R v. Rogers Communications

The Ontario Superior Court of Justice (2016 ONSC 70), 14 January 2016

The Ontario Superior Court provided guidance for police and prosecutors on obtaining customer data from 'tower dumps,' which are a means of obtaining all of the records of a given cell phone tower at a particular time.

In January 2016, the Ontario Superior Court released an important decision in *R. v. Rogers Communications*, 2016 ONSC 70[1] which brings some critical clarity for police and prosecutors about when and how they can obtain customer information from telecommunications providers through 'tower dumps.' Tower dumps are the production of all the records of a cell phone tower at a particular time. Since mobile phones are always communicating with at least one tower, tower dumps can tell the police who is in the vicinity of a particular location at a particular time. Such orders can be important in investigating who was at the scene of a crime, but the records overwhelmingly contain information about people who have nothing to do with the underlying investigation. Justices of the Peace have been granting such orders, but until this decision had no guidance from a superior court on what criteria must be applied to comply with the Canadian Charter of Rights and Freedoms' protections related to unreasonable search and seizure.

The production orders obtained by the Peel Regional Police in this case were broad. The Police were investigating a string of robberies and obtained production orders against Telus and Rogers, looking for the following information related to cellular towers operated by them:

- Names of all customers connected to the towers at the relevant times;
- Addresses of all those customers;
- Who all those customers were calling at the relevant times, including the names and addresses of those persons;
- Who all those customers were texting at the relevant times, including the names and addresses of those persons; and
- Billing information, including credit card and bank information, of all those customers.

Rogers asserted that complying with the order would result in the disclosure of information about 34,000 customers. Telus said their demand would involve 9,000 customers. The vast majority of these customers had nothing to do with the robberies: they were simply in the locations at the relevant times.

Rogers and Telus resisted and went to court to challenge the production orders. The police withdrew them, and argued that the telcos' application was now moot and that Rogers and Telus didn't have standing to assert the privacy interests of their customers. The court disagreed and ordered a hearing, which led to this decision.

The court agreed with the police that tower dumps are a valuable investigative technique. A police detective described the two most common scenarios in which tower dumps are sought:

a. The police have reasonable grounds to believe that a series of crimes were committed by the same person in various locations. For example, a series of robberies with similar hallmarks. Cellular records can identify any subscribers who were in close proximity to more than one of the crime scenes.

b. The police are investigating a single incident, such as a robbery or murder, and have reasonable grounds to believe that the perpetrator used a cell phone at or near the crime scene. The names of persons accessing the cell tower(s) close to the crime scene can then be cross-referenced with other investigative leads. Other such leads might be a list of the owners of Ontario-registered vehicles of the type observed leaving the crime scene or the name of a person whose DNA was found at the scene.

The court framed the issues under review as (a) whether there is a reasonable expectation of privacy in the records at issue, (b) do Rogers and Telus have standing to assert their customers' privacy interests, (c) were the production orders overly broad? Did they thus infringe s. 8 of the Canadian Charter of Rights and Freedoms and what's the appropriate declaration, and (d) what guidance to the police and justices of the peace is appropriate?

With respect to the first question - whether telecommunications customers have a 'reasonable expectation of privacy' in their information recorded by carriers by virtue of tower connections - the Court said it's a matter of common sense[2].

Since the Charter rights of the telecommunications companies themselves were not engaged in the production order, the crown argued that Telus and Rogers have no standing to argue on behalf of their customers. The Court disagreed and most notably came to the conclusion that they may even have a contractual obligation to stand up for their customers:

"[37] The choice is stark. There is an issue concerning the privacy rights of hundreds of thousands of Canadians. If Rogers and Telus are correct, this legal issue can and will be addressed with opposing points of view put forward by counsel. A decision on point can provide guidance to the police and issuing justices. If the Respondent is correct, this legal issue will never be addressed and some justices of the peace will continue to grant similar production orders which, as I will later explain, are overly broad and unconstitutional.

[38] To my mind the choice is clear. Rogers and Telus have standing to assert the privacy

interests of their subscribers and are contractually obligated to do so."

The next question addressed by the Court was whether the production orders at issue were too broad and thus violated s. 8 of the Charter. The jurisprudence requires that such orders be appropriately tailored to the situation and not over-broad[3].

The heart of the decision that will hopefully have a far-reaching impact is the set of guidelines produced by the Court to be followed by the police and justices of the peace. The Court squarely places the onus on the police to only seek appropriately tailored orders in the first instance and not rely on the justice of the peace to scale them back appropriately. In the future, police must include the following information, under oath, to the justice of the peace:

- A statement or explanation that demonstrates that the officer seeking the production order is aware of the principles of incrementalism and minimal intrusion and has tailored the requested order with that in mind.
- An explanation as to why all of the named locations or cell towers, and all of the requested dates and time parameters, are relevant to the investigation.
- An explanation as to why all of the types of records sought are relevant.
- Any other details or parameters which might permit the target of the production order to conduct a narrower search and produce fewer records.
- A request for a report based on specified data instead of a request for the underlying data itself.
- If there is a request for the underlying data there should be a justification for that request.
- Confirmation that the types and amounts of data that are requested can be meaningfully reviewed.

With this information, the justice is able to ensure that all 'tower dump' orders are not overly broad.

For Canada, this is a very important decision that pulls tower dump production orders out of the shadows, shines the light on overly-broad orders and has led to very sensible, balanced rules to be followed by the police and justices of the peace.

David T. S. Fraser Partner
McInnes Cooper, Canada
david.fraser@mcinnescooper.com

1. https://www.canlii.org/en/on/onsc/doc/2016/2016onsc70/2016onsc70.html
2. "[19] Common sense indicates that Canadians have a reasonable expectation of privacy in the records of their cellular telephone activity. Whether and when someone chooses to contact a divorce lawyer, a suicide prevention hot line, a business competitor or a rehabilitation clinic obviously implicates privacy concerns. The location of a person at a particular time also, raises privacy concerns. Was the person at the Blue Jays game instead of at work?
[20] Admittedly this type of information is in the vast majority of cases innocuous. It remains that in a number of cases it will be quite sensitive. It is also not tenable to reason that since only the police will be in possession of this information any sensitive information will never see the light of day. One needs only read a daily newspaper to be aware of the fact that governments and large corporations, presumably with state of the art computer systems, are frequently 'hacked' resulting in confidential information being stolen and sometimes posted online.
[21] I appreciate that cell phone data is not right up there with Wikileaks and Ashley Madison in terms of information likely to be hacked and published. It remains that it is information Canadians certainly regard as private. The law supports this conclusion.
[...]
[23] The Criminal Code, s. 492.2, requires judicial authorization, on a 'reasonable grounds to suspect' standard, to install transmission data recorders, which can capture the telephone numbers of persons sending and receiving communications. This supports the conclusion that there is a reasonable expectation of privacy in this information.
[...]
[31] In my opinion the statutes and case law align with common sense. Canadians have a reasonable expectation of privacy in their cell phone records."
3. "[41] The 'minimal intrusion' principle embodied in s. 8 was described by Mr. Chan in Morelli and Beyond: Thinking about Constitutional Standards for Computer Searches, the Criminal Lawyers Association Newsletter, vol. 33, No. 2, as follows:
'The animating policy is that the state must always be alive to the privacy interests of the individual and must always infringe such interests as little as possible.'
[42] The issuing justice did not have the benefit of the evidence before me and the legal submissions of counsel. With that benefit, I have no hesitation in finding that the Production Orders were overly broad and that they infringed s. 8 of the Charter. The disclosure of personal information the Production Orders required went far beyond what was reasonably necessary to gather evidence concerning the commission of the crimes under investigation. For example, the Production Orders:
a) required production of information relating not only to the cell phone subscriber proximate to the crime scene but also the personal information and location of the other party to the call who may have been hundreds or thousands of miles removed from the crime scene;
b) required production of bank and credit card information which, if it had any relevance at all in locating an individual, could have been sought in a follow-up application for a small number of actual suspects (i.e.) a person whose cell phone was proximate to multiple crime locations; and
c) required production of personal information pertaining to over 40,000 subscribers when all the police were really interested in was information, which could have been provided in a report, listing the few individuals, if any, utilizing a cell phone proximate to more than one robbery location.
[43] I, therefore, make the requested declaration that the Production Orders authorized unreasonable searches and so breached the s. 8 Charter rights of the Rogers and Telus subscribers. As the Production Orders have been revoked nothing would be gained by addressing the further issue of whether the Production Orders also violated the rights of Rogers and Telus."