Windows to our Inner Private Lives

Cell Phones, Informational Privacy and the Power to Search Incident to Arrest in Canada

Pierre-Luc Déziel*

Cet article s'intéresse au traitement par les tribunaux canadiens de la problématique relative au pouvoir de fouille d'un téléphone portable d'une personne mise en état d'arrestation. Dans R. c. Fearon, la Cour suprême a décidé que, sous certaines conditions, ces fouilles tombaient dans les limites du pouvoir de common law de fouille accessoire à une arrestation. Dans cet article, nous défendons l'idée selon laquelle la Cour a fait fausse route, et qu'elle aurait dû formuler une règle claire interdisant toute forme de fouille accessoire à une arrestation d'un téléphone cellulaire, à l'exception des cas où il existe des circonstances exceptionnelles qui justifieraient une telle fouille. Notre argument se décline en quatre temps : (1) d'abord, cette règle préviendrait les fouilles abu-sives de téléphone portable (2) ensuite, elle respecterait les meilleures pratiques en matière d'extraction de données et, par conséquent, elle permettrait une meilleure protection des éléments de preuve potentiellement emmagasinés dans l'appareil (3) elle aurait un impact minimal sur le niveau d'efficacité des activités des services de police et (4) finalement, elle permettrait la mise en place d'un équilibre optimal entre les intérêts de l'État et le droit à la vie privée.

The issue of searches of cell phones incident to arrest has been recently addressed by the Supreme Court of Canada. In R. v. Fearon, the Court has decided that, given certain conditions, 'tailored' cursory searches of cell phone seized fell within the limits of the common law power to search in-cident to arrest (SITA). In this article, I argue that the Fearon case represents a missed opportuni-ty to adapt the age old power of SITA to current privacy concerns, and that the Court should have adopted a bright line and technology-specific rule prohibiting warrantless searches of cell phones absent exigent circumstances. My argument rests on four main points : this rule would (1) prevent abusive searches of cell phones, (2) respect the best data extraction practices and, consequently, better protect the integrity of evidence potentially stored in the device, (3) minimally impact on the effectiveness of law enforcement activities and (4) strike the optimal balance between the state's law enforcement interests and the individual's privacy interests.

* Pierre-Luc Déziel is a postdoctoral fellow at the Centre de recherche en droit public. He would like to thank Claire Brisson for her wise and more than helpful comments.

Windows to our Inner Private Lives
Cell Phones, Informational Privacy and the Power to Search Incident to Arrest in Canada

Pierre-Luc Déziel

INTRODUCTION

In the past few years, lower and appellate Canadian courts have been struggling with the scope and limits of the common law power to seize and search cell phones incident to arrest. Earlier decisions on this question have followed the basic framework originally laid out by the Supreme Court of Canada in the early nineties, and have refused to adapt this framework to fit the concerns and issues raised by the advent of new communication technologies. Recent decisions, however, have been more attentive to the particular privacy concerns associated with these technologies, and have adopted a more restrictive view of the common law power to search them incident to arrest. In these decisions, the heightened expectation of privacy that Canadians should have in the contents of their cell phones has created a context where the balance between the State's interest in these searches and the right to privacy of the individual had to be adjusted to better protect the latter.

The issue of cell phones in the context of the power to search incident to arrest (SITA) has been recently grappled with by the Supreme Court of Canada in *R. v. Fearon*.[1] In a 5-3 ruling, the Court decided that "cursory" or "tailored" searches of cell phones fell within the scope of the power to SITA, and, provided a number of conditions, respected the requirements of s. 8 of the *Canadian Charter*. The dissenting justices, echoing the more recent lower court decisions, argued for the need to adopt a bright line rule forbidding cell phone searches except when exigent circumstances would dictate otherwise.

1. *R.* v. *Fearon*, 2014 CSC 77, [2014] 3 S.C.R. 621 [*Fearon*].

In this article, I will argue that *Fearon* was a missed opportunity to adapt the age old power of SITA to current concerns because it failed to recognize the particular privacy interests cell phones should engage and, as a consequence, did not strike a proper balance between the State's and individuals' interests. To this effect, I will also argue that the Court should have adopted a technology-specific rule prohibiting even cursory warrantless searches of cell phones. Police officers should be able to seize a cell phone incident to arrest but, except in exigent circumstances, they should also need to obtain a warrant before searching the device. My arguments rest on several ideas. First, a bright line rule has the merit of being clear, easily applicable and offers the advantage of adequately preventing abusive searches. Second, this technology-specific rule is compatible with the best data extraction practices and would prevent the destruction of evidence potentially stored in the phone. Third, given the recent progress regarding the capacity of police officers to rapidly apply for, obtain and get access to a warrant, the envisioned rule would not be significantly burdensome for the officers, nor would it unreasonably thwart their efforts to apply the law and bring criminals to justice. Lastly, by optimizing the protection afforded to the legitimate privacy interests of the arrestee, the rule strikes an optimal balance between the individual's right to privacy and the State's interests in law enforcement.

The article proceeds in the following fashion. I will start by presenting the basic framework of the power to SITA in Canada. In the second section, I will review and categorize the different answers Canadian lower and appellate courts have given to the problem of the scope and limits of the power to SITA as it relates to cell phones. The third section will provide a review of both the majority and minority reasons in *Fearon*. In the fourth and last section, I will lay out the my arguments in favour of the adoption of a bright line and technology-specific rule prohibiting, absent exigent circumstances, warrantless cursory searches of cell phones incident to arrest.

1. The basic framework of the power to search incident to arrest in Canada

The legal authority behind the power to SITA is derived from the lawfulness of the arrest itself. Since probable and reasonable grounds are already required for the arrest, it is not necessary to meet this standard a second time in order to search the individual being arrested. Therefore, the precondition that the power to SITA has

to meet in order to be considered valid is that the arrest itself was lawful. A search incident to an illegal arrest will also automatically be considered illegal.[2]

In *Cloutier v. Langlois*, the Supreme Court of Canada established that the common law power to search incident to arrest has to be consistent with the values embedded in the *Charter,* and that its scope must be determined in a manner that will strike a proper balance between the State's law enforcement interests and the respect of individual liberties.[3] Three necessary conditions constrict the exercise of the power to SITA. First, the search should not be automatic nor perceived as a duty imposed on the arresting officers. When the search is not necessary to the safe and effective application of the law, it should not be conducted. In other words, the power to SITA is a discretionary one. Second, the search should not be performed in an abusive manner. The degree of coercion used by the officer in conducting the search should be proportionate to the objectives sought by the arresting officers. Third, - and perhaps most importantly - the search must me done "for a valid objective in pursuit of the ends of criminal justice".[4] To qualify as being incidental to an arrest, the search has to contribute to the achievement of the objectives of the criminal justice system.

We can distinguish between two categories of objectives that should be considered valid from a constitutional standpoint and will justify the exercise of the power to SITA. The first relates to the search of the arrestee for security reasons. Police officers will need to be able to search the arrestee and his immediate surroundings to discover any arms or objects that could compromise their safety or that could be used by the arrestee to escape custody. In *Cloutier,* it is mainly because of this security motive that it was decided that a "frisk" search of an agitated arrestee was valid. The Court considered that this brief and minimally intrusive search "reconciles the public's interest in the effective and safe enforcement of the law on the one hand, and on the other its interest in ensuring the freedman dignity of individuals."[5] The second category of valid motives in the context of a SITA is derived from the need for the officer to secure pieces of evidence that could later on be used in the courtroom. The scope of the power in this category is much more problematic than the first one. How far can the police go to collect and secure evidence? As we shall see, the pith of the problem concerning the SITA of cell phones is the extent to which police officers can go in order to secure or discover new evidence.

2. *R.* v. *Stillman*, [1997] 1 S.C.R. 607 at para 27 [*Stillman*].
3. *Cloutier* v. *Langlois*, [1990] 1 S.C.R. 158 at 184–185 [*Cloutier*].
4. *Ibid.* at 186.
5. *Ibid.* at 185.

For a search to fall within the scope of the power to SITA, a search not only has to be incidental, but it also has to be "truly" incidental. This nuance was added by Chief Justice Lamer in *R. v. Caslake,* where he stated that in order to determine if a search is "truly incidental", one needs to take into account *what* the police was looking for and *why*. There are then both subjective and objective components to the determination of the true nature of a search conducted at moment of an arrest.[6] The subjective component relates to the officer's sate of mind and the nature of the beliefs that motivated the decision to proceed to a search. These beliefs are the first things that the Court should review. As Chief Justice Lamer asserts: "[t]his Court cannot characterize a search as being incidental to an arrest when the officer is actually acting for purposes unrelated to the arrest. That is the reason for the subjective element of the test."[7] The objective component aims at making sure that the beliefs that motivated the search were reasonable in the context of the arrest. In other words, the search must be purposeful, motivated by beliefs and intentions that are objectively reasonable and connected to the objective sought by the officer, and grounded in the circumstances that compose the context of the arrest. The application of these objective and subjective criteria is to ensure that searches are not arbitrary, automatic or accidental.

Searches incident to arrest that do not tend toward the accomplishment of a valid law enforcement objective will be characterized as illegal. Moreover, even if a search is truly incidental to an arrest, there are limits to the capacity of police officers to use this power. Two of these limits were enunciated by the Supreme Court in *R. v. Stillman*[8] and *R. v. Golden*[9]. In *Stillman*, it was decided that the power to SITA did not extend to the power to seize samples of bodily substances.[10] In *R. v. Golden*, the Court ruled that strip searches incident to arrest had to be conducted only if the higher standard of reasonable grounds was met.[11] Thus, the reasonable basis standard normally accepted in the context of a SITA search does not apply to strip searches. One of the fundamental points in the SITA debate is whether or not some sort of limit, such as an outright ban or a higher standard, should be put in place when it comes to searches of cell phone contents seized incident to arrest. As we will see in the next section, Canadian courts have come up with very different answers to this question.

6. *R.* v. *Caslake*, [1998] 1 S.C.R. 51 at para 19.
7. *Ibid.* at para 21.
8. *Stillman*, *supra* note 2.
9. *R.* v. *Golden*, [2001] 3 S.C.R. 679 [*Golden*].
10. *Stillman*, *supra* note 2 at para. 49.
11. *Golden*, *supra* note 9 at para 98.

2. Cell phones and searches incident to arrest before *R. v. Fearon*: the continuation and the technology-specific approaches

In this second section, I want to discuss the lower and appellate courts' decisions regarding cell phone searches incident to arrest, that is, before the matter was taken up by the Supreme Court of Canada. I will distinguish between two jurisprudential approaches. The first - which I will refer to as the "traditional approach" - consists of the decisions where the basic SITA framework is considered as directly applicable to cell phones: if the search of the cell phone is truly incidental, then it is valid. The notion that SITA's traditional framework works even in the context of cell phones stems from the fact that these cases do not establish a fundamental difference between a cell phone and any other physical item an officer will find on an arrestee. In most cases, cell phones are in fact compared to handheld digital devices, log books, diaries or agenda and are then treated as such. This view is in and of itself coherent, but it nevertheless fails to recognize the particular and radically unique nature of cell phones.

The second approach, which I labelled the "technology-specific approach", is an aggregate of cases that were decided by taking into account the singularity of cell phones and the particular issues they raise from an informational privacy standpoint. One of the common threads that run through these cases is that new technologies are not the same as logbooks, diaries or notebooks. The digital information they can store or generate does not even begin to compare, in quantity or in nature, to the information that can be physically stored in these containers. Moreover, not only can cell phones store significant amounts of information, they also generate new information of which the user is not even aware. For the technology-specific approach advocate, the heightened and unique privacy interests engaged by these new communication and information technologies legitimate the carving out of a cell phone exception to the basic SITA framework. Here, two sub-trends will emerge. The first and dominant one will recognize that cell phone seizures fall within the power to SITA, as will a cursory search of the device as long as it is conducted to determine if a full search will lead to the discovery of new evidence. A full search of the device will require a warrant. A more radical view is that the arresting officer will be able to seize the cell phone, but that a warrant will be needed even to conduct a cursory search, except if exigent circumstances dictate otherwise.

2.1. The traditional approach

One of the earliest Canadian cases addressing the issue of cell phones and handheld digital devices in the context of the power to SITA is *R. v. Giles*.[12] This case deals with the warrantless search of the accused's BlackBerry, which was seized at the moment of the arrest. The arrest occurred on April 6th, 2005, but the seized device was sent to the RCMP Technological Crime Branch (TCB) almost 7 weeks later, that is, on May 26th 2005. The instruction given to the TCB was to examine the device and "retrieve any data saved on it".[13] The full search of the accused's BlackBerry led to the discovery and extraction of 164 e-mails, 5 address book contacts, and 9 memos.[14] Counsel for the accused argued that, because devices such as the BlackBerry can store important amounts of personal and 'biographical core' information, the police should have sought prior authorization before proceeding with the search. For the Counsel, the common law power to SITA does not extend to a warrantless and complete search of a BlackBerry and that, consequently, the accused's rights under s.8 of the *Charter* were violated.[15] The Court was not convinced by the defence's argument. Justice MacKenzie ruled that since the search of the device was conducted with the objective of extracting possible evidence of the offence for which the accused was arrested, and since there was a reasonable basis to believe that such evidence was on the device, the full search performed by the TCB was truly incidental and therefore fell within the scope of the power to SITA.[16] She thus concluded that there were no s.8 violations.

Justice MacKenzie's reasons were based on the premise that the particular proprieties and capacities of the BlackBerry did not alter the privacy interest of the accused nor, therefore, the balancing process of the State's law enforcement interests and the individual's privacy interest. According to Justice MacKenzie, BlackBerry devices are similar to logbooks, diaries, briefcases, notebooks or similar objects that could be found on an individual during an arrest and for which no warrant would be needed to conduct a full search.[17] Rejecting the idea that the police should have dual authority to search a digital device - the common law power to seize the device plus the warrant to search it -[18], she stated that:

12. *R.* v. *Giles*, 2007 B.C.S.C. 1147, [2007] B.C.J. No. 2918 [*Giles*].
13. *Ibid.* at para 12.
14. *Ibid.* at para 18.
15. *Ibid.* at para 47–48.
16. *Ibid.* at para 55.
17. *Ibid.* at para 56.
18. *Ibid.* at para 65.

> "While I accept that this particular BlackBerry's password protection and the double encryption characteristic mean that there is an objectively reasonable expectation of privacy in the information contained in the BlackBerry, it is not different in nature from what might be disclosed by searching a notebook, a briefcase or a purse found in the same circumstances. The capacity of this BlackBerry to potentially store volumes of information does not, in my view, change the character of the search from being lawful as incident to the arrest, into a search that required a warrant."[19]

The reasoning and analogies used by Justice MacKenzie in *Giles* were followed in a number of cases that refused to recognize a particular and heightened privacy interest in cell phones or digital devices. In *R. v. Otchere-Badu,* for example, the warrantless search of the memory of a cell phone seized during an arrest and the extraction of the call history of the arrestee was considered as incidental to arrest because its goal was to discover evidence of the offence for which the accused was convicted.[20] In *R. v. Howell* , it was decided that the search of electronic data contained in an arrestee's cell phone and the real-time monitoring and exchange of texts messages with the arrestee's contacts were valid actions because they were driven by an objectively reasonable belief that they might lead to the discovery of new evidence.[21] Similarly, in *R. v. Franko*, the search of the content and the extraction of the data found in two BlackBerry devices seized at the time of the arrest were deemed truly incidental and therefore valid searches.[22]

Another case which follows *Giles* but raises a number of new issues is *R. v. Cater*.[23] The facts in this case can be summed up as follows. Subsequent to a judicially authorized wiretap investigation, Cater was arrested on weapon trafficking charges. A cell phone was seized at the time of his processing in booking. The officer who collected the phone did not perform a cursory search and decided to remove the battery of the phone so that no evidence would be compromised or lost. He then proceeded to send the phone to the RCMP Integrated Technological Crime Unit for a full search and forensic analysis of the data that would be found in the device. The call and text message history of the phone was extracted, as well as the images - some of his girlfriend-, the contact information and the metadata associated with them. A.S. Derrick Prov. Ct. J. claimed that even if this type of information attracts

19. *Ibid.* at para. 63.
20. *R.* v. *Otchere-Badu*, 2010 ONSC 1059 at para 82, [2010] O.J. No 901.
21. *R.* v. *Howell*, 2011 NSSC 284 at paras 38–43, [2011] N.S.J. No. 750.
22. *R.* v. *Franko*, 2012 ABQB 282 at para 157, [2012] A.J. No. 475.
23. *R.* v. *Cater*, 2012 NSPC 2 at para 22 [*Cater*].

a reasonable expectation of privacy, she was not prepared to characterize this expectation as elevated.[24] Her reasons were motivated by the particular nature of the device and the fact that it was not password protected. Concerning the password protection issue, the judge claimed that the use of a password illustrates the owner's will to make his or her cell phone more secure and therefore amplifies the expectation of privacy that the device engages.[25] Since Cater's phone was not protected, it follows that the accused could not claim an elevated expectation of privacy *vis-à-vis* the contents of his phone. Second, concerning the nature of the device, it was determined that it was not a 'smart' phone because it had limited functions and did not work as a mini-computer. It was, in Judge Derrick's view, more akin to an unlocked briefcase:

> "Kyle Cater's cell phone was, I find, the technological equivalent of an unlocked briefcase containing correspondence (text messages), an address book, (contact information), and photographs (digital images). The record of incoming and outgoing calls found in a cell phone might be found in a briefcase in the form of hard copies of phone bills."[26]

Because the seizure and subsequent search of a briefcase, an envelope, a notebook or a diary would not have required prior authorization in the form of a warrant, the same logic should apply to basic cell phones.[27] Moreover, according to Judge Derrick, the imposition of a requirement to obtain a search warrant before conducting a full forensic search would require the police to depart from the best practice standard in matters of data extraction. Her argument raises two main ideas and reacts to the 'technology-specific' jurisprudence. As we will see in greater detail later on, this trend authorizes a cursory search of a cell phone to determine if a more in-depth search of the device would lead to the discovery of new evidence. However, the second and more thorough search would require prior authorization. For Judge Derrick., this general rule would produce counter-productive effects: cursory search could lead to the inadvertent or malicious destruction of evidence - inculpatory or exculpatory - contained in the cell phone, thereby undermining the principal evidentiary function of the search.[28]

This destruction of evidence could result from the inadequate manipulation of the device by the arresting officer or the remote deletion of the compromising data

24. *Ibid.* at para 43.
25. *Ibid.* at para 44.
26. *Ibid.* at para 54.
27. *Ibid.* at para 55.
28. *Ibid.* at para 59.

by a third party or a pre-programmed application - sometimes referred to as a "kill signal". According to the best practice standard on which the Court relies in *Cater*, the arresting officer should simply seize the device and remove the battery without even proceeding to a cursory search of the device. The officer should then give the device to a forensic expert who will be able to extract the data without damaging or deleting the evidence.[29] The removal of the battery by the arresting officer would prevent any kill signal from being sent or received, but will also reduce the risk of having new information coming into the device, thereby overwriting some of the information stored in the phone. In this optic, performing a cursory search in order to determine if a more in-depth search of the device would lead to the discovery of new evidence does not make sense. Moreover, the idea that a 'risky' cursory search would not require a warrant, but that a 'safe' forensic search would require one would seems counterproductive. As Judge Derrick puts it:

> "[N]ot following best practices risks compromising the evidence which the police are entitled to search for incident to an arrest. Compromising the evidence would undermine several of the primary purposes that searching incident to arrest is intended to serve. (…) In case what I am saying is not clear, I will try to put it simply: requiring a search warrant to search the contents of a phone like Mr. Cater's could have the effect of police searching for information without the safeguards associated with a forensic analysis. This would risk undermining the purposes for searching incident to arrest -- the protecting of evidence from destruction, preserving and discovering it."[30]

In order to simultaneously follow best practices and minimize the risk that evidence would be destroyed or damaged, only full, truly incidental and warrantless search of devices seized during the arrest should then be conducted. The *Cater* decision therefore radicalizes *Giles* in the sense that, absent exigent circumstances, cursory searches should never be conducted. What remains unclear, or somehow a little contradictory in *Cater*, is that it is a case where the accused cannot claim to have an elevated expectation of privacy because, contrary to *Giles*, the handheld device is not a "smart" phone that can perform computer-like functions. Would the findings in *Cater* apply to cases where smart phones are at play, and therefore where an arrestee can claim an elevated privacy interest? In my opinion, it seems reasonable to suggest that the potentially counterproductive nature of a cursory search would not vary according to the nature of the phone. To the contrary, it seems that these complex and sophisticated smart phones would increase the likelihood of a manipulation error and the remote or automatic deletion of data. Indeed, Judge Derrick

29. *Ibid.* at para 32.

30. *Ibid.* at paras 57–58.

does not seem to distinguish between smart or dumb phone as she says that : " I am amply satisfied that police should not conduct cursory searches of cell phones seized incident to arrest where it is not urgent to do so."[31]

Concerning full forensic smart phone searches, it is not clear whether or not a warrant would be needed. *Cater* deals with an unlocked "dumb" phone which, for the Court, attracts a lower privacy interest that a locked "smart" phone. On the one hand, the judge claims that refraining from conducting a cursory search of the device in order to meet the best practices standard would mean that police would not have new information *from* the phone to bolster the affidavit for a search warrant. To establish probable grounds to search the phone, police would then have to use the same information that authorized the arrest in the first place.[32] It would then simply be an additional, useless and potentially counterproductive burden that could slow down police in their investigation. In other words, the warrant requirement would add a "further layer of authorization" that is not traditionally part of the common law power to SITA. On the other hand, the Judge also states that, in *Cater,* the search led to the discovery of evidence that could have been found by means of a simple, minimally invasive, cursory search, with the exception of the metadata associated with the images.[33] As we will see later on, the cursory search incident to arrest of a handheld digital device was deemed constitutional in most, if not all, cases that can be classified as relating to the technology-specific approach. The idea that the *Cater* search was not too intrusive thus seems to have weighted in the decision that a warrant was not, in this particularly case, mandatory. But the fact that the full search amounted to a cursory search seems to stem from the nature of the cell phone, that is, from its limited storage capacities and computational functionalities. It therefore seems as if, because the *Cater* phone was not a smart phone that works as a mini-computer, that cursory or full searches are, in terms of data extraction, almost equivalent. We are then brought back to the question of whether or not a warrant would have been necessary if the *Cater* phone had been a smart device.

On this subject, one comment of the judge in *Cater* is particularly pertinent. Judge Derrick distinguishes *Cater* from *R. c. Morelli* [34], a case where the particular circumstances had created a context where prior judicial authorization was deemed necessary to protect the accused's s.8 *Charter* right and ensure the respect of his dignity.[35] In *Morelli,* the Supreme Court of Canada had determined that a personal computer attracts a very high privacy interest because "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and

31. *Ibid.* at para 52.
32. *Ibid.* at paras 61–62.
33. *Ibid.* at para 63.
34. *R.* v. *Morelli*, [2010] 1 S.C.R. 253 [*Morelli*].
35. *Cater*, *supra* note 23 at para 65.

seizure of a personal computer."[36] Distancing *Cater* from *Morelli* highlights the fact that the search conducted in the former was limited in scope and did not amount to a particularly intrusive or invasive invasion of the accused's privacy. It also suggests that, had the *Cater* phone been a smart one, it would have been a very different matter. But is it true that the search in *Cater* was not particularly invasive and was as limited as a cursory search? In all deference, I don't believe so. As Derrick Prov. Ct. J. mentions, the *Cater* search did not lead to the discovery of evidence that a cursory search would have revealed, except for the date-stamps and metadata concerning the photographic images. In my opinion, the relevance of this exception should not be underestimated.

Metadata can reveal a wide range of information about an individual, his or her activities, whereabouts, habits, relationships and preferences. By definition, metadata is information about information. A document recently published by the Office of the Privacy Commissioner of Canada states that metadata is "information that is generated as you use technology, and lets you know the who, what, where, when, and how of a variety of activities."[37] This meta-information is often automatically generated by the technology we use and, therefore, without our consent or even our knowledge. Most importantly, because they can reveal particularly sensitive information, metadata are powerful tools that can lead to the identification of someone and the discovery of substantial amounts of knowledge about this person.[38] From the aggregation, compilation and analysis of metadata can emerge very detailed narrative and patterns of lives of individuals and the people they interact with. Ann Cavoukian, former Privacy Commissioner of Ontario and head of the *Privacy by Design* program, recently pointed out that metadata can actually be more revealing than the data to which it is linked.[39] Metadata should then attract an elevated privacy interest. Moreover, because they are found in all types of phones, they blur the distinction between a "dumb" and a "smart" phone in terms of the reasonable expectation of privacy each device should command.

In the past two years, the Supreme Court of Canada has tackled the issue of metadata in the context of informational privacy in *R. v. Vu*[40]. In *Vu*, Cromwell J. argues that cell phones and computers can store information that is automatically generated by devices that can reveal a wide range of biographical information and could have far reaching implications in the context of a criminal investigation.[41]

36. *Morelli*, *supra* note 34 at para 2.
37. Office of the Privacy Commissionner of Canada, *Metadata and Privacy. A Legal and Technical Overview*, (Gatineau: 2014) at 1 [*Metadata and Privacy*].
38. *Ibid.* at 4.
39. Ann Cavoukia, *A Primer on Metadata: Separating Facts from Fiction*, I.P.C. (Toronto: July 2013) at 4–5.
40. *R.* v. *Vu*, [2013] 3 S.C.R. 657 [*Vu*].
41. *Ibid.* at para 42.

Noting that computers and cell phones will also retain information and data about content that the user will have tried to delete, Cromwell concludes that:

> "computers thus compromise the ability of users to control the information that is available about them in two ways: they create information without the users' knowledge and they retain information that users have tried to erase. These features make computers fundamentally different from the receptacles that search and seizure law has had to respond to in the past."[42]

The fact that cell phones and computers tend to diminish the power of the individual to control his or her personal information means that these devices compromise the right to informational privacy. In a number of decisions, the Supreme Court has endorsed the view, developed and popularized by Alan Westin[43], that control over personal information is a necessary condition of privacy. For example, in *R. v. Duarte*, La Forest J. states that the right to privacy "may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself".[44] In *R. v. Mills*, the Court also stated that the "interest in being left alone by the state includes the ability to control the dissemination of confidential information."[45] The automatic generation of metadata and conservation of information stored outside the realm of control of the individual raises novel privacy concerns, concerns that are specific to these technological devices. Theses concerns are calling out for an up-date of the ways and means by which the justice system protects the right to informational privacy of individuals. Cell phone contents and the metadata associated with them created and stored in personal computers and cell phones - dumb or smart - should then attract a very high level or reasonable expectation of privacy.

Let us recall that in *Cater*, the full search of the cell phone seized during the arrest was justified, in part, because it amounted to a cursory search, except for the metadata (date-stamps) linked to the photographic images on the cell. As we have seen, this exception is significant. The capacity of metadata to reveal biographical core information about the individual should not be underestimated, even if they are by nature relatively mundane. The privacy interest attracted by metadata goes well beyond what they reveal on their own. Metadata can be submitted to data-linking processes that will lead to the creation of novel and additional knowledge about the individual. Accordingly, a cell phone search leading to the extraction of metadata cannot be considered cursory and should attract an elevated privacy interest. Since metadata are found in both "smart" and "dumb phones", they blur the distinction established in *Cater* between the two types of devices which leads to the conclusion that the former should attract a higher privacy interest than the latter. Both types

42. *Ibid.* at para 43.
43. Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7.
44. *R.* v. *Duarte*, [1990] 1 S.C.R. 30 at 46.
45. *R.* v. *Mills*, [1999] 3 S.C.R. 668 at para 80.

of devices should attract a high privacy interest. In all the cases where a traditional approach to the issue of search of a cell phone incident to arrest was applied, the failure to take into account cell phone particularities and the novel privacy issues they raise reveals the need for a technology-specific approach. In the next sub-section, I will discuss some of the SITA and cell phone cases which were decided from a technology-specific perspective.

2.2. The technology-specific approach

In the previous section, I have discussed and analyzed cases that correspond to what I have labelled the traditional approach. This jurisprudential trend considered that cell phones were not different from other items that could be found on an arrestee or in his or her immediate surroundings at the time of arrest. Often harbouring comparisons between cell phones and logbooks, agendas or diaries, these decisions indicate a refusal by some justices to adapt and up-date the basic SITA framework to fit the particular privacy issues cell phones and handheld computing devices raise. This underestimation of the threat to informational privacy that cell phones bring about has lead to a failure to strike a proper balance between the state's law enforcement interests and individual privacy interests. By contrast, the technology-specific approach decisions do not fail to recognize the particularity of cell phones and the novel issues they raise from an informational privacy standpoint.

The justices who presided the technology-specific cases were ready to acknowledge that the changing technological landscape has created a context where the rules had to change. They recognized that the digital realm differs in important ways from the physical world and that a new rule, which would be specific to these new communication and computing technologies, was needed. The need to adopt a fresh and technology-specific perspective on matters relating to new technology was explicitly recognized in a number of cases. For instance, Cromwell J. noted in *Vu* that "[t]he privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets"[46] and that the kind of information computer and cell phones can generate and store "has no analogue in the physical world in which other types of receptacles are found."[47] This line of reasoning was followed in most of the cases we can assign to the technology specific approach.

46. *Vu*, *supra* note 40 at para 24.

47. *Ibid.* at para 42.

The rejection of the analogy the traditional approach draws between cell phones and computers, on the one hand, and logbooks, diaries and other physical receptacles on the other is the starting point of a line of thought that leads to the conclusion that a specific rule, which considers the specifics of modern technologies, is needed in the context of SITA. This rule should be constructed in a manner that will highlight the heightened privacy interests that such devices should attract and consequently limit the power to SITA *vis-à-vis* cell phones. As Sharpe J. suggests in *R. v. Manley:*

> "I would observe it is apparent that the traditional rules defining the powers of the police to conduct a search incident to arrest have to be interpreted and applied in a manner that takes into account the facts of modern technology.
>
> (…)

Cell phones and other similar handheld communication devices in common use have the capacity to store vast amounts of highly sensitive personal, private and confidential information - all manner of private voice, text and e-mail communications, detailed personal contact lists, agendas, diaries and personal photographs. An open-ended power to search without a warrant all the stored data in any cell phone found in the possession of any arrested person clearly raises the spectre of a serious and significant invasion of the Charter-protected privacy interests of arrested persons."[48]

The direct analytical consequence to which leads the idea that cell phones are unique and should attract a higher privacy interest than other objects that could be found during an arrest is that the balance of interests between the state and the individual established by the basic framework has to be modified. In order to establish a reasonable balance between the state interest in matters of law enforcement and the individual interest in the protection of his or her right to informational privacy, additional safeguards should be put in place to further protect the arrestee's right and restrain the arresting officers' power. In *R. v. Liew*[49], Boswell J. therefore asserts that the informational content - and he should have added the metadata attached to this content - of cell phones attracts a heighten privacy interest that "tilts back" the balance in favour of a requirement to obtain judicial authorization before searching the phone that was lawfully seized during an arrest.

In most of the technology-specific cases, the bright line rule envisioned thus demands that, except in exigent circumstances, the power to SITA only authorizes a cursory search of the phone that will enable the police to assess if a full search will

48. *R.* v. *Manley*, 2011 ONCA 128 at para 38, [2011] O.J. No. 642 [*Manley*].

49. *R.* v. *Liew*, 2012 ONSC 182 at para 138, [2012] O.J. No. 1365 [*Liew*].

lead to the discovery of evidence. If this is the case, a warrant is required to proceed to a full forensic search of the device. It should be noted that *Liew* radicalizes this position in the sense that even a cursory search should require a warrant. I will come back to this specific case later on. All the other cases in this jurisprudential trend follow the general rule enunciated above.

A technology-specific perspective on the search of cell phones incident to arrest was first applied in *R. v. Polius* [50], a case that rejected and broke away from *Giles*' line of authority and set the table for other decisions that adopted a technology-specific perspective. The facts of this case are as follows. The defendant Polius was arrested for counselling murder. During the arrest, his cell phone was seized and submitted to both cursory and full search without prior judicial authorization. The examination of the content of the phone led to the production of a 15 page report and a 200 page appendix containing screen shots and images of the information extracted from the phone. The documents contained contact lists, calling history, text messages, voice messages, images and videos.[51] The full search of Polius' phone also revealed the number associated with the defendant's cell phone. Pursuant to s. 487.012 of the *Criminal code,* the police sought to obtain a production order for Polius' Virgin Mobile cell phone records.[52] Virgin produced the records, and the information released was used as evidence to prove the defendant's guilt.[53] To decide if the seizure of the cell phone and the searches to which it was submitted were authorized by the power to SITA, Trafford J., who presided the case, had to first determine if the seizure and the searches were truly incidental to arrest in the sense that they were motivated by a reasonable belief that these actions would lead to the discovery or the preservation of evidence. In this case, the reasonable basis threshold was not met and, as a consequence, the seizure and searches of the device could not be characterized as lawful.[54] Because the seizure and the search were not truly incidental to arrest, Trafford J. did not have to address the scope of the power to SITA with regards to cell phones. Nevertheless, he developed a line of thought that was subsequently applied in other cases dealing with these particular issues.

For Trafford J., it falls within the scope of the power to SITA to conduct a cursory search of an item found during an arrest, in order to determine if there is a reasonable basis to believe it is or contains evidence of the crime that motivated the arrest. Any type of search that goes beyond this cursory inspection is not authorized by the power to SITA. In his words: "the evidentiary value of the item must be rea-

50. *R.* v. *Polius*, [2009] O.J. No. 3074, 196 C.R.R. (2d) 288 [*Polius*].
51. *Ibid.* at para 24.
52. *Ibid.* at para 27.
53. *Ibid.* at para 28.
54. *Ibid.* at para 40.

sonably apparent on its face, in the context of all of the information known by the arresting officer." [55] The judge then goes on to compare the cell phone in *Polius* to a locked briefcase that would be seized during a drug arrest. Here, the comparison does not sit on the material or physical similarities between the two objects as in *Giles* or similar cases, but on the standards that have to be met in order to search an item when it is seized during an arrest. If a locked briefcase was seized during a drug operation, the power to SITA would not include the power to search the briefcase's contents. In the presence of a reasonable basis to believe that the briefcase would contain evidence of the drug offence, it could be seized by the arresting officers, but a warrant would be required to seize and search the briefcase's contents. Trafford J. therefore suggests that the "[a] cell phone is the functional equivalent of a locked briefcase in today's technologically sophisticated world".[56]

It is thus clear that in *Polius*, it was suggested that a cell phone could be seized during an arrest, but only if there was a reasonable basis to believe that it would contain evidence of the offence for which the arrest was made. At this point, only a cursory search would be authorized to determine if the item would serve the evidentiary function of the SITA. Any search that would go beyond this cursory search would require prior judicial authorization. In order to justify this last point, the judge goes over the main argument that was made by the Crown and that was directly taken from the *Giles* case: the idea of obtaining a warrant for the full search of the cell phone would add a superficial and burdensome layer of authorization for police because the warrant would in any ways be routinely obtained.[57] For Trafford J., the issue of cell phones in the context of the power to SITA commands prudence. Cell phones can store an important amount of information that will relate to the intimate, private and biographical aspects of a person's life.[58] Moreover, echoing *Vu*[59], the judge recognizes that cell phones and handheld computing device can generate and keep information even when the user has deleted it.[60] Accordingly, they should command a reasonable and elevated expectation of privacy. The best way to protect this heightened privacy interest in the context of s.8 is to demand that police obtain a warrant if they wish to conduct more than a cursory search of the device. As the judge puts it:

> "It is the range of privacy interests that may be implicated by the information on the cell phone that leads me to conclude the values underlying s. 8 of

55. *Ibid.* at para 41.
56. *Ibid.* at para 47.
57. *Ibid.* at para 49; *Giles*, *supra* note 12.
58. *Polius*, *supra* note 50 at para 52.
59. *Vu*, *supra* note 40.
60. *Polius*, *supra* note 40 at para 53.

> the *Charter* are best cared for by limiting the power to SITA and to seize a cell phone to a power to seize it, where there is a reasonable basis to believe it may contain evidence of the crime, for the purpose of preserving its evidentiary value, pending a search of its content under a search warrant."[61]

In *Giles*, MacKenzie J. wondered about the "reasonable, workable, or practical conditions" that could be imposed by a warrant to reduce the over-seizure of information in a cell phone, but failed to recommend any solution.[62] In *Cater*, Derrick Prov. Ct. J. was curious as to how a warrant would safeguard the right to privacy, but was not able to find "an answer favourable to the Defence position".[63] In *Polius*, Trafford J. did come up with practical solutions and workable conditions that would protect the individual right to privacy by reducing over-seizure of information stored in the phone. Warrants should include information such as the name of a capable person who would ensure that the search is conducted in a technologically sound manner and of an officer who is knowledgeable about the given case. It could also be determined *ex parte* what information in the cell phone should and may be seized, so that only evidence specified in the warrant would be seized during its execution. This would ensure that "[t]he legitimate privacy interests of the arrestee would be optimally cared for during any such execution of the warrant."[64] Moreover, the principle of minimization would be respected because information that is not mentioned in the warrant would not be seized.

The reasons in *Polius* were followed, or at least favourably reviewed, in most of the cases that follow the technology-specific jurisprudential approach. In *R. v. Finnikin* [65], Lederer J. ruled that the search of a cell phone incident to an arrest for possession of stolen property and of a firearm was a s. 8 breach. Because the arresting officer did not have any prospect of finding evidence relating to the offence on the cell phone the search was not truly incidental. To this effect, Justice Lederer did not have to rely on *Polius* to determine that the search was not within a police officer's power to SITA. Even with a traditional approach, such a decision could have been reached simply by following *Cloutier* and *Caslake*. Nevertheless, *Polius* was endorsed by Lederer J. when he mentioned that he agreed with Trafford J. on the fact that the power to SITA does not extend to an "unlimited and unrestricted" power to search a cell phone and that "in some, if not all cases" a search warrant should be issued in order for the police to conduct a full search of the device.[66] This requirement of a warrant is, in fact, what mainly distinguishes *Polius* and *Giles*. It is not the idea that the search should be truly incidental, but that there is a difference

61. *Ibid.* at para 57.
62. *Giles*, *supra* note 12 at para. 69.
63. *Cater*, *supra* note 23 at para 63.
64. *Polius*, *supra* note 40 at para 57.
65. *R.* v. *Finnikin*, [2009] O.J. No. 6016.
66. *Ibid.* at para 51.

between a cursory and a full search of a device and that the latter should be done, absent exigent circumstances, only with prior judicial authorization.

The decision in *Polius* was also approved of in *R. v. D'Annunzio,* a case that resembles *Finnikin* in the sense that it was decided on the basis that the search of the accused's cell phone was not truly incidental.[67] To reach the conclusion that the search was a s.8 breach, Blishen J. simply followed *Caslake*. She nevertheless states that, in the case at hand, the arresting officer should have sought a warrant to seize and search the phone. Referring the *Polius*, she stated that:

> "Requiring judicial authorization in the form of a warrant to search and seize information in a cell phone forces police to take time to give serious consideration to what information will likely be discovered and allows a judicial officer to impose terms and conditions so that only information within the scope of the warrant and related to the target offence can be accessed by police." [68]

This last comment adds a layer of argument to the *Polius* decision in the sense that a warrant should be required if police want to conduct a more thorough search of a cell phone seized during an arrest. It is not only a question of asking the issuing judge to impose conditions on how the search should be conducted, or to require probable grounds, but also to force the police to give some serious thought to the question of whether or not a full search is truly necessary or pertinent.

The next case decided by adopting a technology-specific approach I want to discuss is *R. v. Manley*.[69] In this case, the police proceeded to a cursory search of a cell phone found on an arrestee who was charged with robbery with violence. At the moment of the arrest, the police suspected Manley to be in possession of stolen cell phones. With the search, arresting officers where attempting to determine if the cell phone in question was Manley's personal one, or if it was a stolen cell phone. While proceeding with the search, the officer found a photograph of the accused holding a gun. The photograph was produced in evidence during the trial. One of the main questions here is if the cursory search was lawful. The Court decided that it was lawful since it was done in order to determine if the cell phone was stolen, and therefore, if it could be used as evidence. In that sense, the search was legitimate. But, as Sharpe J. warns, if the identification of the device had been possible without the cursory search, for example if the number was inscribed on the exterior of the cell phone, it would have been a different matter, and a cursory search would not have been authorized. Because the cursory search was not truly incidental, *Polius* was not directly applied in *Manley*. Nevertheless, as we have already seen[70], Sharpe J. adheres to the technology- specific perspective and thinks that one has to be pru-

67. *R.* v. *Annunzio*, [2010] O.J. No. 4333, 224 C.R.R. (2d) 221 at para. 21.

68. *Ibid.* at para 26.

69. *Manley*, *supra,* note 48.

70. *Ibid*.

dent when considering the scope of the power to SITA in the digital realm. In *obiter dicta*, he notes that:

> "While I would not apply *Polius* in the particular circumstances of this case, I am far from persuaded that *Polius* was wrongly decided or that it ought to be overruled. (…) If the police have reasonable grounds to believe that the search of a cell phone seized upon arrest would yield evidence of the offence, the prudent course is for them to obtain a warrant authorizing the search." [71]

Even if *Manley* does not directly follow *Polius*, Sharpe J. clearly agrees with its conclusion. As Boswell J. notes in *Liew*, the *Manley* case does not even establish a general rule authorizing cursory search of cell phone incident to arrest. For Boswell J., *Manley* can "readily be seen to turn on its own peculiar set of facts".[72] Since s. 8 of the *Charter* protects the right to informational privacy of the individual who owns the phone and the data contained in it, the arrestee had a reasonable expectation of privacy only if he was the owner of the phone. Because there was a reasonable basis to believe that Manley was not the owner of the phone, the police had to determine to whom the phone belonged and if Manley had a reasonable expectation of privacy in it. In this case, it was therefore justifiable to take a minimally intrusive method to determine ownership of the phone.[73] Even if the search was authorized, given the particular circumstances of this case, it seems reasonable to think that *Manley* is closer to the intent of *Polius* than to the intent in *Giles.*

R. v. Hiscoe[74] is the next technology-specific case I want to examine. Hiscoe was arrested and charged with possession of cocaine for the purpose of trafficking. During the arrest, the police proceeded to a cursory search of the arrestee's phone, read the text messages and re-read them later that same day. A month later, the device was sent to the RCMP Tech Crime Unit and the entire content of the cell phone was downloaded. This kind of procedure is referred to as a 'data dump' and it is on the lawfulness of this latter search that the appeal focused. In his reasons, Oland J. recognizes that the rapidly changing technological landscape and the advent of the digital age have brought about new risks to informational privacy.[75] Because computers and cell phones can store immense quantities of biographical core information, they should attract a heightened expectation of privacy. Consequently, when dealing with such sophisticated devices, the state should proceed with care and work in a manner that will prevent and avoid any violation of s.8 privacy right.[76] Efforts to minimize the scope of the search and target only information that has a

71. *Ibid.* at para. 39.
72. *Liew*, *supra* note 49 at para 140.
73. *Ibid.* at para 140.
74. *R.* v. *Hiscoe*, 2013 NSCA 48, [2013] N.S.J. No. 188.
75. *Ibid*. at para 70.
76. *Ibid.* at para. 76.

reasonable prospect of discovering evidence should be made.[77] Consequently, simply downloading the entire content of the cell phone does not represent a lawful search incident to arrest.

"Data dumping" is a highly invasive form of search and, absent exigent circumstances, should be conducted only when prior judicial authorization has been granted. Otherwise, the practice is a breach of the right to privacy conferred by s.8 of the *Charter*.[78] The findings in *Hiscoe* were discussed in *R. v. Mann*[79], another case dealing with data dump searches conducted without a warrant. In this case, the entire contents of the appellant's two BlackBerry devices were downloaded by the RCMP's Technological Crime Unit. Following *Hiscoe* and breaking further away from *Giles*, Levine J. stated in *Mann* that the particularly invasive nature of these full download searches made them fall outside the scope of what is permissible under the power to SITA. [80] Individual privacy interests in the content of one's phone outweighs the state's interest in law enforcement and a warrantless full search of the device's contents is an unreasonable breach of s.8.[81]

Up to this point, we have seen that the technology-specific approach to SITA will permit cursory and truly incidental searches of a cell phone seized during an arrest. This search is conducted in order to determine if further investigation, that is, a more in-depth search of the device, will lead to the discovery of evidence of the offence for which the individual was arrested. If it is determined that a full search is desirable, and if there are no exigent circumstances, a warrant should be sought. The warrant should include information as to who should conduct the search and how, and specify what type of information should be targeted. The objective pursued in adding this layer of protection is to prevent over-seizure of personal information and, therefore a breach of a s.8 right. This approach is what we could label the mainstream approach to the technology-specific perspective. But there is a more, shall we say, "radical" approach to cell phone searches incidental to arrest. The gist of this particular trend is to prohibit even the cursory search of a cell phone seized during an arrest. Absent exigent circumstances, a warrant should always be needed when an officer wishes to search an arrestee's cell phone. This approach was laid down by Boswell J. in *R. v. Liew*[82]. As we shall see later, the dissenting reasons in *Fearon* were greatly inspired by the arguments presented in *Liew*.

The defendant Liew was arrested by the RCMP for importing cocaine and possession of cocaine for the purpose of trafficking. His cell phone was seized by the arresting officer who conducted a cursory search of the phone and checked the call

77. *Ibid.* at para. 78.
78. *Ibid.* at para 79.
79. *R.* v. *Mann*, 2014 BCCA 231, [2014] B.C.J. No. 1229.
80. *Ibid.* at para 118.
81. *Ibid.* at para 120.
82. *Liew*, *supra* note 49.

history. A second and "fairly extensive search"[83] of the device was later on conducted, without a warrant. Because the Crown agreed that the second and detailed search of the device was unconstitutional, the case concerned only the first and cursory search of Mr. Liew's cell phone. Boswell J. starts his analysis by underscoring the particular capacities of cell phones to store vast amounts of personal and biographical core information, but also to serve as portals to other applications - Facebook, for instance- where even more personal data are stored. Noting their widespread use and ownership, the judge asserted that the chances that individuals arrested by the police will have in their possession a cell phone is strong and, therefore, that the power to SITA in regards to cell phone is an issue of great and emerging importance.[84]

The particular capacities of cell phones and the novel issues they raise in the context of informational privacy changes the way weighting and balancing processes have traditionally been done. Relying on *Manley*, Boswell J. claims that:

> "Historically, to tilt the balance in favour of the state, and to establish the lawfulness of the search, it has been sufficient to demonstrate that the search was truly incidental to a lawful arrest. But the ubiquitous nature of cell phones and their capacity to contain such substantial amounts of sensitive, confidential, personal information creates new and difficult issues to grapple with in the context of this balancing of interests: on the one hand, the state's legitimate interest in detecting and preserving evidence of criminal activity, and on the other, the individual's heightened expectation of privacy in the contents of the cellular phone."[85]

In *Liew*, the Court thus seeks to develop a "more rigorous and modern approach"[86] to the determination of the scope of the power to SITA in regards to cell phones. This novel approach should take into account that the common law power to SITA is already an exception to the rule set out by s. 8 case law according to which searches require prior judicial authorization in order to be constitutional, and that this exception was carved out in order to meet specific objectives: the security and evidentiary functions of SITA we discussed above.[87] For Boswell J., the evidentiary function can be cared for by simply seizing the phone if there is a reasonable basis to believe that it may contain evidence of the offence at hand. But, because of the elevated privacy interest the data stored in the phone attracts, striking the proper balance between the individual's privacy interest and the state's law enforcement

83. *Ibid.* at para 26.
84. *Ibid.* at para 102.
85. *Ibid.* at para 125.
86. *Ibid.* at para 126.
87. See at 3–4, above.

interest means that a warrant should be obtained even if police want to conduct a brief cursory search of the device.[88]

The notion that a warrant should be required even for cursory search is where *Liew* from the approach suggested in *Polius*. Boswell J. gives two reasons as to why he is not comfortable with the idea that a cursory search of the device is permitted if there is a reasonable basis to believe that it will lead to discovery of evidence. First, cursory searches would be possible on the basis of the standard of reasonable prospect, a low threshold. For Boswell J., in the particular circumstances of a case, police should be able to form the reasonable basis to determine if the cell phone's contents will provide evidence of the offence at stake *without* looking at it. Authorizing cursory searches to determine if the content is relevant puts in place a system that allows an after-the-fact justification of cursory searches that will permit "an unlimited number of unjustified encroachments" on privacy. As Boswell J. puts it: [a]n encroachment on privacy cannot be used to justify itself."[89] The second reason for which the judge wants to discard the idea of authorizing cursory searches of cell phone incident to arrest is because 'cursory search' is a concept that implies a notion of scope that does not easily lend itself to a precise definition. Arresting officers need to follow a precise guideline of clear judicial rules that will ensure that they do not transgress the arrestee's right to privacy and compromise the admissibility of evidence. Even if the *Charter* has to be interpreted in a contextual and purposeful fashion, the police should rely in this matter on an "elegant rule" that is both "simple and with few adjustable factors."[90]

Interestingly enough, Boswell J. relies on *Cater* to build this elegant rule.[91] Recall that in this particular case, which belongs to the 'traditional approach' we have discussed earlier, Cromwell J. ruled that cursory searches of cell phones incident to arrest should not be conducted because they can potentially compromise or destroy the evidence they could store. In order to follow the best practices, the arresting officer should seize the cell phone and bring it back to a competent technician or expert who will be able to extract the phone's contents without jeopardizing its evidentiary value. But, in *Cater*, this second extensive search does not require a warrant. Even if it not for the same reasons, Boswell J. agrees with Cromwell J. on the conclusion that no cursory searches of cell phones incident to arrest should be conducted. The bright line, elegant and simple rule envisioned by Boswell J. in *Liew* is thus that, absent exigent circumstances, arresting officers can only incidentally seize the cell phone and, based on the circumstances of the case, must obtain a warrant to conduct any search of the phone's content. This applies to any phone - dumb or smart - and to any form of search - cursory or full. In other words, absent exigent circum-

88. *Liew*, *supra* note 49 at para 130.

89. *Ibid.* at para 137.

90. *Ibid*.

91. *Ibid.* at para 141.

stances, reasonable and probable grounds are necessary if the police want to look at the content of an arrestee's cell phone or handheld calling device.

Before addressing the Supreme Court of Canada's stance on SITA and cell phones in the *Fearon* case, I just want to sum-up what has been said in this second section. I have identified two general trends in Canadian case law that have a very different approach in defining the scope of the SITA common law power *vis-à-vis* cell phones and handheld digital devices. The first approach, the traditional one, comprises cases where the courts have refused to consider the specificity of cell phones and have treated them like any other object that can be found on a person during an arrest. As long as the search is truly incidental, that is, that there is a reasonable belief that the search will lead to the discovery or the preservation of evidence, cursory and full searches of cell phones are permitted and do not need prior judicial authorization. The notable exception to this trend is the *Cater* case, where the Court claimed that cursory searches should not be conducted. But not because these searches would represent an infringement of a s.8 right, but because they could lead to the destruction of evidence. In the *Cater* case, full and warrantless searches are advised because they would be conducted by competent and expert hands that would not jeopardize the evidentiary value of the content of the cell phone.

The second approach, which, inspired by Orin Kerr[92] I labelled the "technology-specific approach", recognizes the singularity of cell phones and the novel risks and issues they raise in the context of informational privacy law. Because they can store and create radically novel amounts of personal and biographical core data, cell phones should not be treated as any other object. They are not diaries, briefcases or logbooks. The privacy interests they attract modify the previously established balance between individual privacy interest and the state's interest in law enforcement. Additional layers of protection should then be given to the privacy side of the equation in order to strike a proper balance. The cases of this second category therefore advocate the need for police to obtain prior judicial authorization in the form of a warrant before conducting a full search of cell phone seized incident to arrest. Warrantless cursory searches are permitted, but only if they are truly incidental to the arrest and conducted in order to determine if a full and detailed search of the phone's content would fulfill the evidentiary function of the power to SITA. The exceptional and more radical case in this trend is *Liew*, where the Court decided that even cursory searches should require a warrant.

92. Orin S. Kerr, "Foreword: Accounting for Technological Change" (2013) 36 Harv. J.L. & Pub. Pol'y 403.

3. *R. v. Fearon* : the Supreme Court of Canada, cell phones & the power to SITA

In this third section, I want to provide a descriptive account of the reasons of both the majority and dissenting opinions in *R. v. Fearon*. In the next section, I will take a normative stand and provide a critical review of the Supreme Court of Canada's arguments in this case. The *Fearon* case was the first opportunity the Court had to address the issue of cell phone searches incident to arrest. Fearon and an accomplice were arrested for robbery with a firearm and other related offences. During the arrest, one of the arresting officers conducted a pat-down search of Fearon and found a cell phone. The cell phone was searched at that time and later on during the day. On the phone, police discovered an unsent message saying "We did it" as well as some photos of a handgun. A search of the appellant's vehicle, conducted with a warrant, lead to the discovery of the same firearm that appeared in the photo and that, as it was later on found out, was used in the robbery. During the trial, Fearon sought the exclusion of the evidence that is the photo of the handgun because, he argued, the search of the content of his cell phone had violated his privacy right under s.8 of the *Charter.* The presiding judge did not exclude the evidence and decided that the search was conducted incidental to arrest. Fearon was convicted and appealed the decision, but the Ontario Court of Appeal unanimously dismissed it. The Supreme Court was thus faced with the question as to whether or not the search was truly incidental to arrest and if the framework governing the common law power to SITA had to be modified in regard to cell phone. Cromwell J. decided that some minor modifications of framework were in order, and, given these modifications, found that the search in question was not lawful. He decided not to exclude the evidence pursuant to s.24(2) of the *Charter*.

3.1. Reasons for judgment

Writing for the majority in a 5-3 decision, Cromwell J. started off by reviewing the basic SITA legal framework as set out by the Court in *Cloutier* and *Caslake*. He concluded that, from this particular standpoint, the search was truly incidental because it was conducted to achieve valid law enforcement objectives and was motivated by a reasonable belief that some evidence of the robbery could be found in the contents of the cell phone. But Cromwell J. suspended this conclusion pending the assessment of whether or not this basic framework had to be modified to

best fit the particular issues cell phones raise.[93] He thus proceeded to examine the interest of both the State and the individual regarding cell phones in the context of SITA. The judge first determined that searches incident to arrest of cell phones serve important law enforcement objectives because cell phones can be used to facilitate criminal activity. These objectives include the discovery and preservation of evidence, as well as public security objectives. On the latter point, the judge notes that a cell phone can be used to resist law enforcement and facilitate escape.[94] Second, at the individual level, he acknowledged that the content of a cell phone attracts a significant privacy interest[95] and that, "[i]t is unrealistic to equate a cell phone with a briefcase or document found in someone's possession at the time of arrest."[96] Moreover, all types and configurations of phones - smart or dumb, password protected or not - engage the same level of elevated privacy interest.[97] Cromwell J. then asserts 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."[98] The key word, here, is potential: not all cell phone search will lead to significant intrusion in the individual's private sphere. Some will, some might not. Contrary to strip searches, for example, cell phone searches will not *inevitably* lead to a significant invasion of privacy.[99] Cell phones should therefore attract an elevated and unique privacy interest and the SITA framework should be modified to take into account this fact. But cell phone searches incident to arrest are important, and they may not always lead to a significant invasion of privacy. The latter is especially true if the right guidelines are put in place, guidelines that the judge later on develops. Categorical prohibition of cell phone searches incident to arrest are therefore not appropriate measures to deal with the issues they raise.[100] Cromwell J. is also not convinced by the idea of raising the standard for these searches to probable grounds. Police officers will rarely have reasonable and probable grounds to obtain a warrant and, even if they did, this additional step will create delays that will prevent them from acting promptly. This would also compromise police and public safety.[101] This second option thus has to be discarded. The third option reviewed by the judge is the one suggested by Boswell J. in *Liew* : only in exigent circumstances will the police be authorized to conduct any type of cell phone search incident to arrest. For Cromwell J. this approach does not strike a proper balance between the individual and the state's interest because it gives almost no weight to the law enforcement objectives served by the ability

93. *Fearon*, *supra* note 1 at para 43.
94. *Ibid.* at para 48.
95. *Ibid.* at para 53.
96. *Ibid.* at para 51.
97. *Ibid.* at paras 52–53.
98. *Ibid.* at para 58.
99. *Ibid.* at para 54.
100. *Ibid.* at paras 63–64.
101. *Ibid.* at paras 66–67.

to promptly search a cell phone incidental to a lawful arrest."[102] This third option should then also be tossed out.

According to the judge, the task at hand is to find a way to modify the common law power to SITA in a fashion that will reduce the chances that the search will lead to a significant invasion of privacy. Cromwell J. lays down three modifications. First, the extent and the nature of the search must be "tailored" to the purpose it seeks to fulfill.[103] In other words, there must be a reasonable connection between what the police are looking for and the offence they are investigating. If it is a recent robbery, for example, the officers will be able to look a recent texts, phone calls or photographs. But they can not go through all the content of the phone. They must always be able to justify the search by explaining what they were looking for and why. Following *Hiscoe* and *Mann*, which we discussed above, the judge claims that full downloads or data dumping of the entire contents of the phone will rarely be permitted.[104] Only limited searches will thus be considered as falling within the lawful boundaries of the power to SITA. The second modification proposed by Cromwell is that cell phone searches that are conducted in order to discover evidence will be justified only if not promptly conducting them would seriously impede the progress of the investigation. It is not because the officers are looking for evidence that the search will be routinely considered lawful. There should always be a rational explanation as to why it was not "practical" to delay the search.[105] The third and final modification put forward is that officers must take detailed notes of how and why the search was conducted. These notes will include when the search took place, how long it lasted, to what extent it went and what were the applications looked at by the officers. Because there are no prior authorizations required, this procedure ensures the feasibility of an after-the-fact judicial review of police action.[106]

In applying these three criteria to the facts in the *Fearon* case, Cromwell J. found that the lack of details regarding how, when and to what extent the search of the accused's phone was carried out makes it impossible to conduct a meaningful judicial review of the legality of the search. As a consequence, he concluded that the search was abusive and infringed the accused's s.8 *Charter* rights, but that the evidence should not be excluded.[107]

102. *Ibid.* at para 70.
103. *Ibid.* at para 76.
104. *Ibid.* at para 78.
105. *Ibid.* at para 80.
106. *Ibid.* at para 82.
107. *Ibid.* at paras 88–98.

3.2. The dissenting reasons

From the first paragraph of their reasons, the dissenting judges commit to a technology-specific perspective. Writing for them, Karakatsanis J., highlights how cell phones, because they can store extraordinary quantities of biographical core data, are "windows to our inner private lives".[108] Because technology evolves, our laws have to adapt and change. Cell phones represent unique threats to privacy that command similarly unique legal protection. Because privacy is essential to a thriving democracy and to individual freedom, the power of the state to pry upon its citizens should be carefully circumscribed. For Karakatsanis J., then, the common law power to SITA should not extent to cell phones and private digital devices found on an arrestee.[109] Echoing Boswell J.'s argument in *Liew*[110], the judge claims that, in order to prevent unjustifiable violations of the individual's right to privacy, a "clear, practical and effective" legal protection ought to be put in place. This protection is that, absent exigent circumstances, police must obtain a warrant before conducting any type of search of the cell phones or other digital devices found on the arrestee.

As in all the cases associated with the technology-specific approach, the idea behind this claim is that the advent of cell phones has altered the previously established balance between the state and the individual's interest. For the dissenting justices, cell phones and other private digital devices engage a privacy interest that is "quantitatively and qualitatively different from that in other physical items traditionally subject to such searches".[111] From this radical difference stems a need to proceed to a new balancing exercise. Relying on previous Supreme Court cases such as *Vu*[112], Karakatsanis J., describes how cell phones can store, generate and retain amounts of information that cannot be matched by any other physical container.[113] Because most of these pieces of data can, alone or in combination with others, reveal highly personal aspects of our private lives, cell phones should attract a "significant and unique"[114] but also "extremely high" privacy interest.[115]As a consequence, striking the proper balance will require additional protection to the individual privacy interest.

108. *Ibid.* at para 101.
109. *Ibid.* at para 104.
110. *Supra* note 49.
111. *Fearon*, *supra* note 1 at para 125.
112. *Vu*, *supra* note 40.
113. *Fearon*, *supra* note 1 at paras 128–130.
114. *Ibid.* at para 132.
115. *Ibid.* at para 134.

The state's interest in law enforcement also carries significant weight. But, and this is the crucial point that distinguishes the dissenting opinion from the majority's, the main objectives of SITA can be attained *without* infringing on the individual right to privacy and despite the additional layer of protection it should be subject to. Let us consider the two main functions of SITA: the security function and the evidentiary function. The security of the public and of the arresting officers is important. On the one hand, contrary to briefcases or other containers, cell phones cannot be used to conceal weapons or dangerous objects. On the other hand, they can be used to call for violent backup. If the officers have a reasonable suspicion that the cell phone will be used for such an attack, then these are exigent circumstances that will justify the warrantless search of the device. The mere possibility that cell phones could be used to coordinate such attacks does not justify a warrantless search.

The second function served by SITA is the evidentiary one, that is, the preservation and the discovery of evidence. The biggest issue concerning the destruction of evidence is the possibility that a "kill signal" would be remotely sent to wipe out the contents of the phone. If there are reasonable grounds to believe such signals will be sent, these would be exigent circumstances where a warrantless search of the device would be considered lawful. But the mere possibility that such a signal will be sent should not justify a warrantless search of the device. Moreover, some technological and practical solutions exist that more than significantly minimize the risk that the contents of the phone leading to the destruction of evidence can be sent. For example, and we will come back to this point in the next section, officers can place the device in a "faraday bag", which isolates the phone and blocks the signals from and to the phone, making it almost impossible for the kill signal to reach the device. In the case of the discovery of evidence, the dissenting justices acknowledge the fact that delays caused by the necessity to obtain a warrant will thwart the capacity of the police to access evidence whose value will decrease with time : contact information of possible accomplices or witnesses for example. There is, in other words, a certain need to follow the trail while it is fresh. At the same time, cell phones are a "virtual gold mine of information" and the reasons that make it so attractive for the police to be able to excavate that mine are the same reasons that explain why a cell phone attracts such a high and unique privacy interest. Moreover, here again, modern technologies can be used to reduce the delay between the application and the granting of the warrant. Karakatsanis J. gives the example of Telewarrant, which makes it possible, on a 24 hour a day basis, to quickly apply for a warrant.[116]

Considering the fact that modern technologies can provide practical solutions to some of the issues raised by the need for police to acquire prior authorization and that individuals enjoy a heightened privacy interest in the contents of their cell

116. *Ibid.* at para 147.

phones, the dissenting justices found that, except in exigent circumstances, the privacy interest of the individual outweighs the law enforcement interest in conducting warrantless searches of cell phones seized incident to arrest. Consequently, officers will be authorized to seize cell phones found during an arrest, but will have to obtain a warrant if they want to search the contents of the device.[117] This approach is, for the dissenting judges, the only one that makes it possible to protect the individual right to privacy and provide clear and practical guidelines to the police in matters relating to SITA and cell phones. It is flawed not only because it does not provide straightforward and unambiguous rules to the officers, but also because, by asking the arresting officers to 'tailor' the search, we put the balancing decision in their hands. As Karakatsanis J. suggests, these officers are not in the best position to decide if the privacy interest of the individual is clearly outweighed by their need to conduct the search.[118] Moreover, in cases where the officer would have been wrong to conduct the search, the after-the-fact type of justice envisioned by Cromwell J. would not make the search harmless. Even if the evidence it has yielded is excluded at trial, the arrestee's sense of dignity, security and freedom will still have been violated. Along the same lines, putting the balancing process in the hands of the police would nurture uncertainty and public mistrust towards the police. Alternatively, the requirement to seek a warrant would "give people confidence that their privacy will be respected."[119] Exigent circumstances would exceptionally allow the arresting officers to conduct a warrantless search. This exception makes it possible to protect evidence and public safety in cases where, for example, a violent backup was called for by the arrestee or a kill signal sent by an accomplice to wipe out the contents of the phone.

4. Discussion: why the majority was wrong and the dissent was right

In this fourth and final section, I explain why I think the Supreme Court of Canada was wrong not to adopt a bright line and technology-specific rule authorizing the seizure of cell phones incident to arrest, but prohibiting, absent exigent circumstances, warrantless cursory and full searches of the device. I will present four main arguments. First, this rule will have the merit of preventing unlawful searches and protecting human dignity. Second, the rule is compatible with the best practices in terms of data extraction and will prevent the inadvertent destruction of evidence.

117. *Ibid.* at para 153.

118. *Ibid.* at para 172.

119. *Ibid.* at para 169.

Third, it would not have a significant impact on the capacity of police services to attain their law enforcement objectives. Forth, it would strike an optimal balance between the individual's privacy interests and the State's interests in conducting searches incident to arrest.

4.1. Preventing abusive cell phone searches

From a privacy standpoint, the common law power of search incident to arrest is particularly daunting. Because these searches are conducted without warrants nor probable grounds, - two operating pillar of s.8 of the *Charter* jurisprudence - chances that individual privacy rights may be unreasonably infringed upon are evident. When an individual is said to enjoy a subjectively and objectively reasonable expectation of privacy in relation to a particular subject matter, the onus falls on the Crown to demonstrate that the privacy interest of the individual is outweighed by the law enforcement objectives it seeks to pursue by intruding in his or her private life. Since one of the principal goals of s.8 is to *prevent* unjustified state intrusions, the demonstration of the reasonableness of the state's course of action has to be done *before* it embarks on it. The Court has emphasized this point on numerous occasions. Normally, this is done by demanding prior authorization and applying for a warrant. Accordingly, the Supreme Court stated in *Hunter v. Southam* that warrantless searches are *prima facie* considered abusive and therefore unconstitutional.[120]

When it has been proven that a search was conducted without a warrant, it is the Crown's responsibility to show that, on a balance of probabilities, the search can still be qualified as a reasonable one.[121] The power to SITA is one of these particular instances where warrantless searches can be conducted. But even in these cases where the state's law enforcement objective outweighs the individual's privacy interest, the concern for preventing abuse should not be abandoned. Preventing abuses in these cases means that clear rules have to be in place in order to ensure that the infringement on the individual's right to privacy respects certain conditions and criteria. To this effect, La Forest J. states in *R. v. Dyment* that:

> "If the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. This is inherent in the notion of being secure against unreasonable searches and seizures. Invasions of privacy must be prevented, and where privacy is outweighed by other

120. *Hunter* v. *Southam*, [1984] 2 S.C.R. 145 at 161.

121. *Caslake*, *supra* note 6 at para 11.

> 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."[122]

It should also be noted that the importance of preventing s.8 abuses with clear rules is greater in contexts where the incidence the warrantless searches takes a particularly intrusive form. For example, in *Golden*, the Court stated that preventing abusive searches is more critical in the context of strip searches than in the context of less intrusive physical searches such as frisk searches.[123] The Court's reasoning on this point was based on the fact that strip searches are inherently prejudicial to human dignity and represent a "very direct interference with personal privacy".[124] Without suggesting that cell phone searches are as humiliating or intrusive as strip searches, would it be reasonable to say that they can be harmful to human dignity and represent a very direct interference with informational privacy? If so, how would this impact the need to demand that officers obtain prior authorization before conducting such searches?

The question of whether or not cell phone searches constituted an affront to human dignity received divergent answers in the jurisprudence. In my opinion, the underlying issue is the mere possibility to conclude that there can be such a thing as an affront to human dignity in the context of informational privacy. It is easy to imagine why and how a physical search or a bodily seizure or a strip search can be humiliating and degrading to human dignity, but it may be harder in the context of informational privacy. To this effect, Cromwell J., writing for the majority in *Fearon*, stated that:

> "a cell phone search is completely different from the seizure of bodily samples in *Stillman* and the strip search in *Golden*. Such searches are *invariably* and *inherently* very great invasions of privacy and are, in addition, a significant affront to human dignity. That cannot be said of cell phone searches incident to arrest."[125]

Along the same lines, in *Giles*, MacKenzie J. claimed that the full search of the contents of the accused's Blackberry did not constitute an affront to personal dignity "because it was not invasive as is the taking of bodily samples." [126] It is true that

122. *R.* v. *Dyment*, [1988] 2 S.C.R. 417 at para 23 [I highlighted 'clear rules'].
123. *Golden*, *supra* note 9 at para 89.
124. *Ibid.*
125. *Fearon*, *supra* note 1 at para 55.
126. See *Giles*, *supra* note 12 at paras 66 & 68.

searches in the informational context will not be intrusive or humiliating in the same sense that they are in the personal or physical context. But it does not follow that searches in the informational context cannot represent highly intrusive and humiliating practices. One does not have to go far in order to find Supreme Court precedent a precedent linking dignity and human privacy. In *R. v. Plant*, the Court stated that:

> "[i]n fostering the underlying values of dignity, integrity and autonomy, it is fitting that s.8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[127]

Individuals have a right to keep their private information private. Even if somebody has done nothing wrong and has, as the common adage goes, nothing to hide, he or she has can have an interest to conceal from others details about his or her life that are highly private. People store in their phones pictures they take when they are with their close ones, they can take notes about their thoughts, their feelings, their opinions. Some people, if not most, will find it humiliating to have their private and intimate life exposed to another person or see a police officer browsing through the contents of their phone. It is true that the procedure established in *Fearon* does not give an officer the right to look at will into the phone. The search, as Cromwell J. puts it, has to be tailored to the purpose of the search and the offence for which the individual was arrested. But I find it hard to imagine how this officer will know exactly what he or she is looking for and where he or she will find it. The idea that the search would be tailored implied a certain amount of existing knowledge about the phone itself. It seems to me that the risk that the officer will go beyond the limits of a perfectly tailored search is more than significant.

In my opinion, cell phones generate and store important quantities of information of biographical nature and it is hard to imagine, in the informational privacy context, a more intrusive search than a cell phone or a personal computer search. As Karakatsanis J. claims in *Fearon*, such devices are "windows to our inner private lives".[128] In that sense, one can not be surprise to find that Karakatsanis J. will also state that:

> " The fact that a cell phone may keep and access meticulously taken records about almost every aspect of a person's life explains both why searching it

127. *R.* v. *Plant*, [1993] 3 S.C.R. 281 at 292.

128. *Fearon*, *supra* note 1 at para 101.

would be so useful to law enforcement and why such a search may be so offensive to the person's dignity."[129] (my emphasis)

Because cell phone searches are highly intrusive and can be very harmful to human dignity, it is of critical importance to prevent their abusive practice and not simply reacting to it. The procedure established by the majority in *Fearon* does not do that. To the contrary, it proposes a vague and difficult to apply test by which the arresting officer, and not independent justices, must determine if his or her interest in searching the phone outweighs the arrestee's privacy interests. The procedure in *Fearon* relies on an after-the-fact type of justice that is not sufficient considering the highly invasive nature of the search it would correct. Moreover, as the La Forest J.'s claim in *Dyment* presented above suggests, s.8 of the *Charter* should nourish the feeling of the public that it are protected from abusive searches. In other words, the type of justice envisioned by the majority in *Fearon* will undermine the public's trust in the law enforcement institution and foster a feeling of insecurity. On the other hand, the clear guidelines and rules presented in *Liew* and endorsed by the dissenting justices in *Fearon* have the advantages of preventing abuses, protecting personal dignity and nourishing public confidence in law enforcement institutions.

4.2. Adhering to best practices and protecting the integrity of evidence

One of the main points the majority fails to address in *Fearon* is the fact that the best way to protect the integrity of evidence found in the cell phone is to remove the battery immediately after the seizure and to hand over the device to a technological expert in data extraction. As it has been pointed out in *Cater*[130] and in *Liew*[131], conducting cursory searches increases the risk of damaging or destroying evidence stored in the phone. Two main reasons explain this fact. First, in order to conduct the search, the officer has to keep the cell phone 'on' and 'powered'. Remote or automatic kill signals that would wipe the contents of the phone can be sent in motion. Second, errors made by the arresting officer handling the phone can result in the involuntary destruction of evidence. The *Liew* case provides a clear example of the risks associated with this second reason. The arrestee's phone was configured in the Chinese language and the arresting officer thus did not know how to navigate it. He nevertheless started guessing and pushing buttons for five to seven minutes

129. *Ibid.* at para 145.

130. *See Cater*, *supra* note 23.

131. *See Liew*, *supra* note 49.

and than became nervous that he could delete pertinent information by pushing the wrong button.

As described in *Cater*, the best practice in matters of cell phone data extraction is for the arresting officer to take the power supply of the phone, remove the battery and take the device to a data extraction expert.[132] Because it allows cursory cell phone searches by the arresting officer, the procedure set out in *Fearon* is not compatible with the best practice standard in matters of data extraction. It therefore does not adequately prevent the destruction or the damaging of inculpatory or exculpatory evidence. Since the discovery and preservation of evidence is one of the main law enforcement objectives the power to SITA seeks to achieve, the *Fearon* procedure seems counterproductive. In contrast, the bright line and technology-specific rule set out in *Liew* and in the dissenting opinion in *Fearon* would provide an adequate risk management framework for the preservation of evidence stored in cell phones seized incident to arrest. By prohibiting such cursory searches, except in exigent circumstances, the Court would have been consistent with the best practices in matters of data extraction and would have put in place a framework that minimizes the risks that evidence stored in the phone would be damaged or destroyed before it made it the to courtroom.

4.3. Impact on law enforcement activities

In *Fearon*, Cromwell J. stated that requiring police officers to obtain a warrant to search the content of a cell phone seized incident to arrest would significantly reduce the capacity of law enforcement services to effectively pursue their objectives. Demanding that police officers obtain prior authorization would lead to delays that could jeopardize the investigations. In all deference, I do not agree with this statement. First, as mentioned in the previous point, requiring prior authorization and prohibiting warrantless cursory searches would best manage the risk that evidence would be destroyed or damaged, thereby increasing the efficiency of the evidentiary function of the power to SITA. Second, as Karakatsanis J. points out in the *Fearon* dissenting reasons, modern technologies provide practical solutions to the delays caused by the prior authorization requirement. In cases where there are no exigent circumstances, but exists a need for the police to act quickly, the police could rapidly obtain warrant authorizing a cell phone seized incident to arrest through the Telewarrant system.[133]

132. See *supra*, note 29.

133. *Fearon*, *supra* note 1 at paras 138 & 147.

Telewarrants are warrants obtained by submitting an application by telephone or other means of communication, that is, without appearing in person. Under s. 487.1(1) of the *Criminal code*, a police officer can apply for a telewarrant where an "indictable offence has been committed and that it would be impracticable to appear personally before a justice to make application for a warrant".[134] The notion of impracticability is therefore here crucial. What qualifies as "impracticable" in the content of s.487.1(1)? Does it mean that it has to be impossible, for scheduling or geographical variables, to appear in person before a judge? In *R. v. Erickson*, the British Columbia Court of Appeal interpreted the choice of word by Parliament to mean "something less than impossible and imports a large measure of practicality, what may be termed common sense."[135] The idea that impracticability does not mean impossible, but should be interpreted from of common sense perspective means that an officer can apply for a telewarrant even if he or she could attend in person, but that it would be more practical not to do so. Even if the reason for applying for a telewarrant has to be more than an mere inconvenience, the unusual "impracticability" standard represents «relatively low threshold» standard.[136] More recently, the Ontario Superior Court of Justice has decided that the application for a telewarrant met this standard, in part, because there was a "real need for the police to act quickly in pursuing the issuance of a search warrant".[137]

Telewarrants can be applied for, in Ontario at least, on a 24/7 basis and the time between the application and the authorization can be measured in hours. In *R. v. Boussoulas*, for example, the telewarrant was applied for at 21h31 and the search of the home of the accused was conducted the same night.[138] In *R. v. Côté,* the telewarrant took less than 5 hours to be applied for and issued.[139] The fact that police sometime has to act quickly does not then prevent them from obtaining prior judicial authorization before conducting the search of a cell phone seized incident to arrest. Telewarrant should be seen as a practical solution enabling the police to rapidly pursue their investigation while respecting the right to privacy of the citizens they seek to serve and protect. Moreover, in cases where there is a reasonable basis to suspect a search will prevent an imminent danger to public or police safety, or where there are reasonable grounds to believe that a search will prevent the imminent damaging or destruction of evidence, the doctrine of exigent circumstances advocated by the bright line rule we are here defending will allow warrantless searches of cell

134. *Criminal code*, R.S.C. 1985, c. C-46, s. 487.1(1).

135. *R.* v. *Erickson*, 2003 BCCA 693, at para 33, [2003] B.C.J. No. 2982.

136. *R.* v. *Boussoulas*, 2014 ONSC 5542, [2014] O.J. No. 4525.

137. *Ibid.* at para 77.

138. *Ibid.*

139. *R.* v. *Côté*, [2011] 3 S.C.R. 215.

phones seize from effectively carrying on their duties, and should not be qualified as burdensome for the officers. In cases where nor the exigent circumstances doctrine nor the impracticability standard apply, it is true that police may have a harder time doing their jobs. Nevertheless, in my opinion, this cost does not outweigh the privacy interest Canadian have in making sure the searches they are submitted to have been subject to prior judicial review.

4.4. Balancing the state's law enforcement and the individual's privacy interests

The search of a cell phone incident to arrest engages significant law enforcement interests, but it also attracts an elevated privacy interest. By searching the content of a cell phone seized incident to arrest, police officers are better able to protect themselves and the public, and to discover and preserve important pieces of evidence that can be used in the courtroom. At the same time, they penetrate a very private sphere of privacy and gain access to biographical information that can reveal a great deal about the individual's life. Cell phones are not like any other physical containers that can be found on a person or in his or her immediate surroundings. Smart or dumb, sophisticated or not, these devices can store and generate unique quantities of data and metadata. From a privacy standpoint, one must therefore be prudent when assessing the extent to which police can go to search these devices seized incident to arrest.

In the basic framework of the common law power to SITA, the state's law enforcement interests haves traditionally outweighed privacy interests. Except when the search or seizure engaged very significant privacy interests, such as in the case of samples of bodily substances and strip searches, police where able to seize and search items found on the individual without prior authorization or probable grounds. By allowing 'tailored' and warrantless cell phone searches incident to arrest, the procedure set out in *Fearon* continues in this direction. According to Cromwell J., this formula strikes an adequate balance between the state and the individual interests because it allows the police to effectively pursue the security and evidentiary functions of SITA and to provide a certain level of privacy protection. I do not agree. In my opinion, the bright line and technology-specific rule envisioned in *Liew* and endorsed by the dissenting justices in *Fearon* would strike a more optimal balance because it will allow for even more effective policing and even higher privacy protection. This rule is to prohibit any form of cell phone search incident to arrest, absent exigent circumstances. Police should seize the device indecent to arrest, but should wait prior authorization before searching its content.

For Cromwell J., this would lead to the gutting out of the police power to SITA objectives. Let's review these objectives. First, there is the security function of SITA. Searches of cell phones incident to arrest allows the police to better protect the security of the officers and the public' safety. Cell phones and handheld computing devices are not weapons and do not, from a purely material perspective, represent a significant danger to police or the public. In the context of the security function, the argument is that cell phones can be used to call for violent back up or to coordinate escape. These will be serious cases, but also extraordinary ones. The procedure set out in *Fearon* will allow the police to act promptly and care for the security of the officers and the public. But so is the rule envisioned in *Liew* and in the *Fearon* dissenting opinion. These rare but serious cases will qualify as exigent circumstances and allow the police to search the content of the phone without a warrant. If there is a reasonable basis to suspect a search will prevent an imminent danger, police will be allowed to act quickly. As far as security is concerned, I do not see how the bright line rule would compromise the attainment of the SITA function.

That leads us to the second function of SITA, which is the evidentiary one. Officers can search arrestees and their belongings in order to discover and preserve evidence that can be used in court. This is a very important function since it can be used both to incriminate an individual or to exonerate him or her. In order to enable the police to act promptly, the framework put in place in *Fearon* allows the arresting officers to conduct cursory or tailored, warrantless searches. As we have noted in numerous occasions in this article, and has it as been defended by justices in both the continuation trend and the technology-specific trend, this procedure is contrary to the best practices in data extraction and may lead to the damaging or the destruction of evidence. This is because the cell phone may be vulnerable to remote or automatic kill signals or unfortunate manipulations by the arresting officer. It thus seems that allowing cursory searches of the cell phones seized incident to arrest increases the chances that important inculpatory or exculpatory evidence may be destroyed, lost or damaged. Therefore, allowing these searches is counterproductive and will not lead to the attainment of the evidentiary goals of the power to SITA. On the other hand, demanding that police seek to obtain a warrant that will assign the task of extracting the data to a technologically competent person will increase the likelihood that evidence stored in the phone will be intact and usable in court. Here again, in situations where the risks of conducting a cursory search are outweighed by an imminent threat that will damage or destroy the evidence, the exigent circumstances exception to the bright line rule will allow for the said search. In cases where there are no exigent circumstances, but where the police still need to proceed in a quick fashion, they can apply for a Telewarrant and obtain prior authorization in a matter of hours. Therefore, in the evidentiary function of SITA context, it seems that the bright line rule is more efficient than the procedure set out in *Fearon*.

Let's now turn to the privacy interest and the ways by which the bright linet rule better protects it than the *Fearon* framework. As the Court notes on multiple occasions, section 8 of the *Charter* has been designed to prevent unjustified searches, not to react to them. This is why it was established in *Hunter* that warrantless searches are *prima facie* abusive. Cromwell J. himself stated in *Vu* that the prior authorization requirement prevents abusive searches by making sure "that the search is no more intrusive than is reasonably necessary to achieve its objectives." [140] As I have just mentioned, the rule envisioned by *Liew* and the dissenting justices in *Fearon* provides a more efficient framework from a policing perspective. Because it requires prior authorization to conduct the search of a cell phone incident to arrest, and does not allow warrantless searches absent exigent circumstances, it also prevents abusive searches and provides a higher level of privacy protection. Therefore, the diminished level of privacy advocated in *Fearon* should not be seen as necessary: it does not provide the police with more efficient ways of performing the security function of SITA, and establishes a less efficient way of ensuring the discovery and preservation of evidence. The level of power given to the arresting officers by *Fearon* therefore is not only counterproductive, but it is also unnecessarily detrimental to individual privacy. Moreover, as I have pointed out earlier, this nonessential increase of search power may nourish public mistrust toward police institution, thereby leading to more inefficiency. As I result, the balance struck in the *Fearon* case is not optimal. The proper balance is the one that, when possible, will optimize both the level of privacy protection and the level of police efficiency. Optimizing both these levels is possible in the case of searches of cell phones seized incident to arrest. The manner in which the balance between the state's and the individual's interests reaches its optimal state is by prohibiting, absent exigent circumstances, the warrantless search of cell phone seized incident to arrest.

140. *Vu*, *supra* note 40, at para. 22.

CONCLUSION

The main point of this article was to demonstrate that the framework established in *Fearon* to govern the power to searches of cell phone incident to arrest is not adequate. I have argued that the Court should have adopted a bright line and technology specific rule such as the one envisioned in *Liew* and endorsed by the dissenting justices in *Fearon*. This particular approach, which do not authorized warrantless searches of a cell phone seized incident to arrest, except in exigent circumstances, would have struck an optimal balance between the state's and the individual's interests. The rule recognizes the particularly significant and elevated privacy interests cell phones should command and provides the police with a more effective way to perform the security and evidentiary functions of SITA. It is not that the balance struck in *Fearon* is in and of itself wrong, it is just that it is not optimal. Consequently, I would qualify the *Fearon* case as a missed opportunity to properly circumvent the power of arresting officers to search the contents of a cell phone incident to arrest. I will nevertheless echo Cromwell J.'s concluding remarks in *Fearon* and say that is an area where legislation is desirable. In my opinion, the legislature should adopt the bright line and technology-specific rule which, in the absence of exigent circumstances, would allow the police to seize a cell phone incident to arrest, but require that the police obtain prior authorization before conducting the search of its contents.