THE CONTINUING LEGAL EDUCATION
SOCIETY OF BRITISH COLUMBIA
CLE BC

CRIMINAL LAW PERSPECTIVES 2017
PAPER 2.1

Trending Issues in Electronic Searches—Text Is the New Talk

Gd wms c l hmwcb r f gq Np_argac Nmg l r* wms a_l _aacqq _jj AJC@A amspqc k_rcpg_jq `w qs`qapg`g l e rm r f c
M l jg l c Amspqc K_rcpg_jq Jg`p_pw,

These materials were prepared by Elizabeth P. Lewis of Cobb St. Pierre Lewis, North Vancouver, BC, for the Continuing Legal Education Society of British Columbia, May 2017. This paper had been updated and modified from a paper first presented in February 2016 at the LESA conference in Calgary and Edmonton

and focus on the nature of text messages as private communications with the natural attendant privacy expectations come to the opposite conclusion.

In *R. v. S.M.* 2012 ONSC Nordheimer J. concludes that the accused maintained an "ongoing privacy interest" in text messages located on another persons phone. He writes:

> 24 The fact that a digital record exists of a text message does not substantially change the privacy interest that arises from the nature of the message. It is still a private communication that the sender intends only for the recipient. While I accept that the fact that there is a record of that message beyond the control of the originator slightly lessens the privacy interest, in the sense that the originator must be alert to the possibility that the recipient might show or otherwise transmit the message to others, I believe that there is a qualitative difference between that risk and the risk that the state will seize the message. Again, the observations of La Forest J. in *Duarte* are apposite, at para. 30:
>
> > I am unable to see any similarity between the risk that someone will listen to one's words with the intention of repeating them and the risk involved when someone listens to them while simultaneously making a permanent electronic record of them. These risks are of a different order of magnitude. The one risk may, in the context of law enforcement, be viewed as a reasonable invasion of privacy, the other unreasonable. They involve different risks to the individual and the body politic. In other words, the law recognizes that we inherently have to bear the risk of the "tattletale" but draws the line at concluding that we must also bear, as the price of choosing to speak to another human being, the risk of having a permanent electronic recording made of our words.
>
> 25 I would amend the latter observation of La Forest J., given the realities of the world in which we now live more than twenty years later, to say that the law ought to draw the line between the risk of the "tattletale" who chooses to show a text message to a third party and the seizure by the state of text messages as the price of someone choosing to adopt this form of "new age" private communication over the traditional telephone call.[10]

The contrary position is evidenced in the case of *R. v. Pammett* 2014 ONSC 1213 where McCarthy J. concludes the sender of a text message does not have a reasonable expectation of privacy in the text messages on a phone seized from a third party. He reasons as follows at para 8:

> 8 With the greatest of respect to my brother Nordheimer J., I am unable to agree with his conclusion that text messages generally carry with them a reasonable expectation of privacy. While it may be possible, in an appropriate case, for an accused to establish a reasonable expectation of privacy, this expectation should not, in the absence of some subjective evidence, apply to routinely exchanged text messages. Taking into account the factors as set out in *Edwards*, I am unable to find any indicia of ownership or possession by the Applicant of the text messages in question. One has to presume that the Applicant understood that, in sending a text message, he was surrendering the content of the message, in a written and permanent form, to another party. The party who receives the message on his or her device inherits, from that moment, the unfettered ability and means to preserve, forward or disseminate the message, and indeed to print or archive it.[11]

---

10 See also *R. v. Knox* 2013 ONCJ 484 and *R. v. Ormston* 2013 ONCJ 437 at paras 54 and 55 applying *S.M.*

11 The reasoning of Simard C.Q.J. in *R. v. Noel* 2013 QCCQ 15544 is to the same effect. See also *R. v. Thompson* 2013 ONSC 4624 where Himmel J. characterizes the comments of Nordheimer J, in *S.M.* as

In *R. v. Didechko* 2015 ABQB 642 Schutz J. concludes that Didechko did not have standing to challenge the production orders for the phone records of another party, which of course revealed his sent text messages. Schutz J states as follows at paragraph 297:

> In respect of both Tabs E and J, which were both production orders for records from Ms. McIsaac's phone that included the content of text messages, I find that Mr. Didechko does not have a privacy interest in a sent text message, with the result that there is no privacy interest in the text messages disclosed in Tabs E and J in the sender, namely Mr. Didechko. Accordingly, I find that Mr. Didechko has no standing to challenge these production orders under s 8 of the *Charter*. [12]

The British Columbia case of *R. v. Pelucco,* 2015 BCCA 370 is the first appellate level case to address the question of whether the sender of a text message retains an expectation of privacy in a sent message. Mr. Justice Groberman, in a majority 2-1 decision, concluded that " a sender will ordinarily have a reasonable expectation that a text message will remain private in the hands of its recipient". [13]

Briefly, the facts in Pelucco were that the Nanaimo RCMP pulled a man named Guray over as a result of speeding and erratic driving. Guray was in a rental vehicle. The police became suspicious of Guray as a result of his answering questions in a manner that they did not consider to make sense. While he had no criminal record, computer entries suggested involvement in drug activity, he had a tattoo that said "outlaw" which police refused to believe was unrelated to gang involvement, police thought people often use rental vehicles for criminal activities and Guray was nervous and would not make eye contact. Police asked for and were REFUSED permission to search the trunk. They forged ahead and did it anyway finding a backpack full of $38,000 cash. While no cocaine was found the searching officer said he could smell it. Guray was arrested and his vehicle further searched as incident to arrest. A cellphone was located in the cupholder and police observed text messages they believed related to a planned purchase of one kilo of cocaine. Police continued the conversation and arranged a meeting at the Rugby Club in Nanaimo. Pelucco shows up and is arrested. His vehicle is searched and a kilo of cocaine is located. Relying extensively on the text messages the police obtain a search warrant for Pelucco's residence and a further kilo of cocaine is discovered along with $57,550 cash.

The text messages were lynchpin in the police investigation, without them the grounds for both the arrest and the search warrant fell away. The majority of the British Columbia Court of Appeal agreed with the trial judge that the police were not entitled to rely on the text messages and upheld Pelucco's acquittal. Critical to the Court's conclusion was the finding that Mr. Pelucco maintained an ongoing and reasonable expectation of privacy in his sent text messages.

The reasoning in *Pelucco* was unanimously affirmed by the British Columbia Court of Appeal in the later decision of *R. v. Craig* 2016 BCCA 154.

There is now Appellate authority in Ontario contrary to our Court of Appeal's decisions in *Pelucco* and *Craig. R. v. Marakah* [2016] O.J. No. 3738 is a majority decision declining to follow *Pelucco*. The majority concludes the sender of a text message does not maintain a reasonable expectation of

---

obiter and applying the *Edwards* factors concludes there is no expectation of privacy in sent messages located on a third persons device.

12 *Didechko* was decided on October 13, 2015, less than two months after *Pelucco.* There is no reference to *Pelucco* on this point but the Court does refer to *Pammett, S.M., and Ormston.*

13 *R. v. Pelucco,* 2015 BCCA 370 at para 68. The Crown has elected not to appeal notwithstanding their as of right appeal arising from the dissenting opinion of Mr. Justice Goepel.

privacy in sent message once it reaches the recipient. So the case was decided on the issue of standing. Justice LaForme writes a strong dissenting opinion agreeing with the reasoning in *Pelucco*. The sticking point between the majority and dissent really relates to the role of "control" in the analysis – in other words the applicability of the traditional *Edwards* factors versus a more nuanced approach that places greater emphasis in the privacy interests engaged by the search. The Supreme Court of Canada heard the appeal in *Marakah* in March 2017. It will be most interesting to see how the court rules. The trend in the recent past has certainly been to recognize very significant privacy rights in computers and electronic devices. The Court has historically rejected the risk analysis and third party doctrine so it seems likely that the Court will not resile from that position and continue the trend towards protecting privacy interests., given the ample search powers already available to police.

A finding that the sender of a text message continues to have standing to challenge its search and seizure does not preclude the police from obtaining it lawfully. The police have ample search powers. They may search incident to arrest within the parameters of *Fearon,* in the event of urgency the police always have resort to the doctrine of exigent circumstances and of course there always remains resort to prior judicial authorization by telewarrant or otherwise.

III. Step One – Establishing a Reasonable Expectation of Privacy

It is well settled that an applicant must establish a reasonable expectation of privacy in the subject matter of the search in order to be in a position to challenge any state intrusion. [14] Mr. Justice Cromwell put the matter in the following terms in *Spencer*:

> 16 The first issue is whether this protection against unreasonable searches and seizures was engaged here. That depends on whether what the police did to obtain the subscriber information matching the IP address was a search or seizure within the meaning of s. 8 of the *Charter.* The answer to this question turns on whether, in the totality of the circumstances, Mr. Spencer had a reasonable expectation of privacy in the information provided to the police by Shaw. If he did, then obtaining that information was a search.

If the Applicant cannot establish an expectation of privacy that will end the matter: no *Charter* challenge can be advanced. In addressing this issue it is important to remember that establishing an expectation of privacy is not an all or nothing proposition, the issue is plainly one of degree ranging from no expectation in some cases, lessened expectation in others and heightened expectation in yet other things such as computers or homes.

The question of whether a reasonable expectation of privacy exists is to be determined based on the "totality of the circumstances" tailored to the facts of each case. One of the leading cases on this issue is undoubtedly the SCC decision in *Edwards*. In that case Mr. Justice Cory addressed the totality of the circumstances test in the context of an apartment where the accused was a mere visitor. He identified a list of factors that have come to gain wide acceptance in determining this issue.

> 45 A review of the recent decisions of this Court and those of the U.S. Supreme Court, which I find convincing and properly applicable to the situation presented in the case at bar, indicates that certain principles pertaining to the nature of the s. 8 right to be secure against unreasonable search or seizure can be derived. In my view, they may be summarized in the following manner:

---

14 See *inter alia R. v. Edwards* [1996] 1 S.C.R. 128 at para 33, *R. v. Patrick* 2009 SCC 242 at paras 27-28 and *R. v. Spencer* 2014 SCC 43 at para 16

(1) A claim for relief under s. 24(2) can only be made by the person whose Charter rights have been infringed. See R. v. Rahey, [1987] 1 S.C.R. 588, at p. 619.

(2) Like all Charter rights, s. 8 is a personal right. It protects people and not places. See Hunter, supra.

(3) The right to challenge the legality of a search depends upon the accused establishing that his personal rights to privacy have been violated. See Pugliese, supra.

(4) As a general rule, two distinct inquiries must be made in relation to s. 8. First, has the accused a reasonable expectation of privacy. Second, if he has such an expectation, was the search by the police conducted reasonably. See Rawlings, supra.

(5) A reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances. See Colarusso, supra, at p. 54, and Wong, supra, at p. 62.

(6) The factors to be considered in assessing the totality of the circumstances may include, but are not restricted to, the following:

(i) presence 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.

(viii) See United States v. Gomez, 16 F.3d 254 (8th Cir. 1994), at p. 256.

(7) If an accused person establishes a reasonable expectation of privacy, the inquiry must proceed to the second stage to determine whether the search was conducted in a reasonable manner.

46 Taking all the circumstances of this case into account, it is my view that the appellant has not demonstrated that he had an expectation of privacy in Ms. Evers' apartment. While the factors set out in Gomez, supra, are helpful, they are certainly not exhaustive and indeed other factors may be determinative in a particular case. Nonetheless, it is significant that, apart from a history of use of Ms. Evers' apartment, the appellant cannot comply with any of the other factors listed in Gomez, supra.

While it is true that the *Edwards* factors have gained wide acceptance (the Crown urged the court to apply them in Pelucco both at trial and on appeal) it is equally true that they are not the be all and end all of this inquiry. The cautionary language of Mr. Justice Cory; namely this is a non-

exhaustive and non-determinative list, seems at times to be forgotten as the factors have been slavishly applied in circumstances where they do not seem to be a particularly good fit. [15]

When confronted with privacy issues that impact personal or informational privacy issues *Spencer* provides a far more helpful analytical paradigm. In that case the question was whether the police were entitled to obtain the name and address information connected to an IP address without warrant. In assessing whether Mr. Spencer maintained a reasonable expectation of privacy in this information Mr. Justice Cromwell affirms the totality of the circumstances approach and groups the factors to be considered into four general categories as follows:

> 17 We assess whether there is a reasonable expectation of privacy in the totality of the circumstances by considering and weighing a large number of interrelated factors. These include both factors related to the nature of the privacy interests implicated by the state action and factors more directly concerned with the expectation of privacy, both subjectively and objectively viewed, in relation to those interests: see, e.g., *Tessling*, at para. 38; *Ward*, at para. 65. The fact that these considerations must be looked at in the "totality of the circumstances" underlines the point that they are often interrelated, that they must be adapted to the circumstances of the particular case and that they must be looked at as a whole.
>
> 18 The wide variety and number of factors that may be considered in assessing the reasonable expectation of privacy can be grouped under four main headings for analytical convenience: (1) the subject matter of the alleged search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances: *Tessling*, at para. 32; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 27; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at para. 40. However, this is not a purely factual inquiry. The reasonable expectation of privacy standard is normative rather than simply descriptive: *Tessling*, at para. 42. Thus, while the analysis is sensitive to the factual context, it is inevitably "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": *Patrick*, at para. 14; see also *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 34, and *Ward*, at paras. 81-85.

IV. The Subject Matter of the Search

Identifying the subject matter of the search is an important first step in assessing whether a reasonable privacy expectation exists; however, this is not always a simple matter and *Spencer* itself is an example of this. While the information sought was a name, address and telephone number the Court had no difficulty concluding that in the context of linking that address to particular internet activity the true subject matter was the very identity of the user. In assessing this issue Cromwell J. cautions against adopting a narrow and technical approach to the question saying:

> The correct approach was neatly summarized by Doherty J.A. in *Ward*, at para. 65. When identifying the subject matter of an alleged search, the court must not do so "narrowly in terms of the physical acts involved or the physical space invaded,

---

15 In Pelucco the Crown relied on *R. v. Pammett* 2014 ONSC 1213 (Edwards factors applied to text messages) and *R. v. Noel* 2013 QCCQ 15544 (Edwards factors again applied in the context of text messages). Groberman J. found the analysis in both cases to be "not persuasive" as they gave superordinate weight to considerations of property and control and failed to emphasize reasonable expectations.

> but rather by reference to the nature of the privacy interests potentially compromised by the state action".

Identifying the subject matter of a search in the case of text messages is not a straightforward matter. In the case of messages that have not yet reached the recipient it is clear that these are private communications within Part VI of the Criminal Code.[16] While we would argue that received messages fall into the same category this is unfortunately less than clear. The Court of Appeal did not address the question directly in Pelucco moving directly to a consideration of the factors of objective and subjective expectations of privacy to resolve the issue. Justice Groberman noted that Part VI of the Criminal Code has no application to messages already received relying on the BCCA decision in *Belcourt*[17], where the Court concluded a production order was sufficient to obtain past recorded text messages from the service provider. However, the trial judge in Pelucco was clearly of the view that text messages are private communications no matter where they are in the chain of transmittal and, based on the *Telus* decision, he considered that standing should be presumed.[18]

In *R. v. Croft*[19] Mr. Justice Burrows considers the question of whether a Part VI authorization is required for the state to acquire past text message communications stored on the service provider's computer system. In that case the police had obtained a production order for the acquisition of past text messages. Justice Burrows analyzes the reasoning in the *Telus* decision and concludes that the legal analysis undertaken by Madam Justice Abella leads ineluctably to the conclusion that the acquisition of past text messages is as much an interception of private communications as is their prospective collection. Justice Burrows identifies thirteen (13) elements of the reasoning applied by Madam Justice Abella in *Telus* and concludes that each of them clearly supports the conclusion that the acquisition of past text messages is an interception of private communications.[20]

In *R. v. Didechko* 2015 ABQB 642, Schutz J. declined to follow *Croft*, preferring the analysis of Madma Justice Kirkpatrick in *Belcourt* to the effect that obtaining past recorded text communications is not an interception of private communications and a Part VI order is not required.

This apparent discord in the authorities is really more about the form of order required to access historical text messages be it a Part VI authorization, production order, search warrant or general warrant. For present purposes the key point is that a sender maintains an ongoing expectation of privacy in his or her sent messages and SOME form of lawful authority is required before the police are entitled to access same. While we advanced the need for a Part VI order in the Pelucco case for British Columbians it would seem that ship had sailed with *Belcourt*. Albertans, on the other hand may yet be able to argue that police need to comport with the more onerous requirements of Part VI to access historical text messages, at least where they are obtaining them from the service provider.

---

16 *Telus Communications supra.*,footnote 7

17 2015 BCCA 126, See also *R. v. Carty* 2014 ONSC 212 where Boswell J. concludes a Part Vi order is not needed to obtain historical text messages – a production order will do. See also *R. v. Webster* 2015 BCCA 286 where the Court unsurprisingly follows its prior decision in *Belcourt*.

18 *R. v. Pelucco* 2013 BCSC 588 para 35

19 *2013 ABQB 640*

20 See *Croft* paras 29, 43 – 52 and 66.

V. The Nature of the Privacy Interest Engaged

The Supreme Court of Canada has identified three broad categories of privacy being, territorial, personal and informational. These categories are said to be useful analytical tools in determining the existence of a reasonable expectation of privacy, recognizing that they are not strict or mutually exclusive. [21] Identifying the privacy interest or interests engaged is significant in determining which factors will assist in the analysis. Factors such as proprietary control or presence at the time of the search obviously seem more relevant to searches that engage territorial privacy interests than say informational privacy interests.

In the context of text messages we say the privacy interests engaged are really personal and informational. While Mr. Justice Groberman did not comment directly on the nature of the privacy interests engaged in Pelucco it seems clear he did not consider territorial interests to be significant saying the trial judge was right to focus on the subjective and objective expectations of privacy as the two most important elements in the analysis.

VI. Practical Advice – Building the Evidentiary Foundation

The content and context of the text conversation in *Pelucco* drove the conclusion that Mr. Pelucco had a subjective expectation of privacy. Justice Groberman's said this at paragraph 53:

> 53 I agree with the trial judge's conclusion that Mr. Pelucco had a subjective expectation that his text conversation with Mr. Guray was private. Although the defence called no evidence to establish that expectation, the circumstances leave little room for any other conclusion. It would strain credulity to suggest that a reasonable person would have engaged in such a conversation if they thought that the messages would be shared with others.

Of course this may not always be the case and counsel will have to assess on a case by case basis whether evidence is required as to the senders subjective expectation of privacy. This was clearly an issue for Justice Goepel who noted that Pelucco did not testify and his relationship with Guray was unknown, Justice Goepel was not prepared to infer an expectation that the conversation would remain private.[22]

With respect to objective expectations while Justice Groberman says a sender will ordinarily have a reasonable expectation that a text message will remain private, once again it is clear that the content of the message or the circumstances can lead to a different result. He writes:

> 65 While there will be situations in which the content of the text message or the situation negative these ordinary expectations, it seems to me that the social norm is to expect that text messages remain private communications between the sender and recipient.

The need to lay a proper evidentiary foundation to support the submission that there is both a subjective and an objective reasonable expectation of privacy cannot be overstated. As we seek to extend the reach of *Pelucco* into other mediums of communication it may well be crucial to lead technical evidence as to the functioning of a particular technology, the privacy policies of the service providers, the subjective expectations of the users and the societal norms associated with the use of the technology.

---

21 See *Spencer* at paras 34 and 35

22 See paras 119 and 120 of the dissenting opinion in *Pelucco*

For example *R. v.S.M.*[23] evidences the notion that email should be treated differently than text messages.

> 18. Text messages are a relatively recent phenomenon but their increasing use as a method of communication between individuals cannot be denied. Text messages are instantaneously transmitted and it is generally expected that text messages will receive an equally timely response. The contents of the text messages in this case demonstrate that reality. Text messages are not like email messages where an immediate response is not an expectation inherent in the mode of communication used - although a quick response may nonetheless be wanted. Text messages occur very much more in "real time". Indeed, text messages are often a substitute for an actual conversation and thus are much more akin to a traditional telephone conversation than they are to other modes of communication. Emails, on the other hand, are more akin to an electronic version of a letter.[24]

Our goal today is not to resolve whether emails are on the same footing as text messages, although we would suggest they plainly ought to be treated the same given the many similarities in these methods of communication, but rather to raise the issue of establishing the evidentiary foundation in a particular case for subjecting them to a similar analysis. Obviously a bulk email will engage different considerations than say a private email between, doctor and patient, husband and wife, mother and child, or even among close friends.

VII. Step Two- Was the State Intrusion Unreasonable

Once a reasonable expectation of privacy is established the next question is whether the state intrusion is reasonable.

While the debate simmers on what form of authority is needed to authorize a search for historical text messages, it is clear that some form of lawful authority is required. The point is that absent lawful authority the state intrusion will not be reasonable and a section 8 breach will be established.

Depending on the form of authority relied upon by the state this inquiry may necessitate a consideration of the validity of a production order, search warrant, Part VI authorization or even the grounds for arrest is the search happens to fall within the limited scope permitted by *R. v. Fearon* 2014 SCC 77.

Where text messages have been obtained as a result of a search warrant or arrest (as in Mr. Guray's case) involving a third party it becomes necessary to explore the lawfulness of police conduct as against that third party in order to assess the reasonableness of the state intrusion. In Pelucco's case for example it was beyond obvious that the arrest of Mr. Guray was unlawful and the search of his cell phone could not be saved as an incident to a lawful arrest. We turn now to consider this issue of just how far an applicant can go in litigating the violation of a the rights of a third party.

---

23 *supra.,* page 3

24 2012 ONSC 2949 . See also para 108 and 109 of the Goepel dissent in Pelucco. The analysis of McCarthy J in *Pammett* relied on there as to the similarity between email and text is persuasive but in that case was used to support the idea that there is no continuing expectation of privacy in either medium once the message is sent.

VIII. New Frontiers

In closing I suggest that counsel would be wise to consider the privacy interests impacted in the search for data on any form of electronic device in terms of whether to police require judicial authorization to search. In *Fedan* 2016 BCCA 26, the argument did not work with respect to air bag modules in part because of the very limited nature of the information captured. Would it work in the case of GPS records, or other information stored in a vehicles on board computer? Perhaps it would. What about this video records stored in a Ring doorbell or other home surveillance system, is there a REOP there? Perhaps – it will all depend on how the subject matter of the search can be characterized and whether counsel can surmount the hurdle of establishing a reasonable expectation of privacy in the totality of the circumstances.

Gd wms c l hmwcb r f gq Np_ar gac Nmg l r* wms a_l _aacqq _jj AJC@A amspqc k_rcpg_jq `w qs`qapg`g l e rm r f c M l jg l c Amspqc K_rcpg_jq Jg`p_pw,