Canadian Journal of Law and Technology

Volume 13 | Number 2 Article 3

6-1-2015

Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smartphone Data Granted in R. v. Fearon

Jordan Fine

Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smartphone Data Granted in *R. v. Fearon*

Jordan Fine[*]

Given the incredible rate of smartphone technological evolution, is it about time the Supreme Court of Canada devised a special test to give law enforcement agents significantly more power to search through phone data without a warrant upon arrest of a suspect? In R. v. Fearon*, the majority did just that. But this article argues the opposite is true: the increasing potential for immense privacy infringements when police search powerful and constantly evolving technological devices demands a greater limitation to police powers.*

In recent cases, the Supreme Court has agreed with the position that limitations are needed concerning computers. Additionally, the weaknesses in law enforcement procedure described by the majority are already served sufficiently by existing principles which do not infringe Canadians' Charter *rights. Future cases should distinguish the majority decision for these reasons and recognize the thoughtful and practical dissent. Otherwise, there is a danger that this unreasonable expansion of police power to search citizens, combined with anticipated technological evolution in both smartphones and government surveillance initiatives, will have a corrosive effect on the freedom guaranteed to Canadians by section 8 of the* Charter.

> 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 . . . 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.
>
> *R. v. Morelli*, Fish J.[1]

> 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 . . . In these reasons, then, when I referred to "computers"', I include within that term the cellular telephone.
>
> *R. v. Vu*, Cromwell J.[2]

---

[*] JD Candidate 2017, *Osgoode Hall Law School*.

1 *R. v. Morelli*, 2010 SCC 8, 2010 CarswellSask 150, 2010 CarswellSask 151, [2010] 1 S.C.R. 253, [2010] S.C.J. No. 8 (S.C.C.) at para 2 [*Morelli*].

2 *R. v. Vu*, 2013 SCC 60, 2013 CarswellBC 3342, 2013 CarswellBC 3343, [2013] 3 S.C.R. 657, [2013] S.C.J. No. 60 (S.C.C.) at para 38 [*Vu*].

INTRODUCTION

The Supreme Court of Canada in *R. v. Fearon*[3] devised an exception giving law enforcement agents significantly more power to search cell phones upon the arrest of a suspect, a decision both peculiar and alarming. The exception is peculiar because it was developed after a flurry of recent jurisprudence which acknowledged the profundity of privacy infringement when police search powerful technological devices. It is alarming because, if followed, it gives law enforcement a right of way through the *Charter*'s protection of privacy interests, directly into the private lives of Canadians. Moreover, the exception grants power to law enforcement where sufficient and appropriate authority to search cell phones already existed. Future cases should distinguish *Fearon* for these reasons and recognize Justice Karakatsanis's thoughtful and practical dissent. Otherwise, there is a grave danger that this unreasonable expansion of police power to search citizens, combined with anticipated technological evolution in both smartphones and government surveillance initiatives, will have a corrosive effect on the freedom promised to Canadians by Section 8 of the *Charter*.

I. A CURSORY OVERVIEW

(a) The Peculiar Facts

Two men, one armed (allegedly Kevin Fearon), robbed a jewellery merchant. They were arrested, but the handgun and loot eluded police. Immediately upon arrest, Fearon's phone was searched. The officer, Sergeant Hicks, "'had a look through the cell phone, saw some things in that cell phone, and seized it at that point in time as evidence in relation to the investigation.'"[4] Hicks testified that while he did not recall specifics, "[h]e was looking to see if there was any evidence that might be on there, so he could take it under control for himself or to let somebody else know who may be doing the investigation that there are things on that phone that may be related to their ongoing investigation."[5] The police found photos of the elusive "smoking gun" as well as a draft text referring to jewellery with the self-incriminating words "[w]e did it."[6]

Despite his criminal incompetence and likely guilt, Fearon is, as a Canadian, still entitled to protection from unreasonable search and seizure as set out by section 8 of the *Charter*.

---

3 *R. v. Fearon*, 2014 SCC 77, 2014 CarswellOnt 17202, 2014 CarswellOnt 17203, [2014] 3 S.C.R. 621, [2014] S.C.J. No. 77 (S.C.C.) [*Fearon*].

4 *R. v. Fearon*, 2010 ONCJ 645, 2010 CarswellOnt 10077, [2010] O.J. No. 5745 (Ont. C.J.) at para 20, affirmed 2013 CarswellOnt 1703 (Ont. C.A.), affirmed 2014 CarswellOnt 17202, 2014 CarswellOnt 17203 (S.C.C.) [*Fearon* C.J.].

5 *Ibid* at para 21.

6 *Ibid* at para 24.

(b) What Did the Court Do?

The issue in *Fearon* was framed as: "Does [the common law power enabling police to search incident to a lawful arrest] permit the search of cell phones and similar devices found on the suspect?"[7] The answer should have been "yes and no"—yes to the device, no to the data inside.[8] The majority chose instead to merely answer in the affirmative, and included limiting conditions that did not differentiate between devices and data.

During the Court's deliberations, the majority acknowledged that "the search of a cell phone has the potential to be a much more significant invasion of privacy than the typical search incident to arrest."[9] Yet, the majority's response to the question at issue inexplicably trivialized that potential. They set forth a four-step approach allowing cell phone searches incident to an arrest (SITA) under restrictive circumstances:

> [A] search will comply with s. 8 where:
> (1) The arrest was lawful;
> (2) The search is truly incidental to the arrest in that the police have a reason based on a valid law enforcement purpose to conduct the search, and that reason is objectively reasonable. The valid law enforcement purposes in this context are:
> (a) Protecting the police, the accused, or the public;
> (b) Preserving evidence; or
> (c) *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;
> (3) The *nature and the extent of the search are tailored to the purpose of the search*; and
> (4) *The police take detailed notes* of what they have examined on the device and how it was searched.[10]

The potential erosion of the privacy protections promised to Canadians by section 8 of the *Charter* is highlighted by the italicized passages above. Investigations are inherently stymied where evidence exists, but is not discovered. While it appears most investigations will meet these criteria, the cost of being unable to acquire valuable evidence must be weighed against privacy interests.

What does the Court mean by taking "detailed notes," and how is it regulated? Justice Cromwell details an obligation to "keep a careful record"

---

7 *Fearon*, *supra* note 3 at para 1.

8 Megan Savard & Rebecca McConchie, "Come Back with a Warrant: Why and How Courts Should Protect our Privacy Interest in Digital Information" (2013) 34:4 For the Defence.

9 *Fearon*, *supra* note 3 at para 58.

10 *Ibid* at para 83 [emphasis added].

which includes "applications searched, the extent of the search, the time of the search, its purpose and its duration."[11] Yet, this direction is general, non-exhaustive, and sets a low threshold of stymying an investigation, the combination of which does not appear to serve as clarification for law enforcement agents. It may be less evident from the facts of *this* case, but consider that perfectly innocent citizens may be lawfully arrested on reasonable and probable grounds.[12] Despite such citizens' innocence, the grounds for arrest may effortlessly permit a search through their smartphone data under the *Fearon* test.

(c) What Was the Majority's Motive?

Though it may appear that Fearon's patent guilt led the majority to formalize the new test, this notion is quashed by both the Court's holding that the search infringed on Fearon's rights, and in Justice Cromwell underlying reasoning. Fearon's appeal concerned arguments based on sections 8 and 24(2) of the *Charter*, meaning if the Court established evidence taken from his phone was done so in an unreasonable manner infringing his section 8 rights, that evidence could be excluded from proceedings. The need to bypass that infringement would explain why the majority crafted such an exception. Nonetheless, they concluded that the search of Fearon's phone did indeed breach his section 8 rights.[13]

The underlying reasoning the majority offered for modification is short-sighted. Justice Cromwell's explanation was that "a prompt search of a suspect's cell phone may serve important law enforcement objectives."[14] While the virtue in serving important law enforcement objectives is obvious, this explanation is unsatisfactory. There are many paths to serving those objectives—the imposition of constant surveillance on all citizens, for example. But surveillance states are criticized precisely because the *Charter* demands that we balance law enforcement objectives with privacy interests. For this reason, it is unsurprising that Justice Karakatsanis leads her dissent by referencing George Orwell's *1984*, as it encapsulates the need to limit developments which may serve law enforcement, but whose adverse consequences far outweigh its benefits.[15] The modified test does not account for the obvious potential it has to infringe on Canadians' liberties.

Justice Cromwell's test intends to help law enforcement, but overreaches at the cost of infringing privacy, while also failing to serve its own purpose. The expansion of police powers to do cursory searches of phones in SITAs is partially

---

[11] *Ibid* at para 82.

[12] Tim Quigley, "R. v. Fearon: A Problematic Decision" (2015) 15 C.R. (7th) 281.

[13] *Fearon*, *supra* note 3 at paras 86-88.

[14] *Ibid* at para 46.

[15] *Ibid* at para 102, Karakatsanis J., dissenting.

redundant to the existing doctrine of exigent circumstances, which allows a desirable scope of power without significantly infringing privacy.

Before addressing the wealth of reasons to resist the panoptic-friendly jurisprudence applied by the majority, I will let the Court itself explain why there is such a high privacy interest at stake in smartphone searches.

II. THE SUPREME COURT. . .

(a) On Section 8 Searches and Privacy Interests

What makes this case an outlier is that the Supreme Court has recently dealt with multiple cases where privacy rights and technology intersect.

To begin, a majority of the Supreme Court in *R. v. Cole* confirmed that employees have a reasonable expectation of privacy in their computers under section 8. They explained:

> Privacy is a matter of reasonable expectations. An expectation of privacy will attract *Charter* protection if reasonable and informed people in the position of the accused would expect privacy. If the claimant has a reasonable expectation of privacy, s. 8 is engaged, and the court must then determine whether the search or seizure was reasonable.[16]

Once engaged, two opposing forces have stakes in section 8. The first is the protection it affords Canadians' liberties. Justice Cromwell recently described privacy as "a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society."[17] Undoubtedly, the Supreme Court has acknowledged that *Charter* protection against unreasonable search and seizure is essential to our freedom.

The competing force is found in the language of section 8 and the use of the word "unreasonable." The prohibition against searches is not absolute—there exists common law recognition that law enforcement agents can make SITAs.[18]

---

[16] *R. v. Cole*, 2012 SCC 53, 2012 CarswellOnt 12684, 2012 CarswellOnt 12685, [2012] 3 S.C.R. 34, [2012] S.C.J. No. 53 (S.C.C.) at paras. 35-36 [*Cole*] [citations & emphasis omitted].

[17] *R. v. Spencer*, 2014 SCC 43, 2014 CarswellSask 342, 2014 CarswellSask 343, [2014] 2 S.C.R. 212, [2014] S.C.J. No. 43 (S.C.C.) at para 15 [*Spencer*].

[18] *Canada (Director of Investigation Research, Combines Investigation Branch) v. Southam Inc.*, 1984 CarswellAlta 121, 1984 CarswellAlta 415, (*sub nom.* Hunter v. Southam Inc.) [1984] 2 S.C.R. 145, [1984] S.C.J. No. 36 (S.C.C.); *R. v. Beare* (1987), 1987 CarswellSask 674, 1987 CarswellSask 675, EYB 1987-67944, [1988] 2 S.C.R. 387, [1987] S.C.J. No. 92 (S.C.C.) [*Beare* cited to S.C.R.]; *R. v. Debot*, 1989 CarswellOnt 111, 1989 CarswellOnt 966, EYB 1989-67472, [1989] 2 S.C.R. 1140, [1989] S.C.J. No. 118 (S.C.C.) [*Debot* cited to S.C.R.]; *Cloutier c. Langlois*, 1990 CarswellQue 8, 1990 CarswellQue 110, EYB 1990-67780, [1990] 1 S.C.R. 158, [1990] S.C.J. No. 10 (S.C.C.) [*Cloutier* cited to S.C.R.]; *R. v. Caslake*, 1998 CarswellMan 1, 1998 CarswellMan 2, [1998] 1 S.C.R. 51, [1998] S.C.J. No. 3 (S.C.C.).

At a minimum, pat-downs or frisks are acceptable behaviours by police.[19] The range of searches has extended to fingerprints and vehicle searches.[20] Conversely, the scope of the SITA power is limited. Taking blood and performing strip searches have been found as violations under certain contexts.[21] Taking hair samples, teeth impressions, and buccal swabs have been found to "very seriously violate[]. . .the. . .right to be free from unreasonable search and seizure" as well as violate the section 7 right to security and principles of fundamental justice.[22]

These cases, referenced by both the majority and the dissent in *Fearon*, are as helpful as they are troubling: helpful by establishing a spectrum between classes of searches seen as inherently "reasonable" and those seen as contravening section 8 privacy interests; troubling because analogizing between fingerprints and smartphones is risky business. The apparent desire to limit the scope of potential searches suggests the spectrum does not cover immaterial data.

So where on the spectrum does a search of a cell phone's *contents* fall? Where does any technology-based infringement fall? Several cases have begun to set a standard which may clarify the particular circumstances of *Fearon*.

(b) On Technological Issues in Lawful Arrests

Regarding technology, a number of cases have debated the spectrum of the reasonable expectation of privacy. A thermal intrusion on a suspect's dwelling does not violate the reasonable expectation of privacy afforded by section 8, nor does digital recording ammeter data (a device which measures electrical power flowing into a residence).[23] In *R. v. Spencer* the Court defended section 8 in light of police requests for IP address information through PIPEDA, stating:

> Since [in this case] the police do not have the power to conduct a search for subscriber information in the absence of exigent circumstances or a reasonable law, I do not see how they could gain a new search power through the combination of a declaratory provision and a provision enacted to promote the protection of personal information.[24]

---

[19] *Cloutier*, *supra* note 18 at paras 60-65; *Debot*, *supra* note 18 at paras 78-79.

[20] *Beare*, *supra* note 18 at para 22; *R. v. Stillman*, 1997 CarswellNB 107, 1997 CarswellNB 108, [1997] 1 S.C.R. 607, [1997] S.C.J. No. 34 (S.C.C.) at para 128 [*Stillman*]; *R. v. Nolet*, 2010 SCC 24, 2010 CarswellSask 368, 2010 CarswellSask 369, EYB 2010-175730, [2010] 1 S.C.R. 851, [2010] S.C.J. No. 24 (S.C.C.) at paras. 42-54.

[21] *R. v. Dyment*, 1988 CarswellPEI 7, 1988 CarswellPEI 73, EYB 1988-67715, [1988] 2 S.C.R. 417, [1988] S.C.J. No. 82 (S.C.C.) [*Dyment*]; *R. v. Golden*, 2001 SCC 83, 2001 CarswellOnt 4301, 2001 CarswellOnt 4253, REJB 2001-27031, [2001] 3 S.C.R. 679, [2001] S.C.J. No. 81 (S.C.C.).

[22] *Stillman*, *supra* note 20 at paras 48-51.

[23] *R. v. Tessling*, 2004 SCC 67, 2004 CarswellOnt 4351, 2004 CarswellOnt 4352, REJB 2004-72161, [2004] 3 S.C.R. 432, [2004] S.C.J. No. 63 (S.C.C.) at paras. 63-64; *R. v. Gomboc*, 2010 SCC 55, 2010 CarswellAlta 2269, 2010 CarswellAlta 2270, [2010] 3 S.C.R. 211, [2010] S.C.J. No. 55 (S.C.C.) at paras. 41, 95.

[24] *Spencer*, *supra* note 17 at para 73.

Unfortunately, these cases did not involve a lawful arrest—otherwise they could have provided more guidance for following SITA protocol for electronic devices.

The Ontario Superior Court in *R. v. Polius* recommended cell phone-specific SITA-related privacy expectations. In that case, the suspect *was* arrested lawfully.[25] The contents of his phone were exhaustively examined without warrant for three days.[26] The Court ruled that the arresting officer had reasonable grounds to search the accused's phone based on witness testimony alleging the suspect had communicated to a murder accomplice regarding the victim. The Court stated outright that "the power to seize a cell phone during a SITA where there is reason to believe it may afford evidence of the crime does not include a power to examine the contents of the cell phone without a prior judicial authorization, absent exigent circumstances."[27] The Supreme Court in *Fearon* found the judgment in *Polius* unpersuasive.

(c) On the Most Profound Invasions of Privacy

The Supreme Court spoke at length on the nature of computer searches in *R. v. Morelli*, where Justice Fish suggested that searches of personal computers might be the most intrusive invasions of privacy. *Morelli* is not a case of SITA, but an information to obtain a search warrant (ITO). However, Justice Fish expressed the Court's majority opinion on any section 8 breach involving a computer, stating: "[i]t 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."[28]

Given the comprehensive jurisprudential views on section 8 breaches and technology, it is surprising that the majority in *Fearon* could:

1. Admit the similarities between smartphones and personal computers;
2. Suggest that all phones, smart or dumb, are to be treated alike; and
3. Develop and apply a test which gives police the low-threshold power to commit a warrantless breach of section 8 protection on any lawful arrest.

III. THE MAJORITY'S TECHNOLOGICAL MISSTEPS

(a) Failure to Analogize to Computers

The majority overlooked prior pertinent Supreme Court of Canada discussions of Canadians' reasonable expectations of privacy pertaining to electronic devices. In *R. v. Vu*, Justice Cromwell himself delivered a judgment expressing strong sentiments about how computers create information without

---

[25] *R. v. Polius*, 2009 CarswellOnt 4213, [2009] O.J. No. 3074 (Ont. S.C.J.) at para 18 [*Polius*].

[26] *Ibid* at para 23.

[27] *Ibid* at para 32.

[28] *Morelli*, *supra* note 1 at para 106.

users' knowledge and retain information users try to erase. In criminal investigations, "[this information can] enable investigators to access intimate details about a user's interests, habits, and identity, drawing on a record that the user created unwittingly."[29]

The existing implications of privacy over the contents of computers discussed in cases like *Vu*, *Spencer,* and *Morelli* should extend to privacy over the contents of smartphones. All smartphones can store immense amounts of auto-generated data unbeknownst to the user, and usually feature cross-platform capabilities: files on personal computers are uploaded to the cloud, then synchronized with the phone.[30] At a minimum, the smartphone can be considered an extension or peripheral device of the computer, housing the same browsing history, cached files, and correspondence—in addition to being the user's primary communication device and camera. Therefore, if case law suggests laptop searches are significant intrusions of privacy, phone searches are equal if not greater intrusions.

Smartphones are not mere analogues of computers. We do not frequently take photographs or make private calls using laptops. We rarely immediately share our photos and videos using personal computers, broadcasting our location to our social network or the world. The portability and versatility of our pocket-sized, GPS-equipped, always-on mobile devices create a window to intimate personal details which the Supreme Court has confirmed Canadians have a right to withhold from state agents.[31]

Based on Justice Fish's prior commentary, it should have followed that the Supreme Court would agree that if smartphones are *at least* analogous to computers, they accordingly demand as high a level of reasonable privacy expectations as in a search of a suspect's dwellings. The majority even acknowledged smartphones as "the functional equivalent of computers" but then distinguished them, suggesting "not every search is inevitably a significant intrusion."[32] It is unclear why they asserted this despite having established numerous times in prior jurisprudence that high expectations are found to exist in the context of informational privacy.[33] It is possible this illogical conclusion derived from their choice to not differentiate between generations of phones.

---

[29] *Vu*, *supra* note 2 at para 42.

[30] Brian X. Chen, *Always On: How the iPhone Unlocked the Anything-Anytime-Anywhere Future—and Locked Us In* (Boston: Da Capo Press, 2012) at 130-143.

[31] *R. v. Plant*, 1993 CarswellAlta 94, 1993 CarswellAlta 566, EYB 1993-66899, [1993] 3 S.C.R. 281, [1993] S.C.J. No. 97 (S.C.C.) at para 27.

[32] *Fearon*, *supra* note 3 at para 54.

[33] E. Michael Power, *The Law of Privacy* (Markham, Ont.: LexisNexis Canada, 2013) at 245.

(b) All Phones Are One in the Eyes of the Law

On facts of this case, the majority could have arrived at a more reasonable conclusion based on the differences between smartphones (used for communication, computing, and data storage) and disposable "dumbphones" (including the cheap prepaid "burner phones" typically used for the nefarious purposes expressed by the majority's discussion of valid police objectives).[34] Stating that they "should not differentiate among different cellular devices based on their particular capacities when setting the general framework for the search power," the majority missed an opportunity to distinguish sophisticated smartphones from burners, which have limited features, are more difficult to trace, and provide an inexpensive method of regularly changing phone numbers.[35]

Making that distinction might have worked with the facts of *Fearon*—more importantly, it would have acknowledged the rapidly evolving technological environment to which the law should aim to adapt. Fearon's phone is described in the trial court judgment as a Telus LG285, a discontinued flip phone within the "burner" class of devices, lacking a touchscreen, high-resolution camera, and social media application capabilities.[36] To suggest that this phone bears any similarity to an iPhone 6 is akin to comparing a MacBook Air to a Commodore 64. Smartphones and dumbphones are too distinct to bear any categorical similarities besides the capacity for emailing, photographing, and making and receiving calls. The majority's refusal to differentiate between the two is meritless.

Marking the appropriate legal boundary between classes of phones is not a simple task for the courts, and the technological insight required to do so may be better left to legislation.[37] Nevertheless, declaring that no line should be drawn, ostensibly grouping all mobile devices together, posits an unrealistically static determination of innovation. Assuredly, the constantly evolving nature of technology will continuously distance the resemblance between powerful "'mini-computer[s]'" and their predecessors.[38]

The dynamic nature of technological evolution in smartphones contributes to the majority's miscalculation of the efficacy that a power to perform cursory searches of "burner" phones incident to arrest might yield. The LG285 and

---

[34] *Fearon*, *supra* note 3 at para 52.

[35] Nate Anderson, "Times Square bombing suspect used a 'burner' phone," *Ars Technica* (5 May 2010), online: <arstechnica.com>; Justin Peters, "Can Disposable 'Burner' Cellphones Protect You from Government Surveillance?" (27 June 2013), *Slate: Crime* (blog), online: <www.slate.com/blogs/crime/2013/06/07/verizon_nsa_scandal_can_-disposable_burner_cell_phones_protect_you_from_government.html>.

[36] *Fearon* C.J., *supra* note 4 at para 19.

[37] Savard & McConchie, *supra* note 8; *Fearon*, *supra* note 3 at para 84.

[38] *Fearon* C.J., *supra* note 4 at para 49.

similarly-low-quality cell models lack high-resolution cameras and user-friendly touchscreens and are ill-suited to capture and store intimate photographs and videos. They are less compatible with modern and fully updated social media applications like Twitter, Facebook, Instagram, or even Gmail, all of which are veritable warehouses of intimate personal details. However, these phones might indeed exclusively contain crucial recent communications and (low-resolution) photographs which may—as the *Fearon* test seeks—help protect the police, the accused, or the public, or help to locate additional suspects.

Marking a legal boundary that allows the search of older technology, but not newer, incident to arrest may admittedly be difficult to administer in practice. Barring an exhaustive list of acceptable searchable devices, law enforcement officials would still have to make a judgment call. And, even if a particular phone were included on such a list of accepted phones, there may be reason to conclude that a device might contain more sensitive personal information than usual. Older phones may be improved by connecting external storage devices, making network upgrades, and making internal upgrades to its mechanisms which allow the user to record activity that the phone would not normally record.[39] Despite the difficulty in differentiating between the two, there is merit in the understanding that smartphones and flip phones can be as technologically distinct as flip phones and rotary phones.

(c) No Such Thing as a Pinpointed Smartphone Search

Finally, the language in the *Fearon* test fails to take the nature of smartphone data and police procedure into account, and does not function without a significant section 8 intrusion. The doctrine of exigent circumstances, as defined in the *Criminal Code*, uses the word "imminent" carefully when referring to harm to individuals or evidence.[40] In steps (1) and (2) of the modified test, a search is justifiable if there is a reason—any reason—to conduct a search based on the valid law enforcement objectives listed. Even before reaching steps (3) and (4), it is obvious the police will have no difficulty finding reasons to justify their actions, particularly where step (2)(c) is concerned.[41]

Moreover, there is a logical fallacy: a cursory search to discover evidence cannot be tailored to its purpose, as set out in step (3). Unless law enforcement has been given precise testimony as to where in a device discoverable evidence can be found, an indefinite search through data will have to be made. Even if police received a tip that photographic evidence existed on a phone, its location would be a mystery. Would it be in Instagram, a photo sharing application, or is it a hidden on the SD card? If the evidence is a text message, is it in a common

---

[39] Savard & McConchie, *supra* note 8.

[40] *Criminal Code*, R.S.C. 1985, c. C-46, s. 529.3(2).

[41] *Fearon*, *supra* note 3 at para 83: "[d]iscovering 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."

messaging platform like WhatsApp, or encrypted inside TextSecure? The only way a pinpoint cursory search would purely allow the search of the specific information sought would be if details were available to the police beyond a reasonable margin of error. Otherwise, any search attempt becomes highly invasive, uncovering a great deal of information beyond the scope allotted.[42] This is true even for searches granted by warrants: where exigent circumstances demand urgent action on a lawful arrest, there is no doubt that law enforcement is at a high risk of infringing privacy despite the modified test's attempt to limit that risk.

Furthermore, steps (2) and (3) together allow a near limitless search through the phone. In cases where evidence is discovered after an exhaustive search, it could be retroactively justified if law enforcement can reasonably say it would have stymied the investigation—"stymied" not being a high threshold. The majority has listed several concerns as to why smartphone searches have the potential to be significant intrusions, and in step (3) they effectively give licence to the police to search a phone until they find something with which to incriminate the suspect *and* additional suspects.[43] This is an unacceptable intrusion on section 8 rights, defeating the *Charter*'s purpose, as Justice La Forest expressed best in *R. v. Dyment*:

> [I]f the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. . ..Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated. This is especially true of law enforcement, which involves the freedom of the subject.[44]

IV. DO THESE MISSTEPS RENDER THE TEST INFEASIBLE IN PRACTICE?

(a) Serving Valid Law Enforcement Objectives

Given the *Fearon* test's flaws, how might a cell phone search incident to an arrest operate? The first two conditions of a SITA of a cell phone—that the arrest must have been lawful and that the search must have been truly incidental to that arrest—would yield familiar results, as courts have previously relied on similar requirements.[45]

---

[42] Orin S. Kerr, "Searches and Seizures in a Digital World" (2005) 119:2 Harv L. Rev 531 at 566.

[43] Frank Addario & Andrew Burgess, "If You Don't Care about Privacy, Why Are You Wearing Pants?" (2015) 35:5 For the Defence.

[44] *Dyment*, *supra* note 21 at para 23.

[45] *Quigley*, *supra* note 12.

However, the third law enforcement purpose—discovering evidence in situations where, absent the search, the investigation will be stymied or significantly hampered—is novel, and has already been followed in two recent cases. One Court recently held that searching incoming and outgoing text messages to discover evidence of previous drug selling, the identity of potential buyers, and other information constituted a valid law enforcement purpose under the modified *Fearon* test.[46] A month later, another decision held that a cursory review of recent texts on a cell phone, seized after stopping a car driven by two teenagers suspected of drug dealing, was incidental to a lawful arrest.[47]

Despite, in both cases, there being neither concern for nor discussion of a risk of immediate harm to any person or evidence, the Courts had little difficulty finding that the examinations of those cell phones would recover "relevant information towards the purchase and sale of drugs." Thus, without such an immediate examination, the investigation would have been stymied.[48]

These decisions epitomize the low-threshold of "stymied." If a cell phone present at the scene of a suspected drug deal might contain evidence of drug dealing communications, then it stands to reason that logic would apply to any suspected criminal activity that requires planning or communication to execute. Unlike the prior high-threshold requirement that only urgent circumstances dictate whether a SITA is justifiable, the modified test indicates that the mere premeditated nature of the crime for which an arrest is made will allow a SITA of a cell phone.

(b) Taking Notes

In addition to the problematic supplement to the *Fearon* test's standard list of acceptable law enforcement purposes, two unique conditions—that the nature and the extent of the search are tailored to the purpose of the search, and that the police must take detailed notes—pose practical complications.

The limitations of nature and extent were explained by the majority as meaning that "only recently sent or drafted emails, texts, photos and the call log may be examined."[49] In theory, the limitation has virtue; in practice, it is infeasible. Modern smartphones do not come equipped with filters that can effectively isolate the items listed. In standard Android and Apple text messaging applications, recently *received* texts may be sorted chronologically, but the most recently *sent* text communications are not ordered by default, and will not be instantly discernible to a new handler of the device. Justice Karakatsanis' dissent

---

46 *R. v. Batista*, 2015 BCSC 244, 2015 CarswellBC 412, [2015] B.C.J. No. 294 (B.C. S.C.) at para 133.

47 *R. v. Jones*, 2015 SKPC 29, 2015 CarswellSask 106, [2015] S.J. No. 89 (Sask. Prov. Ct.) at para 55.

48 *Ibid.*

49 *Fearon*, *supra* note 3 at para 76.

articulates this difficulty of performing a "meaningfully constrained targeted or cursory inspection of a cell phone or other personal digital device."[50]

The note-taking requirement, too, is likely to breed confusion. First, there is a matter of accuracy and detail, as note-taking often occurs after the search.[51] Further, in cases where a SITA is necessary under time-sensitive circumstances, such as a risk of harm or destruction of evidence, it is unreasonable to expect perfectly accurate and detailed notes. If the very concept of note-taking is susceptible to inaccuracies due to postponed transcription, what use will they be to either the Crown or plaintiff in litigation or judicial review?

V. WHY THE MAJORITY'S MISSTEPS ENDANGER CANADIANS' FREEDOMS

The modification of a new common law test for smartphone SITAs poses a critical threat to Canadians' freedom, with minimal recognizable offerings of guidance to police investigating criminal activity. And, as Justice Cromwell himself expressed in detail in *Vu*, the potential downsides are numerous, unnecessarily creating wider avenues to wrongful convictions and raising unexpected *Charter* infringements beyond section 8.

There is no debate concerning the need to minimize risk of wrongful convictions. The Supreme Court has recently acknowledged a number of public inquiries highlighting the importance of safeguarding the criminal justice system—and protecting the accused tried under it—from the possibility of wrongful conviction.[52] The *Fearon* test opens a door for the acquisition and admissibility of ambiguous evidence which may be used to impeach a suspect's credibility or even incriminate him. There is a good reason why access to this kind of evidence has to date been afforded protection: the potential to unfairly prejudice the accused in criminal proceedings.

For example, the US case of Gilberto Valle represents a perilous trend toward prosecuting "thought crime." Valle, who fantasized online about killing and eating various women, was found guilty by a jury of conspiracy to commit kidnap—but no real-world, offline steps were taken to kidnap anyone.[53] The jury could not see beyond Valle's repulsive fantastical tastes, holding the belief that he had committed the *actus reus* elements beyond a reasonable doubt.[54] (The verdict was overturned.) This case is highly characteristic of the potential for our private data to portray us unfairly and hinder our freedom of expression, precisely as Justice Cromwell warned in *Vu*.[55] Whether Valle planned to actually eat his wife,

---

[50] *Ibid* at para 164, Karakatsanis J., dissenting.

[51] Quigley, *supra* note 12.

[52] *R. v. Trochym*, 2007 SCC 6, 2007 CarswellOnt 400, 2007 CarswellOnt 401, [2007] 1 S.C.R. 239, [2007] S.C.J. No. 6 (S.C.C.) at para 1.

[53] *U.S. v. Valle*, 301 F.R.D. 53 (S.D.N.Y., 2014).

[54] Kaitlin Ek, "Conspiracy and the Fantasy Defense: The Strange Case of the Cannibal Cop" (2015) 64:5 Duke L.J. 901 at 945.

Americans and Canadians are guaranteed the freedom to think and to express those thoughts regardless of their repugnancy. Section 2(b) of the *Charter* protects us from being held culpable by the state for what is inside our minds, but the *Fearon* test gives law enforcement access to data which may paint an inaccurate picture of our minds.

In addition to infringing on freedom of expression, broader discretion for police to access our phones may also be said to have an inherently infringing effect on our section 7 protection of liberty as a matter of expanding state surveillance. Philosopher Jeremy Bentham's development of the infamous Panopticon prison postulated the theory that people who believe they are being watched will act in a manner vastly more conformist and compliant.[56] The belief that law enforcement may at any time, without reasonable grounds, search through our personal data would cripple any propensity to engage in deviant behaviour regardless of its illegality.[57] Who would input anything questionable into a Google search knowing that it may someday be employed against them as impeaching evidence?

While the collection and permanence of our Internet activity is altogether another matter, the Supreme Court has acknowledged that records of virtual behaviour, recorded unbeknownst to the user, can be accessed via the smartphone hard drive.[58] Combining our online histories with GPS and fingerprint/retina-scanning technology makes smartphones very appealing sources of evidence for law enforcement, but will also serve to render certain legal behavioural choices off-limits.[59] As our electronic devices increasingly act as windows to our innermost personal details, there must be careful limitations to how data is searched, recorded, and exploited in criminal proceedings. Justice Cromwell acknowledged this in *Vu*, stating "[t]he purpose of the prior authorization process is thus to balance the privacy interest of the individual against the interest of the state in investigating criminal activity before the state intrusion occurs."[60]

There are few shortcomings to the existing law enforcement power for searching suspects on arrest. If, as in *Fearon*, officers want to access data on a suspect's phone in a lawful SITA scenario, there are a number of ways they can justifiably do so. The most well established method does not require detailed analysis: there is a lower threshold to seize a device upon lawful arrest when there are reasonable grounds to do so, because there is no heightened privacy

---

55 *Vu*, *supra* note 2 at para 42.

56 Michel Foucault, *Discipline and Punish: The Birth of the Prison*, 2nd ed (New York: Vintage Books, 1995) at 195-228.

57 Neil M. Richards, "The Dangers of Surveillance" (2013) 126:7 Harv L. Rev 1934 at 1948.

58 Chen, *supra* note 30 at 144; *Vu*, *supra* note 2 at para 42.

59 TED, "Why privacy matters" (October 2014), online: < www.ted.com/talks/glenn_-greenwald_why_privacy_matters/transcript?language = en#t-888105 > .

60 *Vu*, *supra* note 2 at para 46 [emphasis omitted].

interest.[61] Following a seizure, a warrant can be obtained allowing lawful access to search the contents. While patience is required, this process serves police objectives to search data fully, if not promptly, for their purposes.

Unquestionably, situations arise where objectives may only be sufficiently met through swiftness. There are two established safeguards providing ample assistance where speed is required:

1. The doctrine of exigent circumstances is cited by both the majority and dissent (the former vaguely explained its flaws while the latter praised its suitability); and
2. The *Waterfield* doctrine has been used sparingly, but effectively, to fill gaps where dire situations have required the police to expand their powers beyond the standard admissible range.

VI. EXISTING LAW ENFORCEMENT POWER

(a) Exigent Circumstances

The doctrine of exigent circumstances is an unambiguous tool law enforcement may use when dire conditions suggest the necessity of a search upon lawful arrest which goes beyond the permissible cursory depth. The *Criminal Code* outlines the powers of police in the circumstances of *Fearon*, and jurisprudence has expanded upon this by acknowledging several bases on which the doctrine may rely.[62]The first concerns imminent loss or destruction of evidence; the second includes a concern for public or police safety. In *R. v. Kelsy*, the Ontario Court of Appeal succinctly explained the need to rely on exigent circumstances, stating:

> [W]hether. . .invoked to search for evidence or to protect the public or for officer safety, it is the nature of the exigent circumstances that makes some less intrusive investigatory procedure insufficient. By their nature, exigent circumstances are extraordinary and should be invoked to justify violation of a person's privacy only where necessary.[63]

Especially in *Fearon*, where a violent crime involving a firearm was committed, the doctrine accordingly afforded the police the capacity to seize a phone if they had reasonable grounds to believe its contents related to the offence committed.

Justice Karakatsanis' dissent stressed the importance of reasonable grounds under exigent circumstances.[64] Without grounds to search a phone, the urgency

---

[61] *Fearon*, *supra* note 3 at para 155, Karakatsanis J., dissenting.

[62] *Criminal Code*, *supra* note 40; Halsbury's Laws of Canada (online), *Criminal Procedure*, "The Search and Seizure Process: Basic Principles: Reasonableness of Search or Seizure: Warrantless Searches" (II.1(4)(b)) at HC2-26 "Validating Factors" (Cum Supp Release 23).

[63] *R. v. Kelsy*, 2011 ONCA 605, 2011 CarswellOnt 9766, [2011] O.J. No. 4159 (Ont. C.A.) at para 35 [*Kelsy*].

necessary to invoke the doctrine is not present. This is a logical limit, as law enforcement agents could otherwise justify any warrantless search by saying "we might have found something of use." It would be trite to say that giving police a groundless power to search unacceptably intrudes on Canadians' privacy rights.[65]

Yet, one can imagine circumstances the majority might have considered when it felt compelled to expand the common law test for smartphone searches. For example: a child is abducted, a suspect is lawfully detained, police have seized the suspect's smartphone on cursory search with an ITO, and the child's location is unknown. One may argue there is no immediate danger to the public or police. If the facts do not display reasonable grounds to suggest the presence of evidence relating to the kidnapping on the phone, nor the imminent danger of the destruction of that evidence, would this situation not demand immediate action? In light of this concern, there is a potential legal solution: the *Waterfield* test.

(b) Waterfield

The *Waterfield* doctrine developed from an English Court of Appeals case which employed a two stage test to determine whether the police had acted within their professional obligations, in order to validate a charge of assault against an officer in the course of executing his duties.[66] The *Waterfield* test was integrated into Canadian jurisprudence, and transformed by the Supreme Court of Canada into an ancillary police powers test that could justify new common law conduct which might otherwise fall outside the spectrum of statute-imposed police conduct, such as exigent circumstances.

The test is a balancing act to determine whether police conduct "(a). . .falls within the general scope of any duty imposed by statute or recognised at common law and (b) whether [it], albeit within the general scope of such a duty, involved an unjustifiable use of powers associated with the duty."[67] For the infringement to be justified, the police action must meet a "reasonably necessary" standard.

Recently, the Supreme Court of Canada recognized limits to *Waterfield* and directed courts to further consider three factors when justifying police powers[68]:

1. The importance of the performance of the duty to the public good[69];

---

64 *Fearon*, *supra* note 3 at paras 175-179, Karakatsanis J., dissenting.

65 Addario & Burgess, *supra* note 40.

66 Richard Jochelson "Ancillary Issues with Oakes: The Development of the Waterfield Test and the Problem of Fundamental Constitutional Theory" (2012-2013) 43:3 Ottawa L. Rev 355.

67 *Kelsy*, *supra* note 63 at para 19; *R. v. Waterfield* (1963), [1963] 3 All E.R. 659, [1964] 1 Q.B. 164 (Eng. C.A.) at p. 661 [All E.R.] [*Waterfield*].

68 *R. v. MacDonald*, 2014 CSC 3, 2014 SCC 3, 2014 CarswellNS 16, 2014 CarswellNS 17, [2014] 1 S.C.R. 37, [2014] S.C.J. No. 3 (S.C.C.) at paras. 33-45 [*MacDonald*].

2. The necessity of the interference with individual liberty for the performance of the duty[70]; and
3. The extent of the interference with individual liberty.[71]

The common law and legislation have both strived to give the police as much power as possible to preserve the peace and administer justice, while carefully acknowledging that law enforcement's power should not be unlimited.[72] Even if the preservation of evidence or the safety of the public or police is not at stake, the *Waterfield* test may justify a search which infringes on privacy rights based on the totality of the circumstances.[73]

The trend of using the test to create common law power is not without controversy. In the first Canadian case to employ *Waterfield*, Chief Justice Dickson's powerful dissent criticized the majority judgement's law-making role and implied that invoking the ancillary powers test was a danger to civil liberties and would erode the rule of law.[74] Yet, in the 30 years since *Dedman*, the Supreme Court has shown itself willing to adopt the doctrine in a handful of cases.

A major complaint from commentators concerns the use of *Waterfield* to sidestep legislation, and in the process extend police power thereby increasing the potential for unjustified law enforcement overreach.[75] This criticism is powerful, and as the Supreme Court might be developing distaste for *Waterfield* in this context, it would be imprudent to advocate for the ancillary powers doctrine as a comprehensive alternative solution.[76] Yet, similar criticism—that deployment of ambiguous judicial guidance may precipitate abuses of power—equally suits the *Fearon* test. Thus, while invoking *Waterfield* to justify a cursory search of a cell phone may not be superior to clear unambiguous legislation defining the scope of police conduct, it would at least be preferable to granting a low-threshold licence for law enforcement to infringe Canadians' privacy on arrest provided they later take detailed notes.

In the above kidnapping hypothetical—presuming the conduct passes the first stage of the *Waterfield* test—the Supreme Court would likely find that a cursory cell phone search of a suspected and lawfully detained kidnapper passes

---

69 *R. v. Mann*, 2004 SCC 52, 2004 CarswellMan 303, 2004 CarswellMan 304, REJB 2004-68801, [2004] 3 S.C.R. 59, [2004] S.C.J. No. 49 (S.C.C.) at para 39 [*Mann*].

70 *R. v. Dedman*, 1985 CarswellOnt 103, 1985 CarswellOnt 942, (*sub nom.* Dedman v. R.) [1985] 2 S.C.R. 2, [1985] S.C.J. No. 45 (S.C.C.) at para 35 [*Dedman*]; *R. v. Clayton*, 2007 SCC 32, 2007 CarswellOnt 4268, 2007 CarswellOnt 4269, [2007] 2 S.C.R. 725, [2007] S.C.J. No. 32 (S.C.C.) at paras. 21, 26, 31 [*Clayton*].

71 *Dedman*, *supra* note 70 at para 35.

72 *Clayton*, *supra* note 70, at paras 26-31.

73 *Mann*, *supra* note 69 at para 34.

74 *Dedman*, *supra* note 70 at paras 22-37.

75 James Stribopoulos, "The Limits of Judicially Created Police Powers: Investigative Detention after *Mann*" (2007) 52:3-4 Crim L.Q. 299.

76 *MacDonald*, *supra* note 68 at paras 33-34.

muster of *MacDonald*'s three considerations. In such a case, a court would not be using the status of the arrestee (e.g., phone ownership) to define the scope of police power to carry out cursory phone searches on arrest. Rather, it would recognize the context and needs of the specific circumstances (e.g., a kidnapping) to justify police conduct which infringes Canadians' section 8 rights.[77] The retroactive approach of *Waterfield* is not ideal, yet it is preferable to the *Fearon* test in terms of minimizing the potential for privacy infringement.

CONCLUSION

Considering the numerous conditions from which an arrest can lead to a tolerable search of smartphone data, cursory searches must endure as a legal safe zone. Protecting smartphones from warrantless SITAs (barring exigent circumstances or reasonable necessity in line with *Waterfield*) accords with common law privacy interest protection. The Supreme Court has spoken at length about profound infringements in SITA scenarios. It has repeatedly agreed that, despite the need for police powers, it is supposed to be difficult for the police to invade one's privacy.

The fear that law enforcement may become powerless to procure valuable evidence to indict criminals whose guilt appears assured is undoubtedly a compelling reason to allow the police to search suspects' cell phones. But to balance vital *Charter* rights with the administration of justice, any changes to the powers of law enforcement demand a careful strategy which is lacking in the majority, but notably present in the dissent.

Two realities are evident in Justice Karakatsanis' dissent. Firstly, despite the majority's attempt in *Fearon* to address alleged deficiencies in the administration of justice process, no deficiency truly exists where law enforcement wishes to search a cell phone.[78] Either there are reasonable grounds to invoke the doctrine of exigent circumstances, or a search is *prima facie* unreasonable. Growing technological concerns simply do not create new legal powers to authorize warrantless searches of the form and content of electronic devices.

Secondly, and more importantly, the majority never raises the point that the privacy rights guaranteed by section 8 are not device-based, but data-based.[79] In *Cole*, the Court expressly stated that "the subject matter of the alleged search is the data, or informational content of the laptop's hard drive, its mirror image, and the Internet files disc—not the devices themselves."[80] As Justice Karakatsanis outlines, a distinction between data and device interests would have helped improve the majority's understanding of the perceived deficiency of the test they have proclaimed. (Alarmingly, the majority only uses the word "data" once, compared to the dissent's seven.)

---

77 *Clayton*, *supra* note 70 at para 26.

78 *Fearon*, *supra* note 3 at para 105, Karakatsanis J., dissenting.

79 *Ibid* at paras 128-134.

80 *Cole*, *supra* note 16 at para 41 [emphasis omitted].

A likelihood of discovering evidence may be too low of a threshold to demand a search of data under exigent circumstances, but that evidence might be destroyed is generally a reasonable basis for seizing a device. As Justice Karakatsanis points out, "[t]he police may usually seize a phone incident to arrest in order to preserve the evidence, but will require a warrant before they can search its contents."[81] If the police can search a phone when urgent circumstances demand it, *or* they can seize it and then seek a search warrant, what does the majority's test accomplish in either improving clarity for law enforcement or protecting our *Charter* privacy interests?

In *Fearon*, the majority should not have granted the police the unprecedented power to search suspects' cell phones as they have done—though they are correct that legislation may be desirable to meet similar apprehensions of deficiencies, in order to improve the functionality of law enforcement. The existing law demands a protection of privacy rights where smartphone data is concerned. The doctrine of exigent circumstances gives law enforcement the power, when needed, to balance privacy interests with the urgent need for security, and protection and/or discovery of evidence, based on reasonable grounds. More protection of evidence exists in the low-threshold reasonable basis test to seize data storage devices.

Future cases adjudicating the search of cell phones, particularly smartphones, should distinguish *R. v. Fearon* for these reasons, and recognize the sensible and thoughtful dissent of Justice Karakatsanis. This would lead to an appropriate balance of *Charter* privacy protection with the valid law enforcement objectives the majority sought (but failed) to guide in *Fearon*.

---

[81] *Fearon*, *supra* note 3 at para 153 [emphasis omitted].