Telus: Asking the Right Questions about General Warrants
Steve Coughlan

The Supreme Court's decision in *Telus* is a complicated division between the judges taking part which can conceal what was actually decided. In some sense the most interesting issue in the case is the status of text messages, and the question of whether they should be considered to be the equivalent of a "communication" for wiretap purposes. That is not the central issue in the case, however, which actually concerns the possible scope of a "general warrant" under section 487.01 of the *Criminal Code*. Though less well-known as an issue, that is in fact also an important question, and *Telus* is the Supreme Court's first decision about the scope of that potentially very intrusive investigative technique.

It is important to note that, despite the 3-2-2 split among the justices here, Justice's Moldaver's reasons attract a 5-2 majority. Justice Moldaver says that a general warrant is not available when what the police want to do is "substantively equivalent" to a technique governed by an existing statutory scheme. Justice Abella specifically agrees with that conclusion (see para 20), but goes on to find that what the police wanted to do here was not only substantively equivalent to an interception under Part VI of the *Code*, but actually was an interception. Justice Moldaver finds it unnecessary to consider that question.

No doubt, as a practical matter, it will sometimes be easier to show that a general warrant is not available because the technique proposed falls exactly within the confines of some other statutory scheme, rather than that it is substantively equivalent. That is nothing more than a practical approach to the issue, however, and the majority test established here does not require it. The majority test only requires substantive equivalence.

That distinction has practical implications. If one took the test to require showing that the proposed technique would fall squarely within some other scheme, one opens the door to the argument that "the application would not succeed under that other provision, therefore no other provision authorizes this technique". That, in fact, is precisely the argument that the majority "substantively equivalent" argument is meant to prevent. Indeed, that goal is shared by the dissenting judges, who differ on this point only in how to go about achieving it.

The real purpose of the majority test is to ask not "would this application succeed under another section", but "whether this application would succeed or fail under another section, is that other section the governing authority". That is the point of looking for substantive equivalence: to locate those situations where the rules have anticipated investigative techniques such as the one in question and have decided they are not permitted. It is to see to it that the limits consciously attached to those other procedures continue to control the application.

There is a more substantial disagreement between the dissenting reasons of Justice Cromwell and Justice Abella's reasons. Justice Abella, reaching the conclusion that the production of prospective text messages is in fact an interception, adopts a perspective which depends on the perception of the ordinary person to the nature of the activity. We attach the greatest level of procedural protections to electronic surveillance because we recognize that private communications attract a particularly high privacy interest. For the lived experience of people in their daily lives, texting simply is another way of talking: the technology might be different, but the social role played is the same. As Justice Abella notes:

> Despite technological differences, text messaging bears several hallmarks of traditional voice communication: it is intended to be conversational, transmission is generally instantaneous, and there is an expectation of privacy in the communication.[1]

Justice Cromwell, on the other hand, disagrees that recovering text messages amounts to an interception when done in the way proposed here. He argues that if that were true, it would run contrary to much current authority, and would mean that:

> wiretap authorizations may well be required for a host of searches that are clearly not contemplated by Part VI of the *Code*. Police may well have to obtain a Part VI authorization any time they wanted access to the content of private communications, no matter when the message had been sent or whether it had been received or stored on the recipient's device. For example, on a broad reading of "acquire" police seizing e-mails on a Blackberry device would be engaged in an interception because they are acquiring the content of private communications. Similarly, a person authorized to search a computer system as contemplated under s. 487(2.1) would need a wiretap authorization to seize copies of personal communications stored on those computers (including, for example, e-mail messages and stored copies of Internet chats). This approach would run counter to a line of cases in which Canadian courts have found that search warrants are sufficient to allow police to access documents and data stored on a computer....[2]

Justice Cromwell intends this observation to be a kind of *reduction ad absurdum*, showing the unpalatable results which would result from Justice Abella's conclusion. With respect, although Justice Cromwell is quite correct about where the implications lead, it is not clear that those results should be seen as unpalatable. Perhaps *Telus* leads to the conclusion that some of those prior warrants have been improperly issued.

---

[1] *Telus*, para 1.

[2] *Telus*, para 155.

It is for many people an accident of the technology that a searchable record of their instantaneous communications is made by the devices through which the communication takes place. It is in some ways analogous to the Court's recognition in *Morelli*[3] that most computer users should not be seen as having downloaded a file simply because their computer has automatically stored a viewed image in the cache. It is therefore an entirely defensible position to suggest that it is the social role of the communication which is important and which should govern the approach of the law, not the technology which made the communication possible.

At a minimum, Justice Abella's position should be seen as an invitation for judges to seriously reconsider the approach taken to the increasingly common issue of the search of a cell phone incident to arrest (see for example the recent decision of the Ontario Court of Appeal in *R v Fearon*[4]). Searching a cell phone incident to arrest often involves looking through the recent text messages sent from and received on that phone: exactly the kind of search which Justice Abella here finds is an "interception" and therefore attracts the most stringent protections of any warrant provision. That precisely the same search could be conducted on a warrantless basis would therefore be quite anomalous.

This result can be seen by examining an issue which arose in this case but was not before the Court. The initial general warrant here covered text messages for a period of four weeks, two of which had already passed when the warrant was served on Telus and two of which were in the future. The Court's decision concerned only the "prospective" portion of the order, because the Crown and Telus both agreed that a production order could have been used for the existing messages. Because that question was therefore not in issue, Justice Abella observes that: "we need not address whether the seizure of the text messages would constitute an interception if it were authorized after the messages were stored".[5]

In fact, it seems that whether one approaches that issue from the point of view of Justice Abella or that of Justice Cromwell, the answer is that the Crown and Telus were mistaken in agreeing that a production order would be sufficient to obtain those prior records. On Justice Abella's approach, nothing about the underlying policy will be different simply because of the date of the authorization: when making the communication the persons involved will still have intended it to be conversational, will have communicated instantaneously, and will have expected privacy. At a more specific level of the legal argument relied upon by Justice Abella, it will still be true, even if the authorization is not sought until two weeks or two years after the texts were sent, that:

---

[3] *R. v. Morelli*, 2010 SCC 8.

[4] *R v Fearon*, 2013 ONCA 106.

[5] *Telus*, para 15.

> text messages qualify as telecommunications under the definition in the *Interpretation Act*....these messages, like voice communications, are made under circumstances that attract a reasonable expectation of privacy and therefore constitute "private communication" within the meaning of s. 183. Similarly, there is no question that the computer used by Telus would qualify as "any device" under the definitions in s. 183.[6]

The only remaining requirement to invoke Part IV of the *Code* is that what occurred was an interception, and the very point of Justice Abella's reasoning was to reject a "narrow or technical definition of 'intercept' that requires the act of interception to occur simultaneously with the making of the communication itself".[7] As she concludes:

> The interpretation of "intercept a private communication" must, therefore, focus on the acquisition of informational content and the individual's expectation of privacy at the time the communication was made.[8]

In that event any application seeking text messages sent two weeks earlier would equally be an interception, and so a production order ought not to be allowed as the method of investigation.

Similarly, a police officer using an arrested person's own cell phone (which would also be a "device") to scroll through the texts on it would also be intercepting them. Indeed, the argument is probably even more compelling in these circumstances, since typically police will be interested in texts very recently sent: in other words, although the interception need not be contemporaneous, a search incident to arrest will be more likely to gather the information about the private communication very shortly after it was made.

Both of these results also follow on Justice Cromwell's view of the matter, though of course he disapproves of that result. The essence of his argument is that all the general warrant in this case ever authorized was the disclosure of text messages after they had already been lawfully intercepted by Telus, as opposed to the actual interception of those messages. If that is an accurate description, it is also an accurate description of the messages gathered in the previous two weeks. In that event, Justice Abella's reasons would apply equally to both sets of messages, those of the first two weeks and those of the second. Similarly, if obtaining after the fact text messages which have already been stored on an electronic device is an interception, then that

---

[6] *Telus*, para 32.

[7] *Telus*, para 34.

[8] *Telus*, para 36.

should remain equally true whether the particular electronic device is the service provider's computer or the arrested person's cell phone.

This particular dispute of how to treat electronic communications generally, however, remains unsettled. Justice Moldaver deliberately leaves unanswered the question of whether what was sought amounted to an interception. His reasons go no further than finding that a general warrant could not be used for this purpose, because another process was substantively equivalent. Nothing prevents most other warrants (or for that matter the search incident to arrest power) from being used when some substantively equivalent warrant also exists, and so his conclusion does not have the same implications. In the final result, then, three judges say obtaining texts is an interception, two say it is not, and two express no opinion.