Osgoode Hall Law Journal

Volume 55, Issue 2 (Spring 2018) Article 2

9-4-2018

Textual Privacy and Mobile Information

Simon Stern
Faculty of Law, University of Toronto

Citation Information
Stern, Simon. "Textual Privacy and Mobile Information." *Osgoode Hall Law Journal* 55.2 (2018) : 398-439.
DOI: https://doi.org/10.60082/2817-5069.3289
https://digitalcommons.osgoode.yorku.ca/ohlj/vol55/iss2/2

Textual Privacy and Mobile Information

Abstract

The Supreme Court of Canada's decision in R v Marakah attempted to resolve the privacy status of text messages under section 8 of the Charter, but offered an incomplete solution because it failed to address the normative basis for protecting such communications. Despite the complexity of section 8 analysis (which itself is a product of multiple and inconsistent tests used to answer the same questions), the privacy of text messages allows for a relatively simple analysis. Normatively speaking, letters, email, and text messages all attract the same basic privacy interest, and should be treated analogously. However, if the police have objective grounds for believing that particular individuals have been exchanging text messages in furtherance of a crime, reasonable suspicion may justify a limited search, aimed solely at obtaining those messages. This approach protects the public from random and baseless police searches while giving the police access to these communications when there are objective grounds to believe they will disclose evidence of crime.

Keywords

Text messages (Cell phone systems)--Law and legislation; Privacy, Right of; Canada

Textual Privacy and Mobile Information

SIMON STERN*

The Supreme Court of Canada's decision in *R v Marakah* attempted to resolve the privacy status of text messages under section 8 of the *Charter*, but offered an incomplete solution because it failed to address the normative basis for protecting such communications. Despite the complexity of section 8 analysis (which itself is a product of multiple and inconsistent tests used to answer the same questions), the privacy of text messages allows for a relatively simple analysis. Normatively speaking, letters, email, and text messages all attract the same basic privacy interest, and should be treated analogously. However, if the police have objective grounds for believing that particular individuals have been exchanging text messages in furtherance of a crime, reasonable suspicion may justify a limited search, aimed solely at obtaining those messages. This approach protects the public from random and baseless police searches while giving the police access to these communications when there are objective grounds to believe they will disclose evidence of crime.

* Faculty of Law, University of Toronto. For comments on previous drafts, thanks to Vincent Chiao, Dan Priel, Martha Shaffer, and the Journal's two anonymous referees.

ALTHOUGH EMAIL AND TEXTING are no longer particularly novel forms of communication, the questions they pose for the law of search and seizure continue to create difficulties for the courts. These difficulties are particularly acute when the prosecution seeks to use electronic communications as evidence in criminal cases. The discussion in this article focuses on what I will call "mobile information"—text messages, email, and similar transmissions which, having been created to travel across media, are not embedded uniquely in a single physical device but may be found in various places outside of the sender's custody or control, such as on the phone or computer of the addressee or a further recipient, or on a restricted or open-access web site. When obtained from any source, through a duly authorized search or in circumstances where no search has occurred, such evidence does not present difficult questions about admissibility. But when the police acquire mobile evidence during an unauthorized search of the recipient, the question arises whether the sender has a privacy interest in the information itself that justifies excluding the evidence, even though it was not obtained from the claimant. If mobile information is taken from a device that belongs to the claimant, through an unauthorized search, its mobility is insignificant: The privacy interest in the device covers any information extracted during the search. When the device belongs to a third party, on the other hand, it matters fundamentally whether the claimant has a privacy interest in the information itself. In what follows, I propose a framework for evaluating such privacy claims.

The framework proposed here differs, in some fundamental respects, from the one adopted by the Supreme Court of Canada in *R v Marakah*.[1] *Marakah* involved an unauthorized search of a co-conspirator's iPhone in the course of an investigation for conspiracy to engage in illegal firearms sales. The police, having obtained a warrant to search the suspects' homes, seized Marakah's Blackberry and the iPhone of his co-accused, and found incriminating text messages on both devices. The warrants were held to be invalid, but the application judge admitted the text messages, and both men were convicted.[2] Marakah argued that he had an ongoing privacy interest in the text messages, even after their delivery, but the trial and appellate courts rejected that contention.[3] In a majority opinion by Chief Justice McLachlin, the Court reversed the lower court decisions, adopting Marakah's view. However, the Court made no effort to analogize text messages to other forms of written communication, thereby failing to address the normative

1. *R v Marakah*, 2017 SCC 59, 42 CR (7th) 1 [*Marakah*].
2. *Ibid* at paras 2, 3.
3. See *R v Marakah*, 2016 ONCA 542, 131 OR (3d) 561 [*Marakah*, ONCA].

basis for the privacy interest in question. Instead, the majority drew on three considerations in a fashion that aims to establish a privacy interest in text messages as a general matter, but in effect leaves open the possibility that in a given case, the particular circumstances may eradicate that interest.

First as to the "place" of the search, the Court observed that text messaging, no matter where it occurs, can serve to "create private chat rooms between individuals,"[4] and that when it does, this factor supports the sender's privacy interest. Nevertheless, the Court recognized that texting does not always occur within a secluded zone, and concluded that "different facts may well lead to a different result."[5] "Place," then, may enhance or diminish the sender's privacy interest, depending on the circumstances.[6] Second, as to the sender's "control" over the object of the search, the Court stated that after the message has been delivered, the sender's privacy interest may persist by virtue of her "shared control" over it, as when someone shares control over their office computer with an employer who also has access to it.[7] The better answer, however, is that control has little significance in this analysis, just as it does when the police are searching for letters. People generally cannot control what the recipient does with a letter, but the sender's privacy interest does not vanish upon delivery: The police are not free to seize letters, on a warrantless basis, from any of the places where they might be found.[8] That answer would help to show why text messages *generally* attract a privacy interest—the point that *Marakah* seeks to establish. Basing that interest on the sender's *persisting* control, instead, has the undesirable effect of conceding that where the Crown can show definitively that such control is lacking, the privacy interest wanes.

4. *Ibid* at para 28 [emphasis omitted].
5. *Marakah*, *supra* note 1 at para 55. As the Court explained, "messages posted on social media, … [or] in crowded Internet chat rooms, or … on online message boards" do not attract a privacy interest; more generally, various factual circumstances, relating to how and where the message is sent or read, can also eliminate the privacy interest (*ibid*). A vast array of contingencies that may have that effect, and so the possibility of "a different result" necessarily depends on the facts of the case (*ibid*).
6. One might read *Marakah* as making this point directly—as, for instance, when the Court observes that "[t]he place of the search is simply one of several factors that must be weighed" (*ibid* at para 30). However, given that the Court singled out three factors for discussion, rather than reviewing all of the potentially relevant factors to separate the inconclusive ones from the others, the Court evidently meant to confer on these three a significance that the others lacked.
7. *Ibid* at para 42 (likening the "shared control aspect of this case" to one of an employee whose "employer … could [also] access the contents of the computer"). The sender of a text message, however, does not necessarily have any access to the recipient's device.
8. For further discussion, see the text accompanying notes 78-80 below.

Last, the Court observed that because text messages can "reveal[] a great deal of private information,"[9] this factor also supports a continuing privacy interest. Here, the Court comes closest to setting out a normative justification, but stops short, instead making a descriptive statement about the messages' content.[10] Notice that postcards do not typically reveal highly intimate personal details, and yet most people would not consider them any more open than letters to random search, if the police seize them without legal authorization from the recipient's briefcase or residence—nor has any Canadian court ruled otherwise.[11] Conversely, credit card transactions may be highly revealing, and yet no Canadian court has ruled that they attract a strong privacy interest, as a general matter.[12] The likelihood of revealing personal information, however important, does not seem to be the crucial feature. *Marakah* relies on two factors—place and control—that yield variable results, depending on the circumstances, and one factor that cannot, by itself, establish a normative ground for a general privacy interest in text messages.

In this article, I propose such an account, drawing on the similar social norms relating to various forms of written communication. In brief, I suggest that text messages cannot be normatively differentiated from letters, and that they both carry a certain basic privacy interest on the sender's part, because that

---

9. *Marakah*, *supra* note 1 at para 37.
10. In so doing, the majority misconstrues Marshall McLuhan's famous observation that "the medium is the message," *ibid* at para 33 quoting Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: McGrawHill, 1964) at 7. As McLuhan explained, "it is the medium that shapes and controls the scale and form of human association and action" (*ibid* at 9). McLuhan's point was that the same content carries a different meaning, when read in the paper, or heard on the radio, or seen on the television (or, he might have added, read on the internet) because those different media shape and control content in different ways. But the *Marakah* majority takes this in precisely the opposite fashion, reasoning that the *content* is the message, and that it thereby determines the significance of the medium. According to the Court, "[t]he medium of text messaging broadcasts a wealth of personal information capable of revealing personal and core biological information," and this tendency to convey private content helps to establish a privacy interest in the medium that conveys it (*Marakah*, *supra* note 1 at para 33). This may be a sound legal conclusion, but McLuhan offers no help in establishing it.
11. There is little jurisprudence concerning protection for postcards, but see Justice Michelle Fuerst, Michal Fairburn & Scott Fenton, "Warrantless search of cell phone text messages may violate message sender's reasonable expectation of privacy" (16 October 2015), *Insider* (blog), online: Thomson Reuters <www.westlawnextcanada.com/blog/insider/police-powers-expectation-of-privacy-466> (commenting on *R v Pelucco*, 2015 BCCA 370, 376 BCAC 226 [*Pelucco*], and observing that "post card[s] [and] letter[s]" generally attract an expectation of privacy).
12. For further discussion, see the text accompanying note 42 below.

is an interest "that society is prepared to recognize as 'reasonable.'"[13] That basic privacy interest is sufficient to protect against random and groundless searches. The police are no more entitled to undertake baseless, large-scale searches of mobile phones, in the hope of finding text messages that would incriminate the sender, than to undertake searches for any other form of written correspondence to acquire documents that incriminate the sender. The interests that animate privacy rights generally in this area—the autonomy, integrity, and dignity interests of individuals in a free and democratic society[14]—would be radically eroded if people had to assume that whenever they communicate with others, the content is presumptively open to random search by the police, unsupported by any articulable justification, whenever the content is preserved in a form that persists after the communication has been received.

Nevertheless, I suggest, the situation is very different when the police have reasonable suspicion to believe that certain individuals are involved in a serious crime. "A 'reasonable' suspicion means something more than a mere suspicion and something less than a belief based upon reasonable and probable grounds."[15] Like the higher standard, however, it must be "based on objectively discernible facts."[16] Courts have used the standard of reasonable suspicion to permit limited searches, such as a frisk or pat-down.[17] Analogously, this may provide a sufficient basis for a search of the recipient's mobile device, aimed specifically at yielding the text messages relevant to the crime, and focused on obtaining only those messages.

In Part I, I show why questions of informational privacy, unlike most other varieties, have traditionally been hard to answer categorically, under the Court's jurisprudence, and have often been answered contingently—which is to say that particular examples are often analyzed individually when challenged in court. As a result, both the public and the police may have great difficulty ascertaining the privacy interest that attaches to a given item (*e.g.*, an email or a text message), leaving the public unsure about their rights, and frustrating the ability of the police to do their jobs effectively. In *Marakah*, the Court sought to offer a categorical solution to the treatment of text messages, but the decision

13. *R v M(A)*, 2008 SCC 19 at para 33, [2008] 1 SCR 569 citing *Katz v United States*, 389 US 347 (1967) [*Katz*].
14. See *e.g. Hunter v Southam*, [1984] 2 SCR 145 at 159, 11 DLR (4th) 641 [*Hunter*]; *R v Plant*, [1993] 3 SCR 281 at 293, 157 NR 321 [*Plant*].
15. *R v Kang-Brown*, 2008 SCC 18 at para 75, [2008] 1 SCR 456 [*Kang-Brown*].
16. *R v Chehil*, 2013 SCC 49 at para 26, [2013] 3 SCR 220 [*Chehil*].
17. See *e.g. R v Solomon*, 2014 ONSC 6857 at para 88, 118 WCB (2d) 259; *R v Atkins*, 2013 ONCA 586 at paras 14-15, 210 OAC 397; *R v Tyndale*, 2010 ONSC 1744 at paras 105-06, 208 CRR (2d) 272.

does not achieve this effect, unless the "personal information" strand of the analysis has the power, by itself, to resolve the question. In further elaboration of this problem, I then distinguish, in Part II, between spatial and informational privacy, both as a general matter, and more specifically with respect to the Court's jurisprudence. Next, in Part III, I turn to the Court's privacy jurisprudence, focusing specifically on two of the prevailing tests, set out in *Edwards* and *Plant*. Part III also confronts the "lack of control" theory adopted by some courts, and by the dissent in *Marakah*. On that view, once the sender loses control over the message, the privacy interest accordingly vanishes. The majority in *Marakah* evaded this argument, reasoning that the sender and recipient may have "shared control" over the message.[18] But that answer seems to concede that without such control, the sender has no privacy interest. As will become evident, this theory crumbles upon scrutiny, because once we look to the social norms concerning written correspondence, we see that control is not a very significant consideration when assessing the sender's privacy interest. Finally, in Part IV, I turn to the normative grounds for concluding that individuals have a reasonable expectation of privacy in text messages, but I show, in Part IV(B), how the standard of "reasonable suspicion" may be applied so as to permit the police limited access to only those text messages for which there are objectively ascertainable grounds to believe that they were exchanged in furtherance of a crime.

In the ensuing discussion, I consider an array of problems arising in this area, but I focus on informational privacy in text messages—an issue that accentuates, with unusual clarity, the problem of the categorical and the contingent. To show why, and to specify more precisely the questions these cases raise, it will help to describe a common scenario—essentially the one that arose in *Marakah*. Having identified several suspects in a conspiracy to sell or distribute contraband, the police proceed to search them. The incriminating evidence that emerges includes text messages relating to the conspiracy, sent between the suspects. It eventually transpires that legal authorization to obtain the messages was lacking—either because they were outside the scope of an authorized search, or because the police acted without a valid warrant and without a valid exception to the warrant requirement. Nevertheless, when each suspect moves to exclude that evidence, the prosecution responds that none of them may contest the search of another's phone; thus a message sent from A to B, and retrieved from B's phone, is admissible against A. The defendants reply that a reasonable expectation of privacy accompanies all text messages no matter where they travel, and that because there was no legal authorization for the search, the messages are

18. See the text accompanying *supra* note 7 above.

inadmissible. Formerly, the prosecution would have replied that no one has any reasonable expectation of privacy in a text message. Now, after *Marakah*, the prosecution would assert that the accused has no privacy interest in these particular text messages (so long as any of the factors singled out in *Marakah* tilt in the other direction). Thus the defence would propose a categorical answer and the prosecution would reply that the analysis is contingent—*i.e.*, that it depends on the particular circumstances of the case.

I. THE CATEGORICAL AND THE CONTINGENT

To make sense of the legal landscape in this area, it will help to begin by distinguishing between two kinds of problems that arise in the law of search and seizure. Some of these problems can be resolved categorically and others—under the existing jurisprudence—tend to be resolved contingently. The concern to balance privacy and security prompts the courts, when considering the legitimacy of a search, to undertake a complex multifactor analysis that includes a careful and measured appraisal of each component, and that often turns on contentious claims about objectively justified understandings of privacy.[19] This elaborate and nuanced approach is best suited for questions that can be answered categorically—that is, questions about the privacy interest in places or things,

19. See *e.g. Katz*, *supra* note 19 at 361 ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'") (Harlan J, concurring); *R v Patrick*, 2009 SCC 17 at para 17, [2009] 1 SCR 579 [*Patrick*]. On the contentious nature of these ascriptions, consider, *e.g.*, the observation that "[p]rivacy analysis is laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy" (*ibid* at para 14). The disputable nature of these judgments was demonstrated long ago in a study revealing widespread disagreement between the US Supreme Court and the public as to the extent of the privacy interest in various activities that have figured in the jurisprudence. See Christopher Slobogin & Joseph E Schumacher, "Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at 'Understandings Recognized and Permitted by Society'" (1993) 42:4 Duke LJ 727.

such as lockers, backpacks, and mobile phones, as a class.[20] When such a question arises for the first time and a court conducts a balancing analysis, the result is to specify the privacy interest in all members of the class. When the question next arises, rather than having to inquire anew into the totality of circumstances, the court need only refer to the categorical answer supplied earlier.

That categorical answer has the great advantage of yielding a bright-line rule for the police and the public. Because the first backpack case effectively deals with virtually all future cases (subject to various exceptions that also apply generally in the law of search and seizure), the decision enables people to assess, with a fair degree of accuracy, whether a prospective search of a backpack would be legally valid, and on what grounds. Where the courts can deliver a categorical answer, specifying the privacy protection that applies to lockers, curbside garbage bags, and heat patterns,[21] the balancing test yields the same kind of result as any other precedential opinion that tells individuals how to direct their conduct in accordance with the law, how they may legitimately expect to be treated, and what would count as a legal violation. The result is to inform the public about their privacy rights in a clear and comprehensible fashion, and to provide guidance to the police, whose ability to do their job effectively depends on the availability of reliable bright-line rules.

But although the Court has emphasized that questions of privacy "must be framed in broad and neutral terms,"[22] it has crafted jurisprudence that makes categorical answers difficult in some contexts. Some questions about the validity of a search are answered contingently, not categorically, and in these cases the balancing test is not very helpful in informing the public or in guiding the conduct of the police. This has been a persistent difficulty in the area of informational privacy—and remains so even after *Marakah*. To ask what privacy interest attaches to email or text messages, for instance, under the existing

---

20. See *R v Buhay*, 2003 SCC 30 at paras 18-24, [2003] 1 SCR 631 [*Buhay*] (lockers); *R v M(A)*, *supra* note 13 at paras 61-65 (backpacks); *R v Fearon*, 2014 SCC 77 at paras 51-58, [2014] 3 SCR 621 [*Fearon*] (cell phones). Notice that in "reject[ing] the idea that s. 8 of the *Charter* categorically precludes any search of a cell phone seized incidental to a lawful arrest" (*ibid* at para 64), the Court was refusing to adopt a categorical *exclusion* from an *exception* to the warrant requirement, not refusing to make a categorical statement about the nature of the privacy interest in cell phones.
21. See *supra* note 6 and the accompanying text. See also *Patrick*, *supra* note 19 (garbage bags); *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 [*Tessling*] (heat patterns).
22. *R v M(A)*, *supra* note 13 at para 70 quoting *R v Wong*, [1990] 3 SCR 36 at 50, 120 NR 34 [*Wong*]. See also *R v M(A)*, *supra* note 13 at paras 116, 120; *Kang-Brown*, *supra* note 15 at para 138 quoting *Wong*, *ibid* at 50; *R v Buhay*, *supra* note 20 at para 19 quoting *Wong*, *ibid* at 50.

jurisprudence, is to ask the wrong question: The multifactor balancing test yields answers that apply to particular examples rather than to the class as a whole. Asking what privacy interest someone has in a text message is like asking the same question about a conversation. It is difficult to answer as a general matter because a given conversation could fall anywhere along the spectrum of privacy interests, depending on factors such as who was present and where the conversation took place.[23] For example, in the case that introduced the balancing test to this area of law—a case involving an unauthorized recording of a call placed from a public phone booth—the Court emphasized that the defendant had "shut[] the door behind him," and this act turned the booth into a "temporarily private place."[24] A door left open could yield a different result. The same considerations apply to text messages. Thus, in *Marakah*, the Court distinguished between messages that are shielded from others' eyes and messages that are readily visible to others, *i.e.*, between messages over which the sender retains "shared control" after delivery and those for which such control is lacking.[25] As I will argue in Part III(C) below, a different rationale for protecting text messages—based on social norms—would yield a more clearly categorical solution.

Given that the contingent problems must be resolved after the fact, on a case-by-case basis, the predictive value of any particular legal decision for law enforcement officers, and for the public, is limited, because the *ex post* balancing analysis may apply differently in another case with slightly different features. A workable solution to this privacy question must be one that allows for a certain amount of reliable assessment *ex ante*—a solution that strives, provisionally, to offer categorical answers where practically possible, without altering the structure of a jurisprudential arrangement that provides for contingent answers

---

23. Thus, although some courts have likened text messaging to conversations with the aim of showing why both should generally be viewed as highly private, the analogy merely restates the problem rather than resolving it. See *e.g. Marakah*, ONCA, *supra* note 3 at paras 109, 111 ("[A] typical exchange of text messages … is essentially a modern version of a conversation and *can* contain *as much* private information as an oral conversation" [emphasis added]) (LaForme J, dissenting). Even if an electronic or oral exchange reveals private information, it may fail to attract a privacy interest because of the circumstances in which it took place. Hence, so long as that interest depends on "the totality of circumstances," and those circumstances must be ascertained for any given example, the analogy does not have the categorical force seemingly attributed to it. Courts pursuing this analogy usually cite *R v Telus Communications Co*, 2013 SCC 16 at para 5, [2013] 2 SCR 3 (in which the Court noted that "[t]ext messaging is, in essence, an electronic conversation"); however, for the reasons just given, the analogy marks the beginning of an analysis, not the end of one.
24. *Katz*, *supra* note 13 at 517 (Harlan J, concurring).
25. See *supra* note 7 and the accompanying text.

whenever appropriate. Consider phone booths again: To say that they are treated differently, depending on whether the door is open or closed, goes a long way towards the *ex ante* guidance that a categorical rule would offer. Not all questions of informational privacy can be resolved in this fashion, but there are some means of managing these problems in ways that tilt more towards the categorical.

To raise this point is not to suppose that the courts should prefer an approach that gives the police readier access to more information on a relatively low standard; a workable solution is one that tells the police clearly what is permitted and what is prohibited. A doctrine that serves to deprive the police of warrantless access to nearly all text messages—as *Marakah* aims to do—is a significant improvement over the prior jurisprudence, which evaluated the privacy interest in each message *ex post*. Providing guidance does not require that investigations must be as easy as possible; rather, it requires clarifying in advance, as much as possible, what the police may lawfully search and what is off limits. In what follows, I will suggest an approach that takes precisely this form: By adopting a requirement of reasonable suspicion as to certain objectively specifiable features of the text messages in question and the circumstances surrounding them, the courts would deprive the police of warrantless and groundless access to most text messages—including some that are open to warrantless scrutiny, under *Marakah*—while affording warrantless but justified access if the police can show that they have sufficient grounds to believe that the particular messages they seek to obtain were related to specific criminal activities. In these cases, the basis for the search, though insufficient for a warrant, is strong enough to ensure that the police are not using random fishing expeditions to acquire incriminating evidence. Before developing that approach, however, I will explain the currently applicable doctrine in more detail.

In an area where those who are guided by the law must often make quick decisions using limited information, clarity and predictability are particularly important. Their absence generates significant costs in terms of misdirected or needlessly duplicative police efforts, lost prosecution opportunities as well as ill-advised prosecutions, and risky and expensive information-gathering techniques that are adopted because of uncertainty about cheaper and safer alternatives. The framework proposed in this article is aimed at yielding clarity and predictability, without eliminating or reducing the basic privacy interest at issue. Categorical solutions also pose some danger because they operate so bluntly; however, they have the great virtue of applying in a "broad and neutral" fashion,[26] allowing the police and citizens alike to tell how a privacy interest is

26. See *supra* note 22 and the accompanying text.

likely to attach. Contingent solutions are much more dangerous, because they can make rights opaque and uncertain. Perhaps there can be no perfect solution, but the one suggested in this article strives for a more categorical approach, capable of allowing a reasonable *ex ante* assessment of privacy rights.

II. SPACE, INFORMATION, AND PRIVACY

Although courts never tire of repeating the truism that constitutional limits on search and seizure "protec[t] people, not places,"[27] many of the easy questions in this area are easy precisely because they involve places for which the applicable privacy interest can indeed be specified categorically.[28] It is when the question relates not to places, but to information conveyed by one individual to another, that the emphasis on "people" becomes greater and the answers become harder. Consider the following examples involving places. Someone driving on the street or making a purchase at the drugstore is acting in public, and, because of the location, cannot invoke a constitutional privacy interest to keep law enforcement officers from observing this conduct.[29] Someone at an airport or border crossing has a diminished privacy interest because of the location.[30] Residences, backpacks, and lockers are all entitled to constitutional solicitude because the courts have regarded them as spaces of a certain type—intimate, sealed—such that the owner has a right against unauthorized intrusion. These cases are easily resolvable insofar as they address the privacy interest in a particular kind of space: When it is seen as a personal and enclosed alcove, it receives more privacy protection, and when it is seen as open and public, it receives less.

Analogously, when evaluating privacy protection for mobile phones, courts have often likened them to places. For a good while, courts afforded

---

27. *Hunter*, *supra* note 14 at para 159 quoting *Katz*, *supra* note 13 at 351.
28. As Professor David Alan Sklansky notes, the US Supreme Court has continued to "read the Fourth Amendment to provide protections that are place-specific," and this practice of "[t]ying reasonable expectations of privacy to special, constitutionally protected places has seemed to drain *Katz* of much of its significance." See David Alan Sklansky, "'One Train May Hide Another': *Katz*, Stonewall, and the Secret Subtext of Criminal Procedure" (2007) 41:3 UC Davis L Rev 875 at 884-85.
29. See *e.g. R v Felger*, 2014 BCCA 34 at paras 46, 52, 350 BCAC 53: "The 'search' occurred in a retail premises that was open to the public … there was no reasonable expectation of privacy in the retail premises."
30. See *e.g. Kang-Brown*, *supra* note 15 at para 45: "The security measures taken at airports have of necessity resulted in a diminished expectation of privacy in that setting."

them little protection if they were not "locked" (*i.e.*, password-protected),[31] but more recently the Court has repudiated that conclusion while nevertheless preserving the analogy:

> Like the private sphere of the home, our digital devices remain intensely personal, even when we do not take every possible precaution to protect them. An individual who leaves her front door unlocked does not forfeit her privacy interest in her home to the state; the same is true of her phone.[32]

The emphasis on "personal" details, which might seem to call attention to the subject matter rather than the location, quickly gives way to a spatial analogy. The recognition that spatial analogies support categorical answers may explain why the Court in *Marakah* held that the "place" of the search is a factor that supports the sender's privacy interest, even while acknowledging that "an electronic conversation does not occupy a particular physical place,"[33] and that when electronic messages and conversations are visible to others, the conceptual wall that creates a "zone of privacy" dissolves, and the sender's privacy interest erodes.[34]

Other privacy problems, currently treated as categorical, might yet drift into the realm of the contingent, and these problems typically feature *liminal* spaces—usually spaces that border ambiguously on the domestic. Heat patterns emanating from a residence are, at present, treated as a fairly blunt information source, incapable of revealing specific and granular details about the activity inside a building. According to the Court, a forward-looking infrared camera (FLIR) can measure only the total quantum of electricity being consumed, and so cannot convey information about the inhabitants' personal habits—at least not in a way that would reveal "biographical core" information.[35] But that could change, for example, if the technology becomes capable of isolating the particular

---

31. See *e.g. R v Belcourt*, 2012 BCSC 229 at para 32, [2013] BCWLD 3351: "[N]one of the items seized … including the cell phone [were] … locked, in such a way as to indicate that the owner or possessor maintained a reasonable expectation of privacy in it"; *R v Thompson*, 2013 ONSC 4624 at para 44, 113 WCB (2d) 741: "[A]s the cell phone was neither locked nor password protected, the police were at liberty to conduct a cursory search of the phone to ascertain if it contained evidence relevant to the alleged crime."
32. *R v Fearon*, *supra* note 20 at para 160.
33. *Marakah*, *supra* note 1 at para 28.
34. *Ibid* at para 37.
35. *Tessling*, *supra* note 21 at para 62: "The information generated by FLIR imaging about the respondent does not touch on 'a biographical core of personal information,' nor does it 'ten[d] to reveal intimate details of [his] lifestyle' … . It shows that some of the activities in the house generate heat." *Cf Kyllo v US*, 533 US 27 (2001) at 38: "The Agema Thermovision 210 might disclose … at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate.'"

room where electricity is being used or the kind of device at work. Under such circumstances, the Court might revisit the question and conclude that each time the police wish to record that information, their request must be assessed individually—not as a generic instance of FLIR measurement, but as a particular intrusion whose legality requires an individuated balancing analysis.

Courts have also addressed the privacy interest in garbage bags by dwelling on spatial considerations, and here again, one may discern a certain kind of hesitation about the answer, because of the bags' liminal location. The contents of a trash bag may, of course, reveal "biographical core" information, and yet the Court has treated the issue categorically, holding that when people leave garbage at the curb to be collected, they "intend[] to abandon [their] proprietary interest in the physical objects," thereby rendering the contents open to police inspection without any need to articulate a justification for the search.[36] The Court took some pains to rationalize its holding in spatial terms, explaining that only after "the garbage [has been] placed *at or within reach of the lot line*, [can] the householder … be said to have unequivocally abandoned it"[37] By this logic, the differing privacy interests that would otherwise attach individually to each of the various contents within the bag are all effaced once it has been placed in a certain location. Although the Court analyzed the problem in spatial terms to generate a categorical answer, Justice Abella concurred separately, noting that garbage bags "may contain the most intensely personal and private information about ourselves,"[38] and proposing that they should be "protect[ed] from *indiscriminate* state intrusion"—that is, the kind of groundless search that the police may conduct whenever a reasonable expectation of privacy is lacking.[39] I will return to this point later; for the moment, it is sufficient to observe that these concerns do not arise when someone uses a public trash can. In those cases, there is no dispute that the act of discarding an item allows the police to seize it without any articulable cause, and no one has suggested that reasonable suspicion should be

36. *Patrick*, *supra* note 19 at para 54; Compare the rejoinder of Justice Abella: "What we inelegantly call 'garbage' may contain … intensely personal and private information" (*ibid* at para 76).
37. *Ibid* at para 62 [emphasis added]. Contrast *R v Roy*, 2010 BCCA 448 at para 22, 295 BCAC 191 ("[W]here a person is asked to consent to a search of the trash while it is still located within the home, the person is essentially being asked to consent to an otherwise unconstitutional search").
38. *Patrick*, *supra* note 19 at para 76.
39. *Ibid* at para 77 [emphasis added].

required.[40] The disagreement, then, arises because of the liminal space around the home, not because of the inherent potential for garbage to include highly personal information.

Finally, some questions are answered contingently, because they do *not* relate to places. Credit card purchases, chat room exchanges, email—each of these, under the existing jurisprudence, might attract a greater or lesser privacy interest depending on the subject matter, the way the transaction is conducted, or the involvement of others. In *R v Siemens*, for example, the Provincial Court of Saskatchewan applied the multifactor balancing test to conclude that although the accused might have had a "subjective expectation of privacy" in a credit card transaction involving a car rental, the information it recorded did "not reveal intimate details of his lifestyle or his personal choices,"[41] and consequently the court was "not satisfied … that the accused had a reasonable expectation of privacy in [that] information."[42] Conversely, in *R v Pheasant*, the Ontario Court of Justice observed that individuals "have a reasonable expectation of privacy in their own banking and credit card records," evidently because, when collected in the aggregate, such records could reveal "biographical core" details that a more carefully delimited search would not disclose.[43] Again, in *R v Kwok*, the Ontario Court of Justice held that the claimant had no privacy interest in conversations taking place in "a chat room to which many people subscribed and spoke," but did have a privacy interest once he "move[d] to [a] private chat room," because that "change[d] the nature of the communication and ma[d]e it a private communication."[44] When questions of informational privacy are not answered

40. See *e.g. R v D(B)*, 2011 ONCA 51 at para 14, 273 OAC 241 ("I cannot see how B.D. could have any reasonable expectation of privacy in the documentation she left, discarded, in a store frequented by the general public"); *R v Marini*, 71 WCB (2d) 727, 2005 CarswellOnt 9228 (WL Can) at paras 7, 17 (Sup Ct) (no expectation of privacy in ginger ale cans "seized from a recycling container in the public hallway" and "from a men's washroom provided for use by the public"); *R v Delaa*, 2006 CarswellAlta 2466 (WL Can) at para 124, [2006] AJ No 948 (QL) (QB) (accused was "in a public parking lot of a service station, and [he] cavalierly disposed of the gum in a manner that could not have carried with it any expectation of privacy or secure disposal").
41. *R v Siemens*, 2011 SKPC 57 at paras 29, 52, 374 Sask R 193 [*Siemens*].
42. *Ibid* at para 55. See also *R v Okubadejo*, [2008] OJ 4732 (QL) at para 22, 2008 CarswellOnt 7039 (WL Can) (Sup Ct) (the accused had no reasonable expectation of privacy in a particular record of a "credit card transaction … seized by police from a gas station" at para 1); *R v Stymiest*, 2006 NBQB 160 at paras 23, 46, 304 NBR (2d) 200 (the accused had no reasonable expectation of privacy in the particular travel expense claims and credit card charges that the police had acquired on a warrantless basis).
43. *R v Pheasant* (2000), 48 WCB (2d) 75 at para 55, 2001 GTC 3427 (Ont Ct J) [*Pheasant*].
44. *R v Kwok*, 78 WCB (2d) 21, [2008] OJ 2414 at para 22 (Ct J).

by reference to spatial considerations (as with the curbside garbage bags), the analysis tends to proceed through a careful examination of the challenged records or documents, involving the particular features of each.

Notice that these cases *could* be resolved categorically: For instance, in *Siemens* the court might have ruled (as *Pheasant* did) that because of general capacity for credit card records to reveal highly personal details, they are categorically protected, and it made no difference that the particular record in question conveyed no intimate information. *Marakah*, as we have seen, proposes a categorical solution to the treatment of text messages, but in so doing, draws on factors that could yield "different result[s]" depending on the circumstances.[45]

To sum up, in virtually every case involving privacy in a place or thing (backpacks, cell phones, garbage left at the curb), the analysis has, in effect, been conducted *ex ante* by means of a legal decision that addresses that category. Even when a later court (evaluating the validity of a warrantless backpack search, for example) makes a point of applying the balancing test, comparing the case at hand to the precedential one, the procedure is essentially mechanical, simply designed to reiterate and confirm the logic of the controlling precedent, not to find out whether it can be replicated (as with repetitions of scientific experiments).[46] That courts were content, for so long, to resolve disputes in this area of the law by attending to places rather than people, suggests that the privacy problems flowing from mobile information remained comparatively inconspicuous for most of the twentieth century, making a spatial and categorical solution plausible. Indeed, *Katz v United States*, the decision that sponsored the turn away from places and towards people as the objects of legal protection, was also the case that produced the "totality of the circumstances" test as a byproduct.[47] Just as privacy questions that have mainly to do with protected spaces are usually answered categorically, those that are not readily understood in spatial terms are often taken to require the more thoroughgoing and individuated analysis that *Katz* introduced. Let us turn, then, to the most frequently invoked versions of the balancing test in Canadian jurisprudence.

---

45. See note 5 and accompanying text above.
46. For a valuable comparison between these two methods of repetition and evaluation, see Mary M Kennedy, "Generalizing from Single Case Studies" (1979) 3:4 Evaluation Q 661.
47. *Katz*, *supra* note 13.

III. TWO PRIVACY FRAMEWORKS

Canadian courts have fashioned various tests for evaluating the privacy interests that may protect individuals from an unauthorized search; two of the most prominent were set out in *R v Edwards* and *R v Plant*[48] (I put aside the version sometimes attributed to *R v Tessling* and sometimes to *R v Spencer*, which redescribes the *Edwards* test at a greater level of abstraction).[49] The version in *Edwards* functions generically, with an implicit assumption that the typical dispute involves a contestation over the privacy interest in a place or physical object, while the version in *Plant* focuses particularly on informational privacy. Thus, if a new question arises as to the privacy interest in a certain kind of space, the analysis should proceed under *Edwards* (or perhaps *Spencer*, or both) whereas if such a question arises as to informational privacy, the analysis should also proceed under *Plant*. The availability of several different tests, however, has created some inconsistency in the law: Courts have used nearly every possible combination of the three tests (using one, two, and rarely all three of the above) in the checkerboard array of cases confronting questions of informational privacy.

A. *EDWARDS* AND *PLANT*

Edwards set out a seven-factor test for assessing the "totality of the circumstances" bearing on a claimant's privacy interest, though the Court hastened to add that the list was not exhaustive. Those factors include:

> (i) presence [of the accused] at the time of the search; (ii) possession or control of the property or place searched; (iii) ownership of the property or place; (iv) historical use of the property or item; (v) the ability to regulate access, including the right to admit or exclude others from the place; (vi) the existence of a subjective expectation of privacy; and (vii) the objective reasonableness of the expectation.[50]

In passing, it may be worth commenting on the origins of this formula, which *Edwards* attributed to *United States v Gomez*.[51] *Gomez* was concerned with a claimant's standing to assert "a reasonable expectation of privacy in … [an] area

48. *R v Edwards*, [1996] 1 SCR 128, 132 DLR (4th) 31 [*Edwards*]; *Plant*, *supra* note 14.
49. *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 [*Spencer*].
50. *Edwards*, *supra* note 48 at para 45. *Spencer* condenses these factors into four headings, which might be regarded as an improvement, but carries the risk of presenting the analysis at a level of abstraction that obscures the relevant considerations, and necessitates recourse to *Edwards* (or another test) for more specific guidance about their meaning. See *Spencer*, *supra* note 49 at para 18.
51. *United States v Gomez*, 16 F (3d) 254 (8th Cir 1994) [*Gomez*].

searched"—that is to say, in a place—and said nothing about the presence of the claimant.[52] It is unclear how "presence" entered the *Edwards* test; however, it will be evident that whenever there is a question as to privacy in mobile information as such (rather than in the device holding that information), the factors involving physical considerations have little significance.

In the case of an email, chat-room record, or text message retrieved from a source that does not belong to the claimant, questions of physical custody, ownership, and historical use of the text or record (or device holding that information) can do no work in enhancing the claimant's privacy interest and will generally be irrelevant. In consequence, the questions of regulating access and objectively reasonable expectations of privacy remain as the pertinent considerations. "Presence" may be significant when the police are searching an item or a place in which a claimant could assert ownership (such as a residence, car, locker, or suitcase), and when the police are searching a physical space that the claimant is occupying (*e.g.*, a stall in a public washroom or in someone else's residence).[53] When the police are extracting information from a phone, computer, or similar device in the hands of a third party, the claimant is usually absent, and the search would not be more invasive if the claimant were present. In such a case, the third and fourth *Edwards* factors (ownership and historical use of the property) must also be excluded: The device storing the information is not the property of the accused, nor is the information itself (in the relevant sense of "property"), and the historical use of the device and of the information can have no bearing on the privacy of the claimant (assuming that the "historical use" factor even applies here).

In the case of mobile information, the second *Edwards* factor ("control of the property") amounts to much the same thing as the sixth factor ("the ability to regulate access"). Arguably, "control of the property" applies better to physical property, for which ownership is readily associated with control, whereas "the ability to regulate access" applies better to information, because its intangible nature makes access the more salient question, but a resort to either would ultimately emphasize that when the police obtain mobile information from the recipient, the sender has usually sacrificed some control or regulation over access. The question, then, is what difference that should make in the analysis, and on this point, the courts have diverged significantly. Some courts—including the Court of Appeal for Ontario, in the decision that *Marakah* reversed—have reasoned that sending a message necessarily entails giving up control over

52. *Ibid* at 256.
53. On the last point, see Sklansky, *supra* note 28.

it, and thereby losing any privacy interest, while others have repudiated that conclusion.[54] In Part III(C) below, I will show why the "loss of control" argument establishes very little. Here, it is sufficient to observe that the control/access parts of the test have done much of the work when courts have turned to *Edwards* to resolve questions about mobile information. The only remaining consideration is the inquiry into "objective reasonableness"—a vexed question that bedevils every privacy case, and that has also produced a significant amount of disagreement among the courts, including disagreement as to what grounds this question should encompass. I take up this question below, in Part IV(A).

Turning from *Edwards* to *Plant*, we see that the latter is less apt to provide categorical answers. In focusing on informational privacy, *Plant* poses a series of questions that can sometimes, but not always, be answered before the police conduct a search. *Plant* mentions five factors:

> [1] the nature of the information itself, [2] the nature of the relationship between the party releasing the information and the party claiming its confidentiality, [3] the place where the information was obtained, [4] the manner in which it was obtained and [5] the seriousness of the crime being investigated.[55]

The Court did not apply this test in *Marakah*, even though *Plant* is specifically directed at questions of informational privacy, and *Edwards* is not. From one perspective, that choice makes good sense, because the *Plant* test would significantly complicate the analysis, as the following paragraphs show. On the other hand, if *Plant* does not apply here, then its use in evaluating questions of information privacy more generally would also seem to be open to question. Numerous decisions relating to informational privacy have drawn on the *Plant* test, and if the Court now regards it as inapposite, it would have been helpful to say so directly.

Again, it bears repeating that when a search yields email, text messages, and the like, the significance of a given factor may not be readily evident, because the relevant details may not be available before or during the search. The "nature of the information" bears on a claimant's privacy most acutely when the search yields "biographical core" information.[56] What counts as personal and revealing is sometimes a matter of interpretation. Consequently, a search that may have appeared legitimate when it was underway could eventually prove to be

---

54. See note 7 and accompanying text above. The *Marakah* majority did not rebut this view, but instead reasoned that the sender may sometimes have "shared control" with the recipient. See *Marakah*, *supra* note 1.
55. *Plant*, *supra* note 14 at 293 [numbering added].
56. *Ibid*.

impermissible, on grounds that offer the police no basis for deciding whether or not to conduct a similar search in the future.

The second factor in *Plant*, the "nature of the [parties'] relationship," matters particularly when it is a confidential relationship, and again, the police may be incapable of knowing this in advance—and may be unable to tell even after they have acquired the information. Not all communications will necessarily indicate the nature of the relationship between sender and recipient. Evidence on this point may take some time to emerge. Thus, this factor too has limited predictive value for determining the legitimacy of other, apparently similar, searches.

The question of "where the information was obtained" returns us to the spatial considerations discussed in Part II, above . For example, when the information is obtained, without legal authorization, from a claimant's own residence or mobile device, this feature alone will tend to jeopardize the results of the search. The last two factors of the *Plant* test need not detain us for long. As to the "manner of the search," in the cases that concern us here, there is neither a warrant nor a valid exception to the warrant requirement, but let us assume that there is reasonable suspicion to believe that the suspects are co-conspirators, and that the police conduct a limited search aimed only at disclosing information relating to the conspiracy. Whether that reasonable suspicion can amount to legal authority is precisely the question I will address in Part IV. As for the "seriousness of the crime," let us assume provisionally that the crime in question is very serious, and we can modulate that assumption as needed when refining the analysis.

B. MOBILE INFORMATION AND BALANCING

At the outset, I offered a few short examples to show how contingent privacy questions may receive different answers depending on the circumstances,[57] but it will help to provide some more illustrations, and particularly to show more concretely how the answers may depend on considerations that are unavailable to the police at the time of the search. In some of the cases involving electronic communications and privacy, courts have resolved the issue categorically, and have ruled that the claimant had a strong privacy interest because the emails and other messages were collected *en masse* during a sweeping search of the claimant's computer. In these cases, courts have included email and various kinds of online messages in the blend of materials that revealed "biographical core" information about the claimant;[58] however, this has not been taken to mean that email inevitably attracts a strong privacy interest. When courts have been asked more

57. See text accompanying notes 36-40 above.
58. See *e.g. R v Cole*, 2012 SCC 53, [2012] 3 SCR 34.

specifically about the privacy interest in a particular set of emails or messages, acquired through a focused search, the answers have varied.

Thus, for example, in *R v Lowrey*, the accused was charged with "child luring," and the prosecution's case included a series of Facebook messages between the accused and a fourteen-year-old girl.[59] The court offered various reasons for allowing the messages into evidence; one reason was that "there is no proof that the impugned messages expose highly revealing information *about [the claimant]*. At least on the evidence before me, one gains no glimpse into the biographical core of information personal to Lowrey by reading the contents of [the messages]."[60] As this explanation shows, the court undertook to scrutinize the messages, and the analysis turned on details that the police could not have ascertained in advance of the search. It was perhaps only by chance that the messages were not so revealing as to make the court view the matter differently. Indeed, the British Columbia Court of Appeal took the opposite view in *R v Craig*, another "child luring" case involving internet messages, this time on Nexopia, "a social media website used primarily by teenagers."[61] The court observed that the claimant's messages were "personal … [and] they exposed highly intimate details of [his] lifestyle and personal choices. In his discussions … he is flirtatious, discloses aspects of his sexuality, sexual history, drug use, and arranges to provide liquor to underage persons."[62] The court therefore ruled that the claimant's "expectation of privacy in the messages seized by the police was objectively reasonable."[63] The precise content of the messages, then, may play a significant role in determining whether the search was permissible.

---

59. *R v Lowrey*, 2016 ABPC 131, 357 CRR (2d) 76 [*Lowrey*].
60. *Ibid* at para 67.
61. *R v Craig*, 2016 BCCA 154 at para 3, 385 BCAC 229 [*Craig*].
62. *Ibid* at para 139.
63. *Ibid* at para 142. Ultimately, the court ruled that despite the privacy violation, the messages were admissible under section 24(2) (*ibid* at para 197). For other examples of cases in which evidence was excluded because various items, when examined individually, turned out to reveal "biographical core" information, see *e.g. R v Berry*, 2013 BCSC 307 at para 60, 111 WCB (2d) 821 ("The camera may not have contained Mr. Berry's biographical data as such, but it contained video-recordings showing him in private situations or activities"); *R v Grandison*, 2016 BCSC 1712 at para 93, 342 CCC (3d) 249 ("The content of text messages may be perfunctory and routine or it might consist of very sensitive personal information. … [In this case,] [t]he content of the information gathered … reveals 'core biographical information' about the accused"). Compare *R v O(T)*, 2010 ONCJ 334, 90 WCB (2d) 17: "[T]he seized videos and photographs were of a highly personal nature, revealing details of the Applicant's lifestyle" (*ibid* at para 34), but on balance, analysis under s 24(2) counseled in favour of admitting the evidence (*ibid* at para 64).

The *Lowrey* court also considered another factor involving information that is typically unavailable to the police at the time of the search:

> Lowrey does not appear to have taken many practical steps to ensure that no one could view the contents of his Facebook account and, in particular, the content of text messages. He would leave his Facebook account "open" and accessible on his unlocked cell phone, wherever that happened to be from time-to-time.[64]

A court might be satisfied that so long as the claimant had left the account open, and the phone unlocked, at the moment when the police were conducting the search, that would be sufficient to answer this question; however, it can hardly be coincidental that *Lowrey* dwelt on the claimant's usual practice, apparently over an extended period of time, rather than simply considering the details that the police could observe at the time of the search. Often, the police will have no access to that kind of information until the court does—which is to say, long after the impugned search. Consequently, if the claimant's typical behaviour is a significant factor in assessing the privacy interest, the question can rarely be answered until the case comes to a hearing.

The court took a similar view in *R v Beairsto*, ruling that the claimant's text messages were admissible because, among other factors, he had done nothing to ensure that his confederates would guarantee the privacy of his text messages after their receipt. One of the claimant's associates was arrested, and his phone, seized during the arrest, was "open to a … chat" that was "indicative of drug trafficking."[65] This led the police to Beairsto, who was ultimately convicted of trafficking in cocaine. This conviction was possible, in part, because he lacked a privacy interest in the text messages, but the important point here is that the police had no means of telling, in advance, whether he had tried to protect the privacy of his messages, and indeed the police often have no basis for answering that question at the investigative stage. To premise the admissibility of the evidence on that inquiry, then, is effectively to prevent the police from determining whether the search is legally permissible. In *Beairsto*, the court focused in particular on what the claimant knew about the security practices of his associates (very little, as it turned out). Doubtless, the court noted, "a drug dealer would … hope that his text messages concerning drug dealings would be kept in confidence by the recipient," but there was no evidence that Beairsto had ever met either of the recipients in person, or had "had any knowledge of [their] habits, associates or environment." He had no basis for thinking that the recipients would protect

64. *Lowrey*, *supra* note 59 at para 69.
65. *R v Beairsto*, 2016 ABQB 216 at para 11, 37 Alta LR (6th) 379.

"the confidentiality and security of [his] text communications," or that they would keep "others [from] hav[ing] access to his messages."[66] He lacked "any assurances of privacy or confidentiality," but he "[n]evertheless … chose to use a … means of communicating" that was not "secure."[67] Different answers to these questions—involving details that could only come out while the case was being litigated—might have led the court to find a privacy interest, and to rule that the search was impermissible.

One might think that none of these considerations has any continuing significance for the treatment of text messages, because *Marakah* did not take them into account, and thus it implicitly overrules any analysis that draws on them. However, as we have seen, the Court's reasoning relies more heavily on contingent factors than may at first appear, making it hard to predict whether lower courts will simply ignore *Plant* in future cases involving electronic communications. Moreover, where a privacy interest turns on the general tendency of a certain medium to reveal "biographical core" information, courts may be persuaded that if the evidence in contention did not actually reveal such information, the privacy interest was impaired only minimally, and hence, in spite of the *Charter* breach, the evidence is admissible under section 24(2) of the *Charter*. That is how the court proceeded, for instance, in *R v Jarvis*.[68] The accused, a high school teacher, was charged with criminal voyeurism because he had used a pen camera to make surreptitious video images of female students during gym class. The Ontario Superior Court of Justice ruled that he had a privacy interest in the pen camera because the kind of information such a device contains "may relate to aspects of life that are deeply personal."[69] In the event at issue, however, it turned out

66. *Ibid* at para 46.
67. *Ibid*.
68. 2014 ONSC 1801, 113 WCB (2d) 740 [*Jarvis* (2014)]. The accused was acquitted at trial (see *R v Jarvis*, 2015 ONSC 6813, 25 CR (7th) 330) and the acquittal was affirmed on appeal by a split bench (see *R v Jarvis*, 2017 ONCA 778, 41 CR (7th) 36). The case is now on appeal as of right to the Supreme Court of Canada (Docket No 37833, notice of appeal filed 8 November 2017). The issues in dispute, however, relate to the substantive grounds for determining whether the accused was guilty of voyeurism, as defined in the *Criminal Code*, not the admissibility of the video recordings.
69. *Jarvis* (2014), *supra* note 68 at para 57 quoting *Buhay*, *supra* note 20 at para 24.

that his device "did not contain any personal biographical data."[70] Consequently the police had not seriously infringed on his privacy rights, and the recordings were admissible in court. So long as generally private types of information may be admissible just if the particular examples turn out to rate low on the *Plant* or *Edwards* test, all of the potentially relevant factors from those decisions come back into play—as a means of ruling on the strength, rather than the existence of a privacy interest, and therefore on the admissibility of the evidence. Practically speaking, it makes little difference at which stage of the analysis these factors come into play, because so long as they operate in this fashion, the basic question about how they bear on the legitimacy of a given search, from an *ex ante* point of view, remains the same.

As we have seen, the first two factors of the *Plant* test can make it difficult for police to tell whether they may legitimately undertake a particular search. If we reflect more generally on the results in *Lowrey* and *Beairsto*, however, they can suggest an approach that would help the police to decide whether or not to proceed. In most cases involving conspiracies to sell drugs, firearms, and similar contraband, there is good reason to doubt that the communications among the conspirators would include "biographical core" information. Again, even if the conspirators took some pains to assure each other that they would protect the confidentiality of their communications, that can hardly be a reason for the courts to ascribe a heightened privacy interest to the messages. If the police can show objectively that they have reasonable suspicion to believe that the claimants were conspiring in this fashion, they should be allowed to presume that the claimants had only a basic privacy interest in their communications, and on that basis, the police should be entitled to obtain the relevant text messages (and only those messages). Where that reasonable suspicion is well supported,

70. *Jarvis* (2014), *supra* note 68 at para 93. For similar examples, see *e.g. R v Moldovan*, 85 WCB (2d) 203, [2009] OJ No 4442 (QL) at paras 177-78 (Sup Ct) (impact of *Charter* breach was minimal, even though police lacked authorization to intercept phone conversation, because "the state did not intercept anything of a personal nature … On the contrary, as it happens, the police intercepted only conversations in which the very criminality they were investigating was being discussed" at para 177); *R v Robertson*, 2017 BCSC 965 at paras 78-79, [2017] BCWLD 3946 (impact of *Charter* breach was "minor," even though police "fail[ed] to properly execute the entry pursuant to the knock and announce rule," because, among other reasons, it turned out that the items seized were "not particularly personal or private"); *R v Clarke*, 2016 ONSC 351 at paras 135-36, 129 WCB (2d) 377 (impact of *Charter* breach was "not … on the more serious end of the spectrum," even though bank records were acquired pursuant to deficient production order, because although "[b]ank records contain personal financial information," the material seized did not reveal information about "the most private domains" of the accused's life).

any invasion of a privacy interest is minimal, as in *Jarvis*. Moreover, given that *Plant* refers to the seriousness of the crime as well as the other considerations discussed here, the gravity of an offence such as conspiring to sell firearms might even be sufficient to overcome some factors that would enhance the privacy of one's communications. In that case, even when the conspirators have disclosed biographically significant details or are siblings in a "crime family" jointly engaged in a conspiracy, these considerations may be insufficient to render the fruits of the search inadmissible. By ruling on this point, a court could further enhance the predictability of the analysis, educating the police and public more clearly as to how these considerations will bear on the legitimacy of a search.

C. THE ARGUMENT FROM CONTROL

We have seen that when courts refer to *Plant*, the analysis tends to be individuated, and the predictive value of any given decision is limited. However, some courts have given little heed to *Plant*, drawing primarily on *Edwards* and therefore reaching categorical conclusions. The Court sought to take this approach in *Marakah*, with limited success. With respect to text messages, a significant part of the debate has turned on the fifth *Edwards* factor—"the ability to regulate access." This consideration played a significant role in the lower court judgment that *Marakah* reversed, and also in the reasons of the dissenting opinion of the Court in *Marakah*. That logic also informs the dissent in *R v Pelucco*, a judgment by the British Columbia Court of Appeal addressing the same problem.[71] The analyses in all three decisions are worth considering, because the majority in *Marakah* did not rebut this argument, leaving the impression that it still has some persuasive force if the prosecution can demonstrate that the accused lost control over the text messages. As I will show, this argument cannot withstand close scrutiny.

The *Marakah* dissent offers what is perhaps a more elliptical version of the "loss of control" argument than some other courts have furnished. Justice Moldaver, in his dissent, explains that "a reasonable expectation of personal privacy requires some measure of control over the subject matter of the search,"[72] and that "[c]ontrol distinguishes a *personal desire* for privacy from a *reasonable expectation* of privacy."[73] Citing *Duarte*'s definition of privacy as "the right of … individual[s] to determine for [themselves] when, how, and to what extent [they] will release personal information," Justice Moldaver reasons that once a

71. *Pelucco*, *supra* note 11.
72. *Marakah*, *supra* note 1 at para 113 (Moldaver J, dissenting).
73. *Ibid* at para 119 [emphasis in original].

person loses control over some piece of information, it "change[s] from private to public in nature."[74] The recipient, he observes, has "complete autonomy" over the information,[75] except when, by statute or at common law, the recipient has "a qualified obligation … to maintain confidentiality over personal information [which] provides a measure of constructive control which can support a reasonable expectation of privacy."[76] On this view, the inability to regulate access and the condition of being public are so closely linked that little more need be said about why the former entails the latter. The analysis turns only briefly to the results that follow from lack of control: "The risk that a recipient may repeat what was said during a conversation, or share his or her record of the conversation with others, is a risk that individuals must reasonably assume, and thus may defeat a reasonable expectation of privacy."[77] On this view, whatever cannot be controlled is subject to a risk of being shared, and the very possibility of that risk is the feature that changes the nature of the information.

Marakah reversed a judgment by a split bench of the Court of Appeal for Ontario, and in examining the relation between privacy and control, the majority on that court relied heavily on the *Pelucco* dissent. Indeed, in elaborating its reasoning, the court quoted approvingly, and at length, from the *Pelucco* dissent:

> [W]here a … message reaches its intended recipient, the autonomy interest underlying our s. 8 understanding of privacy is fully realized (see e.g., *Hunter v. Southam* at 159, *R. v. Plant*, [1993] 3 S.C.R. 281 at 293, and *Tessling* at para. 63).
>
> A person who—without any guarantee of confidentiality or indication from the recipient that the message will be kept confidential—communicates information has made an autonomous choice (i.e., determined for himself or herself) [to] who[m], how and to what extent to communicate information to the fullest extent possible. Any further claim against a recipient is a claim that the sender can then determine [to] who[m], how and to what extent the recipient will communicate information to further third parties, which interferes with the recipient's notional sphere of personal autonomy.[78]

---

74. *Ibid* at para 125 citing *R v Duarte*, [1990] 1 SCR 30 at 46, 65 DLR (4th) 240 [*Duarte*].
75. *Marakah*, *supra* note 1 at paras 99, 145.
76. *Ibid* at para 141. This includes, but is not limited to, a relationship with "a lawyer, doctor, psychiatrist or another professional who owes a duty of confidentiality or trust to the claimant," or a regulated entity that is subject to statutory privacy protection (*ibid* at para 137).
77. *Ibid* at para 129.
78. *Marakah*, ONCA, *supra* note 3 at para 78 quoting *Pelucco*, *supra* note 11 at paras 115, 118 (Goepel JA dissenting).

It is usually wise, when encountering block quotations of this length, to skip over them and proceed to the text, but I urge the reader to review the quoted language, because it furnishes the fullest justification yet offered in Canadian jurisprudence as a principled rationale for the termination of the sender's privacy interest on receipt of the message, and as will become evident, the justification rapidly crumbles upon scrutiny.

First, the "loss of control" argument control proves too much. If the inability to control the recipient was sufficient by itself to terminate the sender's privacy interest, it would follow that no one has a reasonable expectation of privacy in a letter or an email, once it has been delivered, and hence that all forms of written correspondence, as a general matter, are freely available to the police on a warrantless basis—because where there is no privacy interest, the police have no need to articulate any justification for search or seizure. Analogously, if someone had a phone that automatically recorded each incoming call, the recording would also be freely available to the police, and could be used in evidence against the caller, even if the police acquired it without any justification. This view finds no support in Canadian jurisprudence. When courts have considered the privacy interest attaching to letters, the question has usually involved correspondence sent by prison inmates, whose privacy interests are diminished to such a point that their letters may be intercepted in transit.[79]

The *Pelucco* dissent cited US jurisprudence to indicate that US courts have indeed taken this view, speaking of the "American rationale that a letter's author does not have a reasonable expectation of privacy [after it has been delivered]."[80] But US courts do not routinely admit letters obtained during police searches that were conducted without either a warrant or a recognized exception to the warrant requirement. Although a number of US courts have asserted this view, in nearly every instance the police acquired the letter either by means of a lawful search or from a third party who voluntarily turned the letter over to law enforcement

79. See *e.g. R v Ballantyne*, 2008 BCSC 1566 at paras 32, 88, [2009] BCWLD 5161 ("Various cases deal with the effect that prisoners in correctional institutions, whether they be on remand or serving a sentence, have a greatly reduced objective expectation of privacy," holding that "Mr. Ballantyne had no reasonable expectation of privacy in the correspondence he mailed from the Winnipeg Remand Centre" at paras 32, 88); *R v Stevens*, 2001 ABQB 340 at paras 35-36, 291 AR 40: "[T]he [two] accused … knew that their letters were being screened or knew there was a substantial and serious risk that the letters were being screened" (*ibid* at para 35). As such, "there existed no reasonable expectation of privacy with respect to the correspondence between [the two accused]" (*ibid* at para 36).

80. *Pelucco*, *supra* note 11 at para 112 (Goepel JA dissenting) citing *Ray v United States*, 658 F (2d) 608 at 610 (8th Cir 1981) [*Ray*], *United States v Hubbard*, 493 F Supp 209 (DDC 1979) [*Hubbard*]. See also *supra* note 81.

officials.[81] These settings do not involve an unauthorized search. Once we set those cases aside, not even a handful of cases remain—and their facts are so ambiguous that they offer only weak support for the conclusion being urged.[82] The "loss of control" argument, according to the very terms in which the *Marakah* and *Pelucco* dissents explain it, would eliminate the privacy interest in most forms of written communication. The existing Canadian and US jurisprudence does not warrant such an extreme view.

Second, the *Pelucco* dissent strives unpersuasively to explain its position by appealing to the sender's "autonomy interest," which is asserted to be "fully realized" on the letter's receipt, such that any further constraint would "interfer[e]

---

81. In those instances, the third parties were individuals, not entities such as banks or internet service providers. For example, in *United States v King*, 55 F (3d) 1193 (6th Cir 1995), the letters came to light because the recipient "asked [the FBI agent investing the case] to remove some items from her apartment" (*ibid* at 1195), and these included "[a] suitcase containing fifty-one letters" from the defendant to the recipient (*ibid* at 1194).

82. According to the leading American treatise on the law of search and seizure by Wayne R LaFave, "[t]he standing of the sender … terminates once delivery of the goods has been made." LaFave cites nine cases to support this view, many of which expressly assert this very proposition; however, in eight of the nine cases, a third party turned the letter over to the police, or the letter was the subject of a valid search warrant, or was in plain view during a validly executed search, or was obtained during a search pursuant to arrest. Wayne R LaFave, *Search and Seizure: A Treatise on the Fourth Amendment*, 5th ed, §11.3(f) (2016). In the ninth case, *State v Kenny*, 224 Neb 638 (1987) [*Kenny*], the Nebraska Supreme Court upheld a conviction that depended, in part, on the prosecution's use of a letter written by the defendant and obtained through a search that was not supported by probable cause or any exception to the probable cause requirement (although the facts suggest that the search may have been supported by reasonable suspicion). Even assuming that there was no articulable basis at all for the search in *Kenny*, this forty-year old decision by a state court can hardly be considered sufficient, by itself, to establish the point in question. One may suspect that the leading treatise in this area would have included more cases not only asserting the proposition, but also applying it, if they were available to be found. The two US authorities cited in the *Pelucco* dissent (see *Pelucco*, *supra* note 11 at para 112 citing *Hubbard*, *supra* note 80, and *Ray*, *supra* note 80) also offer little support. In *Hubbard*, the court observed that the letters in question had been made "available to numerous third parties" (*Hubbard*, *supra* note 80 at 214). Where the recipient has actually shared the information with "numerous" others, one need not speculate about how the privacy interest *could* terminate; by her own actions, the recipient has *in fact* terminated it by making the information public. *Ray* offers no independent analysis of the privacy issue, and instead depends entirely on *Hubbard*. Moreover, *Ray* frames the inquiry in terms of standing, rather than inquiring into the defendant's privacy interest in the letters that the search disclosed: the court was content simply to observe that the defendant "lacks standing to contest the alleged search of [a third party's] hotel room" (*Ray*, *supra* note 80 at 611). In neither case, then, did the mere supposition of what the recipient *might* do explain why the sender had no privacy interest in a letter.

with the recipient's notional sphere of personal autonomy."[83] This argument appears fleetingly in the *Marakah* dissent, when Justice Moldaver refers to the recipient's "autonomy," which, by implication, comes to the fore just when the sender's autonomy terminates.[84] For this proposition, *Pelucco* cites *Hunter*, *Plant*, and *Tessling*,[85] but those cases provide no help; in fact, they undermine the contention. *Hunter*, in the relevant passage, does not use the term *autonomy*, but does speak of the "right of privacy, which is the right to be secure against encroachment against the citizens' reasonable expectation of privacy in a free and democratic society."[86] The relevant passage in *Plant* speaks of "the underlying values of dignity, integrity, and autonomy"—values which the *Charter* recognizes by "protect[ing] a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state."[87] *Tessling*, in the cited paragraph, states that a heat pattern emanating from a residence "offers no insight into [the residents'] private life, and reveals nothing of [their] 'biographical core of personal information.' Its disclosure scarcely affects the 'dignity, integrity and autonomy' of the person whose house is subject of the FLIR image."[88]

As these quotations show, the case law speaks not of autonomy alone, but of dignity and integrity as well. Moreover, the proposition about the expiry of the autonomy interest is simply *Pelucco*'s interpretation, unsupported by any language in the three cited cases. The dissents in *Pelucco* and *Marakah* gloss over the question of whether one's interests in dignity and integrity also expire on receipt of the message, and it cannot go without saying that these interests would vanish so readily; if anything, the latter are more enduring than autonomy in these circumstances. Even if we focus solely on autonomy, however, it is hard to see how that interest can be said to "disappear" once a message has been delivered. Again, it must be emphasized that we are discussing the right of individuals "to be secure against encroachment … in a free and democratic society," and the right of individuals, in such a society, to protect information "from dissemination by the state." The question of whether the *recipient* may share a message, in such a society, should not be readily and casually conflated with the question of how

83. *Marakah*, ONCA, *supra* note 3 at para 78 quoting *Pelucco*, *supra* note 11 at para 118 (Goepel JA dissenting). One may wish to stress the word *notional*, because it reveals one of the weakest aspects of this analysis.
84. See *supra* note 74.
85. See note 78 and the accompanying text above.
86. *Hunter*, *supra* note 14 at 159.
87. *Plant*, *supra* note 14 at 293.
88. *Tessling*, *supra* note 21 at para 63.

that potential result bears on what the *state* may legitimately do, particularly if the recipient has not in fact done anything, but suffers only a "notional" harm to a theoretically postulated "sphere of personal autonomy" in a thought experiment about the use of the message.

Consider a society in which text messages (to say nothing of emails and letters) are open to police surveillance, which is achieved by collecting them from the recipient, so that any given text message is subject to "dissemination by the state," as *Plant* put it. Can anyone doubt that this practice would significantly undermine people's autonomy, and that people would hesitate before sending any message, because of their uncertainty about its ultimate destination and use? The most basic conception of "privacy in a free and democratic society" has to assume that communications are not presumptively available to the police without any articulable justification, yet this is what the "loss of control" argument seeks to prove.

As noted at the outset, when a reasonable expectation of privacy is lacking, the police may search on a warrantless and groundless basis. The sender's lack of control may be a *relevant* consideration in evaluating the privacy interest in written communications, but to make it *determinative* would undermine precisely the values that *Hunter*, *Plant*, and *Tessling* (among other decisions) seek to advance by limiting the government's powers of search and seizure. One need only consider the question briefly to see that all of the interests at stake in the privacy jurisprudence, including autonomy, would be significantly compromised under the "loss of control" theory.

D. THE CONTROL THEORY AND THE THIRD-PARTY DOCTRINE

How did the confusion at the heart of the "loss of control" theory arise? Reduced to its basic form, the theory assumes that because the recipient *may* share a message with anyone else, the sender's autonomy interest *necessarily* expires where the recipient's interest begins, and so the police are entitled to have access to the message without having to specify any articulable grounds. Yet one of the most fundamental principles of the law of search and seizure—and of constitutional law generally—is that restrictions on state power do not apply to private

individuals.[89] Individuals may engage in all kinds of conduct that is forbidden to the state. It seems odd, then, to conclude that an *individual's* ability to disseminate someone else's message (or email, or letter) automatically entitles the *state* to do the same thing. The conclusion does not seem so odd, however, once we realize that, in the law of search and seizure, the "public exposure" doctrine and its cognates have blurred part of the distinction between individual and state action. Items exposed to public view (*e.g.*, atop a dashboard, visible in an unzipped backpack on the subway, posted on a freely available electronic bulletin board) are treated as open to the public and *therefore* open to police inspection.[90] Precisely because any random member of the public might happen to see it, the police may also view it without having to articulate any basis for looking at it—without reasonable and probable grounds or reasonable suspicion. It matters not whether anyone except the police officer *has* seen it, so long as it is publicly observable. By extension, the same logic applies to records of public transactions. For instance, if the owner of a convenience store videotapes activities within the store or passers-by on the sidewalk, the police are not required to articulate any grounds for obtaining the video to use it in an investigation, because what it records is public activity: Any random member of the public may observe it, and so the actor has no privacy right in the publicly observable part of the transaction.[91] Criminal investigations often proceed by collecting information that is available to be seen by others, and hence is "public" in this sense.

Up to this point, the connection between what a person does in public and what the police may acquire, on a warrantless and groundless basis, may seem perfectly sensible. In what is known as the "third-party doctrine," this idea has been taken one step further, and treats many transactions as public even though

---

89. See *Canadian Charter of Rights and Freedoms*, s 32(1), Part I of the *Constitution Act, 1982* being Schedule B to the *Canada Act 1982* (UK), 1982, c 11. Section 32(1) of the *Charter* states that it applies:

> (a) to the Parliament and government of Canada in respect of all matters within the authority of Parliament including all matters relating to the Yukon Territory and Northwest Territories; and
>
> (b) to the legislature and government of each province in respect of all matters within the authority of the legislature of each province.

See also *McKinney v University of Guelph*, [1990] 3 SCR 229 at 262, 76 DLR (4th) 545; *R v Dell*, 2005 ABCA 246 at para 6, 256 DLR (4th) 271 ("the *Charter* only applies to government actions, not interactions between private citizens") citing *Schreiber v Canada (Attorney General)*, [1998] 1 SCR 841 at para 27, 158 DLR (4th) 577.

90. See *supra* notes 29, 40.

91. See note 29 and the accompanying text above.

they are not observable in the same way as in the examples above. In the version adopted by the US courts, information available to *any* third party, even one acting in a quasi-fiduciary capacity (*e.g.*, a bank or phone company), is deemed "public" and so is freely available to the police according to the same logic.[92] But although a deposit includes details shared with bank personnel, it can hardly sustain the same analogy to "public exposure" as a transaction in a convenience store. The mistake, then, is to conclude that whatever an individual shares with *anyone* else should be treated as public. Notably, no one has offered a normative argument in favour of the third-party doctrine; on the contrary the normative arguments all cut the other way.[93]

The confusion underlying the "loss of control" theory is a product of this tacit and misguided logic. Just because *many* transactions visible to third parties are public, it does not follow that *all* such transactions are public. Although it is permissible for the recipient of a text message to forward it to others, the mere possibility of that eventuality does not render the message "public" in the same way that a purchase at a convenience store is public. When activity or information is not exposed to the public, we should recall the constitutional difference between restrictions on state action and on the action of private individuals, instead of blithely assuming that whatever some individual *might* do, the state may immediately proceed to do, even when the individual has actually done nothing. When the recipient of a message *in fact* makes it public, even without the sender's permission (*e.g.*, by posting a text message online), the logic of the "public exposure" doctrine applies; it hardly makes sense to ask the police to avert their gaze from a message that everyone else can observe.[94] The sender may well perceive it as a betrayal of confidence, just as a police informer may

92. Kiel Brennan-Marquez, "Fourth Amendment Fiduciaries" (2015) 84:2 Fordham L Rev 611.
93. See *e.g.* Susan Freiwald, "First Principles of Communications Privacy" (2007) [2007] Stan Tech L Rev 3; Stephen E Henderson, "Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too" (2007) 34:4 Pepp L Rev 975; Susan W Brenner & Leo L Clarke, "Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data" (2006) 14:1 JL & Pol'y 211; Gerald G Ashdown, "The Fourth Amendment and the 'Legitimate Expectation of Privacy'" (1981) 34:5 Vand L Rev 1289 at 1315; Lewis R Katz, "In Search of a Fourth Amendment for the Twenty-first Century" (1990) 65:3 Ind LJ 549 at 564–66. One of the few efforts to defend the third-party doctrine on any ground is Orin S Kerr, "The Case for the Third-Party Doctrine" (2008) 107:4 Mich L Rev 561. However, Kerr offers a descriptive account, not a normative one, and the factors that go into his description are themselves difficult to pin down. See Simon Stern, "The Third Party Doctrine and the Third Person" (2011) 16:3 New Crim L Rev 364.
94. See *Hubbard*, *supra* note 80. This is precisely why *Hubbard* does not support the "loss of control" that the *Pelucco* dissent attributed to it.

betray the confidence of her former associates—but in both cases, this personal betrayal does not translate into a constitutional privacy violation. However, when no such action has occurred, and the courts are left instead to hypothesize that the recipient *might yet* post the message, and that consequently it is *already* exposed to the public. The result is to expand the meaning of "public" beyond any plausible bounds.

The "loss of control" theory, then, yields a qualified version of the third-party doctrine—a doctrine which the Supreme Court of Canada has rejected.[95] More precisely, in *R v Duarte* the Court rejected a specific version of the third-party doctrine, which holds that by sharing information with someone else, an individual takes the risk that the other person "will make a permanent electronic record … at the behest of the state."[96] The "loss of control" theory proceeds along similar but not identical lines, reasoning that when information is conveyed to another, and the sender has no legal grounds (deriving from a statute or a recognized relationship of confidentiality) for controlling the recipient, the information automatically loses its privacy protection, precisely because of the sender's lack of control. The US version of the doctrine cuts even more widely because it pays less heed to the legal conditions restricting the recipient's actions, and treats customers' interactions with banks and credit card issuers as similarly open to police search on a warrantless basis.[97]

The slightly less draconian implications of the qualified version may therefore seem more acceptable, but it remains inconsistent with Canadian jurisprudence, and it becomes even more obviously untenable when its dimensions are fully delineated. It is also worth noting that despite their similar effect, the grounds of the third-party doctrine and the "loss of control theory" are somewhat different: The US version reflects the idea that what has been revealed to another is thereby rendered public—and therefore should be analogized to "public exposure" once it has been shared. The version set out in the *Marakah* dissent assumes that control is a *sine qua non* for privacy—and consequently that when information can be shared *and* controlled (*e.g.*, when it is shared with a regulated entity that has certain obligations of confidentiality), it attracts a privacy interest that the US

95. See *e.g. R v Ward*, 2012 ONCA 660 at para 76, 112 OR (3d) 321 ("Canadian jurisprudence has emphatically rejected the 'risk' analysis featured in American Fourth Amendment jurisprudence … According to that jurisprudence, voluntary disclosure to third parties defeats Fourth Amendment claims") citing *Duarte*, *supra* note 74 at 48 and *R v Wong* (1987), 1 WCB (2d) 415 at para 45, 19 OAC 365 as examples of such Canadian jurisprudence.

96. *Duarte*, *supra* note 74 at 42.

97. See *e.g. United States v Miller*, 425 US 435 at 440-44, 446 (1976) (banks); *United States v Phibbs*, 999 F (2d) 1053 at 1077-78 (6th Cir 1993) (credit cards).

version of the doctrine would not support.[98] Although neither doctrine has found much normative justification, this difference means that the normative critiques of the US doctrine do not map readily onto the Canadian version, as I seek to show in the next Part.

IV. THE PRIVACY INTEREST

If the "loss of control" theory proves unavailing as a ground for vitiating any privacy interest in text messages, what kind of privacy protection should they enjoy? On this question, the *Marakah* majority offers a persuasive answer, but offers no normative justification. If we return to the values whose importance has been reiterated throughout the privacy jurisprudence—autonomy, dignity, and integrity—it is evident that written communications, as a general matter, engage all three interests, even when they are not somehow marked out as especially private, or sent to fiduciaries or quasi-fiduciaries. In this Part, I attempt to provide that normative justification, and show why reasonable suspicion is enough to overcome the privacy interest, when the police can offer objective grounds for suspecting that particular individuals are involved in a criminal conspiracy.

E. THE OBJECTIVE REQUIREMENT

In spite of the many factors animating the various tests on offer, analyses of privacy often turn in the end on the question of whether a claimant's expectation of privacy was "objectively reasonable." As the courts have explained, an "objectively reasonable expectation of privacy" is one that "society is prepared to recognize as reasonable,"[99] and it refers to "a normative rather than a descriptive standard."[100] This is not the place for an extended discussion of the difference between the normative and the descriptive, but it is worth noting, in passing, that for this kind of inquiry, empirical evidence is useful only insofar as it bears on norms, or allows us to infer norms from practices. To content oneself with a list of practices and the beliefs underlying them, as courts often do, reveals nothing about norms because people often regard certain practices or attitudes as commonplace, while also viewing them as normatively objectionable. Therefore, empirical evidence, drawn from practices, may not be very helpful in showing what society is prepared to recognize as reasonable.

---

98. See *supra* note 76. Under the US third-party doctrine, the information shared with these entities is not entitled to constitutional privacy protection.
99. *R v M(A)*, *supra* note 13 at para 33.
100. *Tessling*, *supra* note 21 at para 42.

If we pursue the analogies to letters and conversations, proposed earlier, it is evident that the same normative logic governs all of these forms of communication. A conversation on a park bench or on a public street, no matter how private the topic, merits little protection if it is loud enough to be overheard by a police officer strolling by; society would not be prepared to recognize the interlocutors' expectation of privacy as reasonable. The same is true for a text message that the recipient displays in public (even though the sender forbade it). To be sure, electronic forms of communication are likelier than paper-and-ink correspondence to be widely distributed, or to become publicly visible. But when neither the sender nor the recipient has actually done anything to make a text message available to others, society is prepared to recognize the sender's expectation of privacy as reasonable.

No detailed empirical research or philosophical theory is required to see this because the analogy to other forms of written communication readily shows why the expectation is objectively reasonable. One need only turn to the history of the Fourth Amendment in the United States to see why a belief in the privacy of written communications is objectively reasonable, as a general matter. As every historian of criminal procedure knows, the provisions of the Fourth Amendment (and thus, ultimately, of section 8 of the *Charter* in turn) were prompted in large part by hostility towards the British use of "general warrants"—open search warrants, naming no individual in particular, that allowed government "messengers" to search the homes and offices of anyone they chose, and to seize whatever they found. More specifically, the Fourth Amendment was a response to the use of general warrants during the investigation of John Wilkes and his associates for their involvement in *The North Briton* in 1763.[101] General warrants were objectionable because of the indiscriminate searches that they licensed, and letters were among the many documents that government agents collected, during these searches. In the course of the Wilkes investigation, one of the messengers ransacked the home of the bookseller George Kearsley, "prob[ing] every bureau and drawer in his house, [and] confiscat[ing] his account books, letters, and notes at will,"[102] seeking correspondence from Wilkes. In one of the lawsuits that followed, it was alleged that the messengers had "examined all the private papers, books, letters and correspondence of the plaintiff and his clients."[103]

---

101. See *e.g.* Laura K Donohue, "The Original Fourth Amendment" (2016) 83:3 U Chicago L Rev 1181.
102. William John Cuddihy, *The Fourth Amendment: Origins and Original Meaning, 1602-1791* (Oxford: Oxford University Press, 2009) at 441.
103. *Beardmore v Carrington* (1764), 2 Wils KB 244, 95 ER 790.

Anger about these large-scale searches led to the adoption of a constitutional prohibition on unreasonable searches that violate "[t]he right of the people to be secure in their persons, houses, papers, and effects."[104] The generality of the general warrants was the most important reason for adopting this measure, and by referring specifically to "papers" and "effects," this language makes it clear that its protections extend to letters.

One consequence of a theory that treats text messages and letters in the same fashion would be to eliminate some of the contingency we have seen in the analysis in *Marakah*. Recall that according to the majority in *Marakah*, text messages attract a privacy interest just when they are composed in a fashion that creates a "zone of privacy"—that is, when they are shielded from others' eyes.[105] In the case of a letter, anyone who happened to observe the process of its composition would be free to tell others about it, including the police—but it would not follow that if the police conducted a warrantless and groundless search that happened to yield that letter, they would be free to use it in court. *Marakah*'s treatment of the "zone of privacy," however, seems to yield precisely that result for text messages. Again, the author of a letter often has no control at all over what the recipient does with it—and yet the sender's inability to regulate access to the information has little bearing on the privacy interest that attaches to it. By contrast, *Marakah* secures protection for text messages only when there is "shared control," leaving open the implication that text messages do not necessarily enjoy *Charter* protection when such control is shown to be absent. In short, a theory that looks to the social interests in protecting written correspondence, as a general matter, would result in a more categorical form of protection for text messages, eliminating some of the contingency that the reasoning in *Marakah* allows.

But even if the person who sends a text message has a reasonable expectation of privacy, it does not follow that the police can have access to the text message only when they are executing a warrant that expressly places it within the ambit of the search. Generally, when the police receive evidence from someone who has lawful possession or custody of it, and who is not under any statutory obligation to withhold it, section 8 of the *Charter* does not apply, because there has been no "search" within the meaning of section 8. As the Court explained in *R v Law*, "[t]he principal purpose of s. 8 of the *Charter* is to protect an accused's privacy interests against unreasonable intrusion *by the State*."[106] Similarly, in *R v Gomboc*, the Court contrasted "the voluntary cooperation of a private

104. US Const amend IV.
105. *Marakah*, *supra* note 1 at para 37.
106. *R v Law*, 2002 SCC 10 at para 15, [2002] 1 SCR 227 [emphasis added].

actor with the police" against a request, by police, that an electric utility install a device to record a consumer's power usage.[107] The latter, the Court explained, "constitute[d] a search that infringes s. 8 of the *Charter*."[108] The thrust of these statements is to show that a "search" is precisely analogous to a "seizure," within the meaning of section 8. In *R v Colarusso*, the Court defined a seizure as "the taking of something from a person *by a public authority* without that person's consent."[109] It is the act of a public authority that makes the appropriation a seizure. Consequently, as various courts have held, when someone "obtain[s] … personal information … as a private citizen" and "provide[s] the information … of her own volition" to a state actor, there has been no seizure.[110] Analogously, when a private individual voluntarily provides a letter or a text message to the police, there has been no search. In that case, the state has not intruded on the claimant's privacy interests, and therefore even a heightened privacy interest in the communication will not help to justify its exclusion.

This much may seem obvious in the context of letters and emails that a recipient voluntarily gives to the police; however, courts have sometimes devoted a significant amount of unnecessary space to the analysis of privacy interests in such cases. In *Lowrey* (one of the "child luring" cases), the child's mother contacted the police to report the incident, and the mother and daughter then met with police, to whom they "provided … a printed copy of the 'messages' exchanged" in the course of the online conversations between the child and the claimant.[111] Similarly, in *Craig* (another "child luring" case), the recipients furnished the police with the messages exchanged. As the court noted, "[t]he messages [used in evidence] were all from the [social media] accounts of … the witnesses,"[112] namely, the child whom the claimant had been messaging and her two friends, who "printed off" the messages themselves and gave them to the police.[113] Again, in *R v Sandhu*, the complainant showed the police threatening text messages he had received from the accused, and the trial court inquired into the sender's expectation of privacy.[114] This approach is misguided. The objective reasonableness

107. *R v Gomboc*, 2010 SCC 55 at para 104, [2010] 3 SCR 211.
108. *Ibid*.
109. *R v Colarusso*, [1994] 1 SCR 20 at 58, 110 DLR (4th) 297 [*Colarusso*] [emphasis added] citing *R v Dyment*, [1988] 2 SCR 417 at 431, 55 DLR (4th) 503.
110. *R v McBean*, 2011 ONSC 878 at para 19, 92 WCB (2d) 878 citing *Colarusso*, *supra* note 109.
111. *Lowrey*, *supra* note 59 at para 9.
112. *Craig*, *supra* note 61 at para 42
113. *Ibid* at paras 8-9, 45.
114. *R v Sandhu*, 2014 BCSC 2482, [2015] BCWLD 1274.

of the sender's expectations has no bearing on the analysis, because the police acquired the information through a voluntary act of the recipient. In *Sandhu*, as in *Lowrey* and *Craig*, section 8 was never triggered.

Although it is not tenable to say that the sender's privacy interest vanishes because of what the recipient *might* do with a piece of correspondence, it is a very different matter when the recipient in fact shares it with others. That is precisely why the "loss of control" argument has a superficial appeal: It correctly describes what happens if the recipient actually decides to make the communication available to others. If the recipient of a letter turns it over to the police, the sender's privacy interest has no bearing on the letter's admissibility. There is no reason to treat text messages differently.

Similarly, privacy interests are irrelevant when the police acquire evidence in the course of a lawful search, such as a search incident to arrest. When evidence is properly within the scope of such a search, its admissibility is not in question even if the claimant can make out a heightened privacy interest. The proper scope of a search incident to arrest has, of course, been vigorously debated, particularly with respect to electronic communications, and it is important to stress that the search must be narrowly tailored to meet only the purposes justifying such a search, which include "collect[ing] and preserv[ing] evidence located at the site of the arrest"[115] so long as the evidence is not "in … danger of disappearing."[116] In *R v Fearon*, the Court noted that searches of cell phones, incident to arrest, "may serve important law enforcement objectives" such as "identifying accomplices or locating and preserving evidence that might otherwise be lost or destroyed."[117] In such cases, the Court explained, the search should be limited to "recently sent or drafted emails, texts, photos and the call log … as in most cases only those sorts of items will have the necessary link to the purposes for which prompt examination of the device is permitted."[118] Within that properly defined scope, a showing of a heightened privacy interest as to a certain item makes no difference. When the police conduct a search that is a valid exception to the warrant requirement, and they do not stray outside the permissible scope of the search, any evidence they collect is admissible, whether it is a bus transfer or a personal diary. *Fearon* notes that email and text messages could fall within the scope of the search,[119] and to

115. *R v Stillman*, [1997] 1 SCR 607 at para 48, 144 DLR (4th) 193.
116. *Ibid* at para 49.
117. *R v Fearon*, *supra* note 20 at para 49.
118. *Ibid* at para 76.
119. *Ibid*.

recognize that is to see that even if a particular text message carried a high privacy interest, that would not be a reason for excluding it.

To say, then, that individuals have an objectively reasonable expectation of privacy in letters, emails, and text messages, as a general matter, does not insulate these materials from inspection by the police, even when a warrant is lacking. If the recipient voluntarily turns it over to the police, or if the correspondence comes into view during a search pursuant to arrest, for example, the claimant's privacy interest does not require the suppression of this evidence. The same logic should apply when the police have reasonable suspicion to search for the particular communication in question, as I show in the next Part.

F. REASONABLE SUSPICION

In cases involving the privacy of text messages, the police often discover the incriminating information in the course of a search that was supported by reasonable suspicion, though not by grounds sufficient for a warrant. While that standard cannot justify a wide-ranging search of every message on a suspect's phone, or even all the recent messages, it can support a narrowly targeted search aimed solely at obtaining messages relevant to a crime for which the police are investigating the suspect. Allowing a relatively narrow search of this kind would go a long way towards answering the concerns of the dissent in *Marakah*, which suggested that the majority's "all-encompassing approach" would result in the exclusion of text messages from "a sexual predator who lures a child into committing sexual acts" and "an abusive husband who sends harassing text messages to his ex-wife."[120] In these instances, one may doubt that any search at all has occurred if the recipient chooses to turn over the incriminating information rather than producing it at the behest of the police, but even if these were treated as searches under section 8, the recipient's complaint would be sufficient to create reasonable suspicion as to the messages.

That was precisely the position that the Court adopted in *R v Chehil*, which explained that a search of the claimant's luggage, performed by a sniffer dog that alerted to the presence of drugs, and supported by reasonable suspicion, was "authorized by law."[121] The Court noted that such searches are "minimally intrusive, narrowly targeted, and can be highly accurate," and therefore they "may be conducted without prior judicial authorization."[122] For the search to be legally permissible, there must be a "nexus … between the criminal conduct that is suspected and the investigative technique employed"—a requirement that

120. *Marakah*, *supra* note 1 at para 168 (Moldaver J, dissenting).
121. *Chehil*, *supra* note 16 at para 1.
122. *Ibid*.

was satisfied in *Chehil* by "a constellation of facts that reasonably support[ed] the suspicion of drug-related activity that the dog deployed [was] trained to detect."[123] Having established reasonable suspicion to believe that the suspect was engaged in drug trafficking, the police were authorized to conduct a limited search aimed solely at detecting the presence of drugs.

Chehil reached that conclusion because the Court in *Kang-Brown* had created a new common-law power to conduct such a search. As Justice Binnie explained, "[i]n my view, where the police comply with the requirements of the *Charter*, they possess the common law authority to make use of sniffer dogs in places to which they have lawful access for the purpose of criminal investigations."[124] He concluded that "a sniffer-dog search is authorized by the common law, and the common law itself is reasonable on the basis of reasonable suspicion," because of "the minimally intrusive, narrowly targeted and high accuracy" of such a search.[125] In creating such a common-law power, Justice Binnie added that the Court was "ensuring that the common law reflects current and emerging societal needs and values."[126] Ratifying this view, Justice Deschamps noted that "the law enforcement duties traditionally recognized at common law are 'the preservation of the peace, the prevention of crime, and the protection of life and property.'"[127] Those considerations had previously furnished a proper basis, she observed, for creating a common-law power to allow the police, on reasonable suspicion, to conduct a "random vehicle stop, as part of a program to detect and deter impaired driving," and she reasoned that precisely the same grounds would justify "the use of a sniffer dog by the police as an independent investigative tool," based on reasonable suspicion.[128] Finally, drawing on the same considerations, Justice Bastarache reasoned that where the police "were attempting to identify and apprehend individuals carrying illegal drugs, weapons or other contraband on Canada's public transportation systems," their use of sniffer dogs to pursue those goals "falls within the scope of their lawful duties at common law."[129]

For the police to have legal authority to search for text messages, in cases involving conspiracies to distribute drugs, weapons, or similar contraband, in the narrowly targeted fashion described above, would thus require an extension of

123. *Ibid* at para 36.
124. *Kang-Brown*, *supra* note 15 at para 57.
125. *Ibid* at para 60.
126. *Ibid* at para 62.
127. *Ibid* at para 151 quoting *Dedman v The Queen*, [1985] 2 SCR 2 at 32, 20 DLR (4th) 321 [*Dedman*].
128. *Kang-Brown*, *supra* note 15 at para 157 [emphasis omitted].
129. *Ibid* at para 233.

Kang-Brown and *Chehil*. The rationales offered in those cases would readily justify such an extension. The goals of these different kinds of searches are virtually identical; as formulated here, the search of the phone would have to be as "minimally intrusive, narrowly targeted and high[ly] accura[te]" as a sniffer dog search; and ultimately the search would advance the same law enforcement duties, traditionally recognized at common law, as in *Kang-Brown* and *Chehil*—namely, "the preservation of the peace, the prevention of crime, and the protection of life and property."[130] As with the dog-sniff cases, the effect would be to "ensur[e] that the common law reflects current and emerging societal needs and values."[131]

To date, applications of the "reasonable suspicion" standard have generally involved questions of spatial rather than information privacy.[132] Consequently, analogies to informational privacy may seem awkward at first blush. There is no evidently liminal position from which police may detect information, no exterior of a phone or computer, where they may hover without touching, or while touching only lightly. That view, however, confuses the superficial aspects of the jurisprudence, as it has applied so far, with its underlying goals. Searches based on reasonable suspicion are easiest to imagine (and to visualize) when they can be characterized in physical terms, but the more basic point is that the search must be limited and targeted, and must refrain from inquiring into information that is not relevant to the search.

In explaining what constitutes reasonable suspicion, courts have explained that although it falls short of reasonable and probable grounds, it nevertheless depends on "objectively ascertainable facts."[133] In *R v M(A)*, Justice Binnie elaborated on the "narrowly targeted" nature of the search:

> [T]he dog's communication capacity is limited to a positive alert or a failure to react at all. Unlike a wiretap or a physical search, the police do not obtain a lot of information about a suspect that is not relevant to their specific drug inquiry. While the suspect has a privacy interest in the place where the drugs are concealed, the fact that the sniff will disclose nothing except the presence of illegal drugs in that private place is a factor weighing in favour of moving the balance point to the reasonable suspicion standard.[134]

130. *Dedman*, *supra* note 127 at 32.
131. *Kang-Brown*, *supra* note 15 at para 62 citing *R v Mann*, 2004 SCC 52 at para 17, [2004] 2 SCR 59 and *Duarte*, *supra* note 74 at 670.
132. For instance, besides the use of sniffer dogs to detect drugs in lockers, the courts have used this standard to justify a frisk or pat-down. See note 17 and the accompanying text above.
133. *Kang-Brown*, *supra* note 15 at para 75.
134. *R v M(A)*, *supra* note 13 at para 83.

Analogously, reasonable suspicion would permit the police to look only for messages received from other particular individuals who have already been identified as suspects, or messages received within a narrow time frame, specified in advance, which the police have identified as a period during which the suspects were planning or committing the crime. Any messages not relevant to the crime under investigation are irrelevant and should be excluded, and if the search for messages from other, previously identified suspects yields no results, the question of false positives does not even arise.

In *R v M(A)*, Justice Binnie acknowledged that "the suspect has a privacy interest in the place where the drugs are concealed," but he did not conclude that reasonable suspicion was insufficient to overcome that interest.[135] Rather, he proposed that reasonable suspicion afforded the right "balance point" for the kind of limited search he described.[136] In *R v Melesko*, similarly, the court observed that "a reasonable suspicion standard may be sufficient where the investigative technique is relatively non-intrusive and the expectation of privacy not too high."[137] Thus, to say that individuals have the same reasonable expectation of privacy in all forms of written communication—letters, emails, and text messages—does not necessarily translate into the consequence that none of them are available to the police unless they are acting under a warrant or an exception to the warrant requirement. In most instances, none of the factors in *Plant* will apply to create a heightened privacy interest. This is particularly true for most communications sent between individuals who are conspiring to commit a crime. The interest that attaches, then, is the basic privacy interest applicable to written communication as a general matter. That interest would bar the police from undertaking random and groundless searches, in the hope of finding evidence of criminality. Consequently, this approach would insulate the vast majority of such communications from any police search, while permitting the police to search only when they have objectively ascertainable facts as to a specific crime, and as to specific individuals.

Pelucco and *Marakah* offer appropriate settings for the use of this standard. In both cases, the police had objective grounds, short of reasonable and probable grounds, to search the suspects' phones for text messages related to the crimes under investigation. In both cases, the police appear to have conducted a minimally intrusive and appropriately targeted search, aimed only at the messages relating to those crimes. In both cases, the Crown contended that text messages

135. *Ibid*.
136. *Ibid*.
137. *R v Melesko*, 2010 ABPC 384 at para 158, [2011] AWLD 872.

are categorically exempt from protection under section 8, and therefore did not propose any alternative ground for admissibility, such as that the evidence was admissible under the standard of "reasonable suspicion." Going forward, the adoption of this approach would give the public greater security in the privacy of their communication, while also giving the police clear guidance on how to conduct a *Charter*-compliant search for electronic communications.

V. CONCLUSION

Despite the Court's effort to craft a categorical approach to the treatment of text messages in *Marakah*, the judgment rests on several considerations that leave future cases dependent on the particular circumstances that arise. Moreover, on *Marakah*'s reasoning, the circumstances that drive the outcome are not grounded in normative concerns that help to explain why most people would attach a high privacy value to written correspondence of nearly any kind. A simpler approach, based on social norms, would only offer better protection for text messages while giving the law more predictability. At the same time, a standard of reasonable suspicion for a limited search—akin to the sniffer dog searches permitted by *Kang-Brown* and *Chehil*—would enhance the ability of police to conduct investigations without jeopardizing the privacy status of text messages as a general matter. Some might contend that an even more purely categorical approach—endowing all text messages with a privacy interest and refusing to permit any warrantless searches—would be even more desirable. While that view has some plausibility, the jurisprudence applying the standard of reasonable suspicion offers a well-developed basis for an approach that achieves largely the same goals, while also adapting the common law to "current and emerging societal needs and values," in a fashion that answers the needs of the police while also protecting the public.