequencing matters when it comes to assessing the reasonableness of the manner of search. There may be instances where it is permissible to look in less obvious places. A suspect is not necessarily going to store his incriminating documents in the "incriminating documents" folder. But one would expect that an officer, acting reasonably, would begin with the obvious places first and then move to the less obvious ones.[139] An officer looking for a photograph of a gun should not begin with the Internet browser history. A video record would provide an objective baseline against which one could evaluate the reasonableness of the officer's sequence of search.

If a complete and accurate record of the search is preserved, then counsel will have the proper evidentiary foundation to challenge the manner of search. If the officer cannot articulate why they took a given step in conducting the warrantless search, then the search may be unreasonable and a violation of section 8. On the other hand, officers behaving properly will have video evidence to corroborate their testimony.

---

[139] The United States case law suggests that the police must follow the "obvious to obscure" approach when conducting computer searches as a way to ensure that searches do not become fishing expeditions. See *United States v. Burgess*, 576 F.3d 1078, at 1094 (10th Cir. 2009) (the police must "first look in the most obvious places and as it becomes necessary to progressively move from the obvious to the obscure"). This approach has been adopted in *Sop, supra*, note 121, at para. 145.

II. CONCLUSION

The first five years of the Supreme Court of Canada's digital-search-and-seizure jurisprudence has been a mixed bag for privacy. The Court's awareness of how computer and cell phone technologies affect privacy, and that these new realities should inform the scope of section 8 Charter rights is a welcome development. But these decisions deal primarily with only one aspect of section 8 — the warrant requirement. They do not fully address an equally important prophylactic rule of section 8 — that even lawful searches must be conducted in a reasonable manner.

To strike the proper balance between law enforcement needs and privacy, searches conducted pursuant to a warrant must be appropriately constrained. It will be important to develop rules that constrain the *manner* of a computer search conducted pursuant to a computer search warrant. Going forward, courts ought to (and counsel ought to urge courts to) include "search protocols" in computer search warrants that will impose limits on *how, where, when* and *for how long* the police can search our electronic devices.

The Court's recent decision in *Fearon* poses a different but related set of challenges. *Fearon* permits a warrantless search of one's computer device under the search-incident-to-arrest exception. Although the search power pursuant to this exception is limited, the potential for abuse is vast. The task of trial courts and of counsel is to ensure rigorous *ex post* review of warrantless cell phone searches. This will require precise record-keeping. Mere note-taking may not be enough. Courts ought to insist on the digital recording — either by way of video or other digital device — to ensure the best record of the search incident to arrest. Only such meticulous record-keeping will ensure meaningful *ex post* review of warrantless cell phone searches.