CITATION: R. v. Rogers Communications, 2016 ONSC 70
COURT FILE NOS.: CRIMJ(P)299/14; CRIMJ(P)300/14; CRIMJ(P)299A/14; CRIMJ(P)300A/14
DATE: 20160114

ONTARIO
SUPERIOR COURT OF JUSTICE

COURT FILE NO.: CRIMJ(P)299/14

B E T W E E N:	)	
	)	
Her Majesty the Queen	)	Robert Hubbard and Katie Doherty, for Her Majesty the Queen
	)	
Respondent	)	
	)	
- and -	)	
	)	
Rogers Communications Partnership	)	Scott C. Hutchison and Christine Mainville, for the Applicant
	)	
Applicant	)	
	)	

COURT FILE NO.: CRIMJ(P)300/14

AND B E T W E E N:	)	
	)	
Her Majesty the Queen	)	Robert Hubbard and Katie Doherty, for Her Majesty the Queen
	)	
Respondent	)	
	)	
- and -	)	
	)	
Telus Communications Company	)	Scott C. Hutchison and Christine Mainville, for the Applicant
	)	
	)	
Applicant	)	
	)	

REASONS FOR JUDGMENT

Sproat, J.

INTRODUCTION

[1] The police in Canada sometimes obtain "tower dump" production orders, meaning an order for all records of cellular traffic through a particular cell tower over a specified time period. Every year such orders require cellular providers to produce the names and addresses of hundreds of thousands, if not millions, of subscribers; who they called; who called them; their location at the time; and the duration of the call. These orders may also require that credit card information be provided.

[2] Rogers and Telus have a contractual obligation to keep subscriber information confidential. They were prompted to seek relief after being served with particularly broad and onerous production orders which I will later describe in detail. Rogers and Telus apply for a court ruling that will make plain that production orders must be tailored to respect the privacy interests of subscribers and conform with constitutional requirements.

[3] In earlier reasons, *R. v. Rogers Communications Partnership*, 2014 ONSC, [2014] O.J. No. 3403, I decided that Rogers and Telus were entitled to proceed with these applications notwithstanding the fact that the orders that were initially challenged were revoked. As explained in that decision the challenge to the

original production orders became moot as the police decided to seek a much narrower production order so that their investigation would not be delayed.

THE EVIDENCE

[4] Mobile telephones check into wireless networks by connecting to antennas that are generally mounted on towers. Cell phones typically access the closest tower but may access more remote towers due to obstructions such as buildings or due to high demand having utilized all capacity at the closest tower. A record is created whenever the telephone attempts or completes a communication which could be a phone call, text message or e-mail. The record identifies the particular tower at which the phone connected to the network. Each tower serves a geographical area ranging from a 10-25 kilometer radius in the country to less than two kilometers in the city.

[5] On April 11, 2014 the Peel Regional Police ("PRP") obtained production orders (the "Production Orders") to further an investigation into a string of jewelry store robberies by identifying persons using cell phones in the vicinity of each store around the time it was robbed. The Production Orders against Rogers and Telus, pursuant to s. 487.012 of the *Criminal Code*, are in similar form (section 487.012 has been replaced by s.487.014 which is similarly worded). The orders require cell phone records for all phones activated, transmitting and receiving data through:

a) all of the Telus towers proximate to 21 municipal addresses. (As noted a call from a particular location would not necessarily access the closest tower so more than 21 towers would have to be dumped.

b) 16 Rogers towers identified by a police officer who made test calls from particular locations to determine the towers being accessed.

[6] The Production Orders require the name and address of every subscriber making or attempting a communication through the particular cell tower. They are framed such that if both the person initiating and the person receiving the communication are Rogers (or Telus) subscribers, then information regarding the recipient must also be provided and the cell tower the recipient used must also be provided. The Production Orders also require billing information which may include bank and credit card information. Telus and Rogers are both contractually obliged, subject to narrow exceptions, to keep the personal information of their subscribers private and confidential.

[7] In order to comply with the Production Orders, Telus estimated it would be required to disclose the personal information of at least 9,000 individuals. Telus needs to conduct separate searches for telephone calls and text messages. There are typically more text messages than telephone calls. Rogers estimated that it would be required to conduct 378 separate searches and retrieve approximately 200,000 records related to 34,000 subscribers.

[8] The Production Orders do not specify how customer information is to be safeguarded and do not expressly restrict the purposes for which the PRP may use the information.

[9] The Telus affidavit indicates that since 2004 it has dealt with thousands of court orders requiring cell records. In 2013 alone, it responded to approximately 2,500 production orders and general warrants. To the knowledge of the Telus deponent, the order that it now challenges is the most extensive to date in terms of the number of cell tower locations, and the length of time periods, for which customer information is required.

[10] The Rogers affidavit indicates that from 1985 to 2014 it has complied with many thousands of court orders requiring the production of cell records. In 2013 alone, it produced 13,800 "files" in response to production orders and search warrants.

[11] The nature and extent of the work and time required to comply with a production order varies from company to company and location to location. The searches that are necessary to comply with a production order utilize the subscriber records maintained for billing purposes and must often be run outside of regular business hours. The search required to identify the phone numbers

that utilized a particular tower is separate and apart from the search required to relate a subscriber name and address to the numbers.

[12] Tower dump production orders are a valuable investigative technique given that criminals routinely use cell phones to facilitate the commission of crimes and/or leave their cell phones turned on while committing crimes thereby leaving a trail of any outgoing or incoming calls and their location at the time.

[13] Detective Douglas Cole of the York Regional Police Service, who filed an affidavit and was cross-examined, has extensive experience in obtaining tower dump orders and using them to solve serious crimes. In cross-examination he agreed that there are typically two scenarios in which a tower dump order is 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.

[14] Detective Cole explained that when the police focus on a suspect, such as a person proximate to multiple crime scenes or a person who is proximate to a crime scene who owns the type of vehicle that left the scene, further orders can be sought to obtain more extensive telephone records for that person which might in turn identify other suspects.

[15] Detective Cole stated that his practice is to limit the information sought in an initial production order to ensure that the amount of data is manageable and can be meaningfully reviewed. Subsequent orders can then be obtained. For example, in the serial crime scenario the police do not need to know the names and addresses of all cell phone users at the location of every crime. The police only need the names and addresses of perhaps a few users whose phone was used in proximity to more than one crime scene.

[16] While Detective Cole can obviously not speak on behalf of all police services, he indicated that he consulted with experienced officers at other services, including the RCMP, in order to formulate his suggestions as to appropriate guidelines.

[17] Detective Cole identified a number of general principles and instructions that he believed would help ensure that police apply for effective and 'privacy enhanced' tower dump production orders. His suggestions were distilled by Mr.

Hubbard into a number of suggested best practices which I will later discuss. Detective Cole did, however, caution that:

> a) These general principles and practices, are not designed to deal with all possible scenarios [...] Determining the appropriate amount and type of data to seek in a specified tower dump production order requires a case-by-case analysis of the particular facts and circumstances in each investigation.

THE ISSUES

[18] The parties identified the issues as follows:

a. is there a reasonable expectation of privacy in the records ordered to be produced?

b. if there is a reasonable expectation of privacy, do Rogers and Telus have standing to assert it?

c. do the Production Orders infringe s. 8 of the *Canadian Charter of Rights and Freedoms* ("the *Charter*")? Are they overly broad? What declaration is appropriate?

d. what guidance to police and issuing justices is appropriate?

IS THERE A REASONABLE EXPECTATION OF PRIVACY IN THE RECORDS?

[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 on-line.

[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.

[22] First, the relevant statutes. The *Personal Information Protection and Electronic Documents Act*, S.C. 2000, C.S. ("*PIPEDA*"), which applies to Rogers and Telus, provides as follows:

> b) s. 2 "personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.
>
> c) s. 3 "The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and

> the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances"

[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.

[24] The Production Orders were issued pursuant to s. 487.012(3) of the *Criminal Code* which provided that:

> (3) Before making an order, the justice or judge must be satisfied, on the basis of an ex parte application containing information on oath in writing, that there are reasonable grounds to believe that:
>
> a) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed;
>
> b) the documents or data will afford evidence respecting the commission of the offence; and
>
> c) the person who is subject to the order has possession or control of the documents or data.

[25] Mr. Hutchison stressed the point that tower dump orders are unusual in that, by their nature, 99.9% of the records sought will relate to innocent persons. For that reason he argued that there was a heightened need to protect the privacy interests of these individuals.

[26] Turning to the caselaw, in *R v. Mahmood*, [2008] O.J. No. 3922 (S.C.), affd. [2011] ONCA 693, 107 O.R.(3d) 641 the police were investigating a jewellery store robbery. As Quigley J. explained, the police initially sought a 'tower dump' warrant to obtain:

> ...name, home and business address and date of birth, date and time of call, and all telephone numbers dialed or received by the account holder. (para. 15).

[27] The information to obtain the tower dump search warrant simply asserted that robbers commonly use cell phones. There was no case specific information to suggest the jewellery store robbers had used cell phones in the course of the robberies.

[28] Through investigative measures independent of the tower dump records, the police identified Fundi as a suspect. He was placed under surveillance and observed frequently associating with Mahmood, and two other men Sheikh and Malik. The police then applied for a further "subscriber" warrant to obtain the cell phone records of Fundi and Malik which disclosed several calls between them around the time of the robbery and that their phones were in the vicinity of the jewellery store at the time of the robbery.

[29] Quigley J. ruled that the "tower dump" warrant violated s. 8 and that the evidence should be excluded under s. 24(2) of the *Charter*. As to the expectation of privacy in "tower dump" records Quigley J. stated:

> Nevertheless, while not adopting their reasons, I agree generally with Ferguson J. in *R. v. MacInnis* and Donnelly J. in *R. v. Bryan* , in their conclusions that when this kind of information is revealed or exposed in this age, recognizing the protean nature of the inquiry, it may well by the use of the technology itself, or by the application of further inquiry or technology to the raw data, expose detail of the "lifestyles" of the Applicants or information that approaches that of a biographical nature that is *Charter* protected. In the context of the robbery investigation that was underway, this information did disclose who and where these individuals or their cell phones were, and what numbers they or their cell phones were communicating with and how frequently, and equally importantly, when those numbers were not communicating while the robbery was in progress. It is that collated information, which when further examined and cross-referenced to other information obtained by police that could and did, in this case, reveal details of the activities and movement of the Applicants. It permitted the police here to determine that two or three of the four Applicants were in the vicinity of the robbery when it occurred, a fact that was central to their belief of their involvement in this crime.

[30] On appeal, Watt J.A. agreed that there was a reasonable expectation of privacy in the tower dump records. He did note, however, that there was a reduced expectation of privacy given that the customer name and location information was far removed from the biographical core of personal information such as intimate details of an individual's lifestyle and personal choices.

[31] In my opinion the statutes and caselaw align with common sense. Canadians have a reasonable expectation of privacy in their cell phone records.

DO TELUS AND ROGERS HAVE STANDING?

[32] The Respondent raised a number of technical and procedural objections. The first was that there was in fact no search and seizure made pursuant to the Production Orders so that s. 8 of the *Charter* is not engaged and no *Charter* remedy is available under s. 24(1).

[33] The Rogers and Telus Notices of Application, however, claimed various forms of relief including a declaration that the Production Orders were unreasonable and inconsistent with s. 8 of the *Charter*.

[34] Rogers and Telus are simply interested in having judicial consideration of the issues raised. As such, the fact that a s. 24(1) *Charter* remedy may be unavailable is not an impediment to granting the declaration sought.

[35] Secondly, the Respondent submitted that any privacy interest at stake was that of the subscribers. As such, Rogers and Telus lack standing to claim any relief.

[36] As discussed, each subscriber has a reasonable expectation of privacy in the information sought by the PRP. Each subscriber has contracted with Rogers and Telus for an assurance that the subscribers personal information will, within certain limits, be kept confidential. It is impractical in the extreme for Rogers and Telus to give tens of thousands of subscribers notice of the fact the PRP is

seeking their personal information. It is also clear, as a practical matter, that no individual subscriber would have an interest in litigating with the government over these issues.

[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.

ARE THE PRODUCTION ORDERS OVERLY BROAD? – DO THEY INFRINGE s. 8 OF THE CHARTER? WHAT DECLARATION IS APPROPRIATE?

[39] Section 8 of the *Charter* provides that:

> Everyone has the right to be secure against unreasonable search and seizure.

[40] In *R v. Vu* [2013] 3 S.C.R. 657, Cromwell J., for the court, stated:

> [21] Section 8 of the *Charter* — which gives everyone the right to be free of unreasonable searches and seizures — seeks to strike an appropriate

> balance between the right to be free of state interference and the legitimate needs of law enforcement. In addition to the overriding requirement that a reasonable law must authorize the search, this balance is generally achieved in two main ways.
>
> [22] First, the police must obtain judicial authorization for the search *before* they conduct it, usually in the form of a search warrant. The prior authorization requirement ensures that, before a search is conducted, a judicial officer is satisfied that the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance the goals of law enforcement: *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 160. Second, an authorized search must be conducted in a reasonable manner. This ensures that the search is no more intrusive than is reasonably necessary to achieve its objectives. In short, prior authorization *prevents* unjustified intrusions while the requirement that the search be conducted reasonably limits potential abuse of the authorization to search.

[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.

[44] I will also comment briefly on the submission by Mr. Hutchison that the issuance of an overly broad order requires the police and the target of the order to negotiate a compromise as to what should be produced and that this constitutes an improper delegation of the issuing justice's authority. I agree that an overly broad order is unacceptable and, as I will discuss, I adopt certain guidelines directed at focusing orders to minimize the intrusion on personal information.

[45] If these guidelines are followed there will no doubt continue to be cases in which compliance with the production order will be more onerous than the police could have contemplated. Circumstances may change as an investigation proceeds which will affect the scope of the information required. In that context, communication between the police and the target of the order should be encouraged as it will further serve the principle of minimal intrusion.

WHAT GUIDANCE TO POLICE AND ISSUING JUSTICES IS APPROPRIATE?

[46] Rogers and Telus also:

> ... ask that the court take the opportunity to provide law enforcement, issuing justices and companies such as the Applicants with guidance as to reasonable parameters for properly confining these types of expansive searches.

[47] Mr. Hubbard submitted, and I agree, that any "guidance" I offer should not be regarded as "bright-line rules", in the nature of conditions precedent, that must be strictly followed before a production order can be issued. Having said that, there are recurring fact patterns that emerge when the police seek tower dump production orders. It follows that there are recurring constitutional considerations which should inform the decision of the issuing justice.

[48] I also note that police services have an obligation to conduct themselves in a *Charter* compliant manner. It is, therefore, improper for the police to seek irrelevant personal information and rely solely on the issuing justice to ensure

constitutional compliance. It remains, of course, that it is up to the issuing justice to adhere to legislative and constitutional requirements.

[49] The Applicants request judicial guidance. The Respondents filed the affidavit of Detective Cole, who believes that such guidance would assist the police in obtaining 'privacy enhanced' production orders. I, therefore, conclude that it is appropriate to identify "guidelines" which I distill from the evidence and the submissions of counsel.

[50] Mr. Hutchison framed his suggestions as "constitutional imperatives". Mr. Hubbard framed his suggestions as "best practices". There was, however, significant common ground.

[51] Mr. Hutchison submitted that:

> 63. To be constitutionally sound, tower dump orders should at a minimum be limited in the following ways:
>
> (1) There should be grounds to believe that all the information sought will meet the standard prescribed by the *Criminal Code,* namely that the information sought "will afford evidence respecting the commission of the offence". If, for instance, the CNA [customer name address] information, the billing information, or the resulting records would not serve that purpose, they should not be obtained;
>
> (2) To the extent possible, the scope of the data obtained should be narrowed by resorting to an incremental approach. For instance, subscriber information should generally be excluded from an initial tower dump authorization;
>
> (3) The scope of the data sought should be narrowed to the extent possible in view of the information available to police. For instance, the

relevant window of time should be as narrow as the information available allows;

(4) The total amount of data that is reasonably anticipated to be produced in response to the order should not in itself be unreasonably large; and

(5) The order should limit the subsequent retention, use and disclosure of the data by police, having in mind that almost all of it will not have anything to do with the offence they are investigating.

[52] Mr. Hubbard identified five "best practices":

1. ***Adherence to the statutory requirements*** - The application and the issuing judicial officer should ensure that there are grounds to believe that all the information sought will meet the standard prescribed by the *Code* in relation to the specific type of Production Order sought.
2. ***Case specific inquiry*** – Efforts should be made to tailor a specific tower dump production order, as much as possible, to the specific requirements of a given case.
3. ***Incremental approach*** – To the extent possible, the scope of the data obtained should be narrowed by resorting to an incremental approach.
4. ***Narrowing the scope of requested information*** – The scope of the data sought should be narrowed to the extent possible in view of the information available to police.
5. ***Requesting a report where possible*** – Where applicable, investigators should consider seeking production of a document based on the requested data, and not the underlying data itself.

[53] Mr. Hutchison's first and third constitutional imperative and Mr. Hubbard's first, second and fourth best practice simply remind of the necessity of adhering to statutory requirements in light of the case specific evidence. While important, I need not discuss them further.

[54] Mr. Hutchison's third constitutional imperative, that there be an incremental approach to production, mirrors Mr. Hubbard's third best practice. I

agree that an incremental approach is supported by the principle of minimal intrusion which animates s. 8 of the *Charter*. One aspect of this, as referred to by Detective Cole, is that the police should not seek such a large amount of personal information that it cannot be meaningfully reviewed.

[55] Mr. Hutchison's fourth constitutional imperative is that the total amount of data sought not be unreasonably large. Mr. Hubbard submits that an absolute restriction based on the volume of material is unworkable. I agree.

[56] The starting point is that if the police and the issuing justice focus on the statutory requirements and the principle of minimal intrusion, the resultant production order will be no more extensive or onerous than is reasonably necessary in order to investigate the crime in question. Further the police, and therefore, the issuing justice, will only have a very general and perhaps inaccurate conception of how much personal information will be captured by a particular production order and how much effort will be required to comply with the order. To ask the issuing justice to speculate as to how onerous it would be to comply with a requested order, and impose a cap on that basis, would be arbitrary and contrary to the best interests of the administration of justice.

[57] It remains that anyone in the position of Rogers and Telus, who wishes to oppose a production order on the basis that it is unreasonable, or unduly

onerous, can request a variance of, or exemption from, the order under what is now s. 487.0193 of the *Criminal Code.*

[58] At the time the Production Orders were sought, s. 487.012(1) of the *Criminal Code* provided that a production order could compel a person to prepare and produce a document based on documents or data already in existence. This provision was repealed and replaced by s. 487.014 which is similar. I think that Mr. Hubbard's fifth best practice, that investigators consider seeking a report based on specified data, and not the underlying data itself, is particularly helpful. Consider the common scenario in which a tower dump order is sought to attempt to identify individuals proximate to multiple crime scenes. The underlying data may relate to where tens of thousands of individuals were at a particular time and who they communicated with. The report, however, would only identify the very few individuals, if any, who happened to be proximate to more than one crime scene.

[59] Mr. Hutchison also suggests that tower dump production orders must address the retention, use and disclosure of tower dump data seized by the police. Certainly, there is much to be said in favour of statutory provisions and business-administrative practices which address the question of how much personal information should be retained and for how long. For example, *PIPEDA*, which by its terms does not apply to the police, incorporates the

Canadian Standards Association Model Code for the Protection of Personal Information which identifies governing principles, including the following:

> 4.5.3. Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

[60] Legislators have been active in enacting privacy legislation. To date, however, no legislation addresses the retention of tower dump records nor other more invasive collections of personal information such as wiretap evidence. On the record before me, I do not think it would be appropriate to offer guidance on post-seizure safeguards. Hearing from all interested parties and determining whether and to what extent safeguards are required is best left to legislators.

[61] Mr. Hutchison also submitted that the guidance I provide should include that tower dump orders only be used, "as a last resort, where traditional investigative techniques have failed". In support he cited Justice Brian Owsley's article: *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps In Its Electronic Surveillance,* Journal of Constitutional Law, Oct. 2013, Vol. 16:1.

[62] I do not accept this submission for two reasons. First, whether to impose this type of general requirement, which imposes strictures on how the police investigate crime, is properly and best left to Parliament. Secondly, where

Parliament has seen fit to impose an investigative necessity requirement it has made this clear. For example, s. 186(1)(b) of the *Criminal Code* makes it a condition precedent, to an authorization to intercept a private communication:

> (b) that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

SUMMARY AND CONCLUSION

Introduction

[63] The guidelines which I now provide reflect the fundamental principles of incrementalism and minimal intrusion. They are guidelines and not conditions precedent. The statutory requirements are now set out in s. 487.014 of the *Criminal Code.*

[64] While I am only able to grant declaratory relief, these guidelines should become known and should make a difference. There is an obligation on the part of the police and the issuing justices to know the law, as I have explained it. Given that a production order is obtained on an *ex parte* basis, there is also obligation on the police to make full, fair and frank disclosure. (See *R v. Araujo*, [2000] 2 S.C.R. 992, at paras. 46-47). This would encompass explaining clearly in the information to obtain how requested data relates or does not relate to the investigation.

Guidelines for Police

[65] The police should include in the information to obtain a production order:

a) **One – 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 awareness of the *Charter* requirements is obviously essential to ensure that production orders are focused and *Charter* compliant.

b) **Two – 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.** – This obviously flows from what is now the s. 487.014(2)(b) *Criminal Code* requirement that there be reasonable grounds to believe that the documents or data requested will afford evidence respecting the commission of the offence.

c) **Three – an explanation as to why all of the types of records sought are relevant.** - For example, the Production Orders sought bank and credit card information, and information as to name and location of the party to the telephone call or text communication who was not proximate to the robbery location. This information was clearly irrelevant to the police investigation.

d) **Four – any other details or parameters which might permit the target of the production order to conduct a narrower search and produce fewer records.** – For example, if the evidence indicates that a robber made a series of calls lasting less than one minute this detail might permit the target of the order to narrow the search and reduce the number of records to be produced. If the evidence indicates that the robber only made telephone calls then there may be no grounds to request records of text messages. (Although the use of voice recognition software may make it difficult to distinguish between a person making a telephone call and a person dictating a text message.)

e) **Five – a request for a report based on specified data instead of a request for the underlying data itself.** – For example, in this case a report on which telephone numbers utilized towers proximate to multiple robbery locations would contain identifying

information concerning only a small number of robbery suspects and not the personal information of more than 40,000 subscribers which the Production Orders sought. This would avoid the concern expressed by Mr. Hutchison that 99.9% of vast amounts of tower dump personal information relates to individuals who are not actually suspects.

f) **Six – If there is a request for the underlying data there should be a justification for that request.** – In other words, there should be an explanation why the underlying data is required and why a report based on that data will not suffice.

g) **Seven – confirmation that the types and amounts of data that are requested can be meaningfully reviewed.** – If the previous guidelines have been followed the production order should be focused which will minimize the possibility of an order to produce unmanageable amounts of data. This confirmation does, however, provide an additional assurance of *Charter* compliance.

Guidelines for Issuing Justices

[66] The guidelines for issuing justices flow from the guidelines for police. Issuing justices should generally insist upon the police providing the information, confirmations and explanations outlined in the Guidelines for Police. Doing so will focus the scope of the production order and ensure that production orders conform to both the requirements of the *Criminal Code* and the dictates of the *Charter*.

Conclusion

[67] I thank counsel for their helpful submissions in relation to this important and topical matter.

Sproat, J.

Released: January 14, 2016

CITATION: R. v. Rogers Communications, 2016 ONSC 70
COURT FILE NOS.: CRIMJ(P)299/14; CRIMJ(P)300/14;
CRIMJ(P)299A/14; CRIMJ(P)300A/14
DATE: 20160114

ONTARIO

SUPERIOR COURT OF JUSTICE

B E T W E E N:

HER MAJESTY THE QUEEN

- and –

ROGERS COMMUNICATIONS PARTNERSHIP

REASONS FOR JUDGMENT

Sproat, J.

Released: January 14, 2016