The Age of Digital Surveillance: Cell Tower Dumps

By Mila Shah

I. INTRODUCTION

Privacy, and the restraints imposed on government to pry into our lives, are critical to the democratic state. As Justice Binnie has stated, "[f]ew things are as important to our way of life as the amount of power allowed to the police to invade the homes, privacy and even the bodily integrity of members of Canadian society without judicial authorization."[1] But the concept of privacy has changed with advents in technology. In the past, privacy was associated with private property: "[i]f the rights of private property were respected, and the curtains of the home (or the drawbridge of the castle) were pulled, the King's agents could watch from a distance but would have no way of finding out what was going on inside." This is no longer true. Modern technology – particularly cell phones – has made our personal information, our communications, and details of our lifestyles increasingly accessible outside the perimeter of our private home.

Today, almost everyone carries a cell phone. Indeed, modern cell phones are much more than just phones. Smart phones allow us to access the internet, send emails and text messages, check the weather, conduct online banking, share photographs, play games, and access social media. We are more connected than ever before. However, this technological advancement comes with a price to our privacy. When we put our cell phone back in our pocket or our purse, a record of our activity remains. The cell phone service provider logs and retains the calls or text

[1] *R. v. Tessling*, 2004 SCC 67 at para. 13.

messages made and received, their length and time, the subscriber who made or received the call, and the approximate location of the subscriber at the time. This information is used for billing and other business purposes. In this way, the major telecommunication companies, such as Rogers Communications or Telus Communications, hold a massive amount of our personal information.

This has significant implications for law enforcement. The rise in cell phone use, and the personal information generated by it, has led to an intrusive, but effective, investigative technique known as a "cell tower dump". The police can obtain the records of cellular traffic through a particular cell tower at a specific time from the cell phone service provider. The records include the names and addresses of subscribers, their call and message history, their location at the time, and the duration of the call. Sometimes, even credit card information is provided. This information tells the police who was in a particular area during a particular crime, allowing them to identify suspects. While this technological development advances the public interest in effective law enforcement, it constitutes a significant intrusion on the privacy rights of thousands of people. It is one of the broadest searches the police can conduct.

This paper will outline the privacy concerns associated with cell tower dumps, examine the legal responses in the United States and Canada, and discuss how the law should be developed to respond to cell tower dumps in a way that strikes an appropriate balance between the privacy interests at stake and our collective right to public safety.

II. BACKGROUND

A. The Technology: Cell-Site Data

Cellular telephone service providers operate large service areas that are divided into segments – or "cells". Each cell is equipped with a "cell site" containing an antenna installation, usually on top of a tower. Cell phones constantly transmit and receive radio wave signals throughout a service provider's network, connecting to the tower with the strongest signal in order to make and receive calls most effectively. This occurs as often as every seven seconds. When the signal from one cell tower weakens (for example, as the cell phone user moves away from the cell tower), the phone transfers to another cell site with a stronger signal.[2]

When the cell phone is used to make or receive a call, transmit or receive a text message, or access the internet, a transceiver sends signals over the air on a radio frequency to the cell site, where the antenna detects the radio signal and connects it to the local telephone network, internet, or another wireless network.[3] Smart phones send signals even more frequently, as they regularly check for new emails and maintain a persistent internet connection.[4]

Anytime a cell phone sends a signal to a cell tower, the service provider automatically logs and stores information about the communications. A record is created of time and duration of the communication and the particular tower at which the phone connected to the network. This information is essential for billing purposes.[5] However, it can also be critical to a criminal investigation, as the cell-site data can tell law enforcement agents where and how a cell phone

---

[2] Elizabeth Gula Hodgson, "The Propriety of Probable Cause: Why the U.S. Supreme Court Should Protect Historical Cell Site Data With A Higher Standard" (2015) 120 Penn St. L. Rev. 251 at at 256-257.
[3] The Honourable Brian L. Owsley, "The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance" (2013) 16:1 University of Pennsylvania Journal of Constitutional Law 1 at 3-5.
[4] American Civil Liberties Union, *ACLU Response to Government Application for Historical Cell Site Data from Cell Towers in the Vicinity of One Location During a Four-and-One-Half-Hour Time period*, online: https://www.aclu.org/aclu-tower-dump-brief?redirect=national-security/aclu-tower-dump-brief.
[5] Owsley, at 5.

was used at a particular time. In this way, the state can reconstruct an individual's specific movements down to the minute.[6]

B. The Investigative Technique: Cell Tower Dumps

If the police have a suspect, they can obtain the suspect's cell site data from the suspect's service provider. This will include a record of the calls made by the suspect, calls received by the suspect, the time and duration of the phone calls, and the cell towers to which the phone connected. In this way, the police obtain a detailed summary of the suspect's movements.

Sometimes, however, the police obtain orders requiring cell phone service providers to produce all records of cellular traffic through a particular cell tower over a specified period of time. This is called a "tower dump", and it provides a listing of any cell phones that used the particular cell tower at a particular time and date.[7] The order may also require the service provider to produce the names and addresses of the subscribers, who they called or messaged, who called them or messaged them, the duration of the calls, and even the subscribers' credit card information.[8]

There are typically two scenarios in which a tower dump order is sought by the police. First, this technique is used when the police have grounds to believe that a series of crimes were committed by the same person in various locations – for example, a series of robberies or sexual assaults with similar hallmarks. Cellular records can identify any subscribers who were in close proximity to more than one of the crime scenes at the relevant time. Second, a tower dump may

[6] Hodgson, at 257.
[7] Owsley, 6.
[8] *R. v. Rogers Communications*, 2016 ONSC 70 at para. 1.

be useful where the police are investigating a single incident and have grounds to believe that the offender used a cell phone at or near the crime scene. The names of the persons accessing the cell tower close to the location of the offence can be cross-referenced with other investigative leads.[9]

For example, in 2009, two men known as the "High Country Bandits" committed a string of bank robberies in northern Arizona and Colorado. They wore jackets, ski masks, and gloves, making it impossible to identify them from bank surveillance footage. When the FBI were brought onto the case, they asked a federal magistrate judge to approve cell tower dumps from four of the robbery locations. The judge approved the request, giving the FBI access to more than 150,000 registered cell phone numbers. One Verizon Wireless phone number registered with the tower closest to the banks on the day of each robbery, leading to the capture of the High Country Bandits.[10]

The Honourable Brian L. Owsley, a judge on the United States District Court for the Southern District of Texas, has commented that cell tower dumps occur routinely. However, they have not garnered much attention in the media, as the government does not like to draw attention to this form of electronic surveillance.[11]

III.PRIVACY CONCERNS

While tower dumps may be an effective investigative technique, they raise two serious privacy concerns. First, the scope of the search is incredibly broad. Tower dumps are, in essence, fishing expeditions that provide the state with mass tracking information about thousands of

[9] *Rogers Communications*, at para. 13.
[10] Owsley, at 27-29.
[11] Owsley, at 17-18.

people who are not connected to the offence. Second, the information requested by the state is held in the hands of the telecommunication companies. The people whose information is being shared may never know. This makes the investigative technique difficult to challenge.

A. Scope of the Search

Tower dumps are unusual searches in that, by their nature, 99.9% of the records obtained relate to innocent persons. [12] Accordingly, the privacy concerns do not just relate to the suspect – tower dumps result in significant breaches of third parties' privacy rights. For example, in the case of the High Country Bandits, the FBI ultimately received over 150,000 telephone numbers.[13] In 2014, the United States government sought a tower dump order covering a number of cell towers in New York City over a 4.5 hour period. The American Civil Liberties Union, in its brief to the judge, pointed out that this was an extraordinary request. Given New York's high population density, such a tower dump would likely implicate a tremendous number of people – particularly given the length of time for which the data was sought.[14] In a recent Canadian case, a tower dump order required Rogers to disclose the information of approximately 34,000 customers.[15]

In describing the privacy concerns associated with a tower dump, the Ontario Superior Court commented:

> Most importantly here, the police did not obtain such information under the Tower Dump Warrants for known or named individuals or known or named cell phone numbers. They had no knowledge of any particular person who may have used a cell phone in that vicinity on that day, and did not channel their search or focus it on any

[12] *Rogers Communications*, at para. 25.
[13] Owlsey, at 18.
[14] ACLU at 6.
[15] *Rogers Communications.*

> individual persons until they obtained the second warrant for the Subscriber Records for several of these four Applicants. It is disingenuous to suggest that the initial Tower Dump Warrants were anything more than a high-tech "fishing expedition" of the broadest order made in the hope that some information would be obtained that would permit the police investigation to move forward.
>
> …
>
> … they resorted to a seizure of many thousands of private records of persons not remotely suspected of being involved in the robbery. In seeking the Tower Dump Warrants on November 30, 2006 … the police cast a wide net. Clearly they hoped they would land a lead that would permit their investigation to progress. It is perhaps understandable that they felt the need to take this step in light of the impasse their traditional investigation had reached, but in the course of doing so, the police systematically invaded the s. 8 *Charter* rights of several thousand people…[16]

Not only is the number of people caught by the search troubling, but the information obtained by a tower dump is also very broad. For example, in *R. v. Rogers*, the Peel Regional Police in Ontario obtained a production order requiring the name and address of every subscriber making or attempting a communication through a particular cell tower, including the information of both the person initiating the communication and the person receiving the communication. The order also required the billing information of each subscriber, including bank and credit card information.[17]

B. The Information is in the Hands of Telecommunication Companies

In this digital age, it is clear that internet and telecommunication companies, such as Telus and Rogers, are the guardians of our personal privacy. They hold a vast amount of personal information, and we rely on them to protect our data. But can we rely on the telecommunication companies to protect our privacy interests when faced with a sweeping tower dump order?

---

[16] *R. v. Mahmood* (2008), 236 C.C.C. (3d) 3 at paras. 72, 95.
[17] *Rogers Communications*, at para. 6.

If a tower dump does not reveal any suspects, and the results of the search are never presented as evidence in court, there is no opportunity to challenge or review the tower dump order. Indeed, the thousands of subscribers whose personal information was swept up in the tower dump are never even notified. Unless the service provider resists the order, the personal information of thousands of non-suspects is handed over to the state, with very little oversight and accountability.

And even if the service provider resists the order, a standing issue may arise, as the privacy interests at stake are those of the subscribers, not the companies. For example, in *R. v. Rogers Communication*, Rogers and Telus were faced with broad and onerous tower dump orders. They applied for a court ruling on the basis that the orders violated the constitutional rights of their subscribers. However, as the privacy of interests of Rogers and Telus were not implicated, the Crown argued that they lacked standing to claim any relief. If this argument had succeeded, the constitutionality of tower dump orders would never be addressed. As the Court noted, it is impractical for the service provider to give thousands of subscribers notice of the tower dump order, and it is clear that no individual subscriber would have an interest in litigating with the government over these issues.[18]

IV. RESPONSES TO THE CONCERNS: AMERICAN VS. CANADIAN APPROACH

Cell tower dumps are used as an investigative technique in several countries, but the law has not caught up to the technology. No country has enacted specific legislation regulating tower dumps, and there is relatively little jurisprudence assessing the impact of tower dumps on

[18] *Rogers Communication*, at paras. 36-37.

privacy interests. This section will examine the emerging case law in the United States and Canada.

A. The American Approach

The United States Constitution does not provide a free standing right to privacy. However, privacy interests are protected by the Fourth Amendment, which ensures that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures which guards against unreasonable searches and seizures, shall not be violated." Generally, a Fourth Amendment violation will occur where the government violates a reasonable expectation of privacy without a warrant.[19]

The U.S. Supreme Court has not commented on whether cell-site data attracts Fourth Amendment protection, and the decisions from lower courts are inconsistent.[20] However, several circuit courts have concluded that there is no reasonable expectation of privacy in this kind of information, and therefore the Fourth Amendment does not apply. The decisions note that the information does not reveal the *content* of phone calls or text messages and cell phone subscribers voluntarily turn over information about their cell phone activity and location to the service provider.[21] The Sixth Circuit Court of Appeals explained:

> This case involves an asserted privacy interest in information related to personal communications. As to that kind of information, the federal courts have long recognized a core distinction: although the content of personal communications is

[19] Kyllo v. United States, 533 U.S. 27, 33 (2001).
[20] Monu Bedi, "The Curious Case of Cell Phone Location Data: Fourth Amendment Doctrine Mash Up" (2016) 110:2 Nw. U. L. Rev. 507 at 516-519.
[21] United States v. Davis, 785 F.3d 498 (11th Cir 2015); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Carpenter, Nos. 14-1572/1805, 2016 WL 1445183 (6th Cir. 2016); United States v. Graham, No. 12-4659 (4th Cir. 2016). See also: Bedi, at 516-517.

> private, the information necessary to get those communications from point A to point B is not. …
>
> …
>
> The business records here fall on the unprotected side of this line. Those records say nothing about the content of any calls. Instead, the records include routing information, which the wireless providers gathered in the ordinary course of business. Carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls. And carriers keep records of these data to find weak spots in their network and to determine whether roaming charges apply; among other purposes. Thus, the cell-site data – like mailing addresses, phone numbers, and IP addresses – are information that facilitate personal communications, rather than part of the content of those communications themselves. The government's collection of business records containing these data therefore is not a search.

The Fourth Circuit Court of Appeals similarly reasoned:

> [t]he question before us is whether the government invades an individual's reasonable expectation of privacy when it obtains, from a third party, the third party's records, which permit the government to deduce location information. …
>
> [t]he cases that establish the third-party doctrine provide the answer. Under the third-party doctrine, an individual can claim "no legitimate expectation of privacy" in information that he has voluntarily turned over to a third party. … The Supreme Court has reasoned that, by "revealing his affairs to another," an individual "takes the risk … that the information will be conveyed by that person to the Government." … The Fourth Amendment does not protect information voluntarily disclosed to a third party because even a subjective expectation of privacy in such information is "not one that society is prepared to recognize as 'reasonable.'"… The government therefore does not engage in a Fourth Amendment "search" when it acquires such information from a third party.

It appears that there is a growing consensus among American courts that the police do not require a warrant to obtain a particular subscriber's historical cell site data from a service provider. Instead, the government can access this information pursuant to s. 2703(d) of the

Stored Communications Act,[22] which permits an electronic communications service provider to disclose stored communications when the government provides "specific and articulable facts" showing that there are reasonable grounds to believe that the records are relevant and material to an ongoing investigation. This is a less exacting standard than probable cause – the standard required to obtain a warrant.[23]

The cases described above address law enforcement requests for the cell-site data of a particular cell phone number. Few decisions address whether the Fourth Amendment applies to cell tower dumps, where government officials request information about all phone activity transmitted through a cell tower at a particular time and location. And again, the decisions are inconsistent.[24] Three opinions issued by Magistrate Judge Brian Owsley conclude that the information sought by a tower dump order is protected by the Fourth Amendment, thereby requiring a warrant based on probable cause. More recently, however, two magistrate judges concluded the opposite: based on the reasoning of recent circuit courts' decisions, a warrant is not required for a tower dump because the information requested was voluntarily disclosed to the service provider, negating any reasonable expectation of privacy.[25]

In summary, the trend in the American jurisprudence is to reject the idea that individuals have a privacy interest in cell-site data and to permit government access to this data without a warrant.

B. The Canadian Approach

[22] 18 U.S.C., ss. 2701-2712 (2012).
[23] Hodgson, at 258-260; Owsley, at See also Owsley at 13-17.
[24] Amanda Regan, "Dumping the Probable Cause Requirement: Why the Supreme Court Should Decide Probable Cause is Not Necessary for Cell Tower Dumps" (2015) 43:4 Hofstra Law Review 1189 at 1213; Owsley, at 23 – 30.
[25] *In re* Application for Cell Tower Records Under 18 U.S.C. s. 2703(d), No. H-15-136M, 2015 WL 1022018 (S.D. Tex. March 9, 2015); Regan, at 1213-1215.

In Canada, privacy interests are protected under s. 8 of the *Canadian Charter of Rights and Freedoms*, which states that "[e]veryone has the right to be secure against unreasonable search or seizure." Like the Fourth Amendment, s. 8 of the *Charter* only protects reasonable expectations of privacy. Where a reasonable expectation of privacy exists, the *Charter* requires the government to obtain a warrant before conducting a search or seizure.[26]

In contrast to American case law, Canadian courts have recognized that there is a reasonable expectation of privacy in information obtained by a tower dump order.

In *R. v. Mahmood*,[27] the Ontario police obtained a warrant requiring Bell, Rogers, Telus, and Telemobile to produce all records of cellular phone traffic that had passed through two cell towers in the vicinity of a jewelry store robbery for the hour and a half that preceded the robbery. The warrant yielded detailed records relating to over 7,000 subscribers. At trial, the accused argued that the tower dump violated their s. 8 *Charter* rights, as the warrant was not based on reasonable and probable grounds. Justice Quigley of the Ontario Superior Court agreed. He held that it was clear that the accused had a reasonable expectation of privacy in the cell phone records:

> [i]t is evident that the overwhelming and pervasive use of cell phones in Canada by an enormous percentage of the population, the advancement of cellular phone technology, and the breadth of information that may be obtained about cell phones and the people who use them, may permit such information to reveal personal and biographical matters about the users. Technological tools such as the ability to isolate and determine the cell phone traffic that passed through any particular cellular transmission tower, or simply the production of billings records with the increased information they may now capture and display, has the potential to reveal information that individuals might have expected would remain private and confidential … It is this expectation that lies at the heart of the privacy interest that

[26] *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145.
[27] *R. v. Mahmood* (2008), 236 C.C.C. (3d) 3.

> s. 8 seeks to protect in an informational context. As LaForest J. said 20 years ago in *R. v. Dyment*…:
>
> > In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish to be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which, it is divulged, must be protected.
>
> …
>
> … While it is clear to me that the nature of the information obtained cannot realistically be regarded as going to the deeper biographical core concepts of inherent dignity and personal integrity that approach the essence of a person's biography, there is no doubt that the cell phone records obtained through both warrants could and did reveal personal information that contained at least some of the elements of biographical core, in terms of providing some general identification of movement, of personal associations, and of frequency of contact with associated persons.[28]

Justice Quigley went on to find that the warrant was not based on reasonable and probable grounds, and excluded the results of the tower dump. While the constitutionality of the tower dump was not at issue on appeal, the Ontario Court of Appeal commented that a reasonable expectation of privacy attaches to cell phone records, though the expectation is one that is significantly reduced.[29]

In the recent decision of *R. v. Rogers Communications*, Justice Sproat of the Ontario Superior Court confirmed that Canadians have a reasonable expectation of privacy in the records of their cellular telephone activity. He went on to find that the production orders in that case violated s. 8 of the *Charter*, as they were overly broad: "[t]he disclosure of personal information

[28] *Mahmood*, at paras. 57, 77.
[29] *R. v. Mahmood*, 2011 ONCA 693 at paras. 127-131.

the Production Orders required went far beyond what was reasonably necessary to gather evidence concerning the commission of the crimes under investigation."[30]

Justice Sproat's decision comes in the wake of the Supreme Court of Canada's ruling in *R. v. Spencer*.[31] In *Spencer*, the Supreme Court concluded that the police cannot obtain subscribers' personal information from Internet service providers without a warrant. The protection afforded by s. 8 of the *Charter* extends to information "which *tends to reveal* intimate details of the lifestyle and personal choices of the individual."[32] This reasoning can easily be extended to cell-site data.

Canadian law, therefore, requires a warrant (or production order) based on reasonable and probable grounds before the state can obtain tower dump information. Helpfully, Justice Sproat also set out guidelines for obtaining the production order based on the fundamental principles of incrementalism and minimal intrusion:

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

[30] *Rogers Communications*, at para. 42.
[31] *R. v. Spencer*, 2014 SCC 43.
[32] *Spencer*, at para. 27.

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.[33]

V. DISCUSSION

In certain circumstances, cell tower dumps can be an extremely effective investigative tool. However, as described above, this technique raises significant privacy concerns. Without appropriate limitations, a tower dump can amount to mass surveillance, with the personal

[33] *Rogers Communications*, at para. 65.

information of hundreds of thousands of individuals being divulged to the government. The question is: how should we balance the collective right to public safety and the critical privacy interests at stake?

American and Canadian courts have struck different balances. In the United States, the balance currently weighs in favour of law enforcement. Courts have taken the view that cell-site data is not private, particularly as the data does not disclose the content of communications and it is voluntarily given to third-party service providers. In contrast, Canadian courts have sent a strong message that cell-site data attracts a reasonable expectation of privacy. Tower dumps not only require a warrant based on reasonable and probable grounds, but they must also be conducted in a way that minimally intrudes on the privacy interests of subscribers.

In this author's opinion, the Canadian approach is preferable. While the information obtained by a tower dump does not reveal the *content* of communications, it reveals personal information about one's lifestyle, including their movements and personal associations. It is clear that there is a reasonable expectation of privacy in this kind of information. As the ACLU has pointed out, a cell tower dump could be used to identify people at home in a neighbourhood on a particular night, the protestors at a political rally, or the congregants attending services at a mosque, synagogue, or church.[34] As the Ontario Superior Court has noted, "[w]hether 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."[35] And it must be remembered that tower dumps allow the police to obtain this information as it relates to *thousands* of subscribers who are unconnected to the offence, amounting to mass surveillance.

[34] ACLU, at 2.
[35] *Rogers Communications*, at para. 19.

Further, the mere fact that this information is voluntarily provided to telecommunication companies does not diminish the expectation of privacy: "situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected."[36] In other words, while a person may disclose confidential information to a third party for particular purposes, the state should not be free to conscript that information for the purposes of a prosecution.[37] The appropriate question is whether the information is the kind of information that society accepts should remain out of the state's hands.[38]

In light of these significant privacy concerns, requiring a warrant for a tower dump strikes an appropriate balance between the competing interests at stake. Justice Sproat's guidelines for obtaining a warrant are a helpful way to ensure that the tower dump is minimally intrusive.

But more is needed to protect the privacy of individuals affected by a tower dump. To date, no legislation addresses the retention, use, and disclosure of the massive amount of data seized by way of a tower dump. There are no assurances that this personal data will not be compromised. Further, there is no requirement that the state notify individuals whose information is revealed in the tower dump. The information of thousands of individuals is handed over to the state without any notification. In order to adequately protect privacy interests, legislation requiring that all affected individuals be notified of the tower dump when such notification would not jeopardize the ongoing criminal investigation should be enacted.[39]

---

[36] *R. v. Dyment*, [1988] 2 S.C.R. 417 at para. 22, per LaForest J.
[37] Steven Penney, "The Digitization of Section 8 of the Charter: Reform or Revolution?" (2014) 67 S.C.L.R. (2d) 505 at 518.
[38] *R. v. Gombac*, 2010 SCC 55 at para. 34.
[39] Owsley, at 46.

Legislative measures ensuring the confidentiality and eventual destruction of the cell-site data should also be put into place.[40]

Finally, the role of the telecommunication companies needs to be clarified. As noted above, we must rely on the telecommunication companies to assert our privacy interests in the face of an overly broad or unconstitutional tower dump order. In *Rogers Communications*, for example, Rogers and Telus resisted the tower dump order but there were other service providers who were prepared to comply with the unconstitutional order.[41] Legislation enacting Justice Sproat's guidelines would ensure that tower dump orders comply with constitutional mandates. However, in the event that the order appears overly broad, the law should be clear that telecommunication companies have an obligation to protect the private information of their subscribers and standing to challenge such orders.

VI. CONCLUSION

Cell phones have become an essential part of our everyday lives. However, our phones leave a trail behind us, revealing where we went and who we communicated with. This, of course, is useful information in criminal investigations. In particular, cell tower dumps can be an extremely effective investigative technique in situations where the police need to identify a suspect. However, tower dumps are broad searches, resulting in the seizure of significant amounts of information about thousands of individuals without any notification or assurances about the retention, use or disclosure of the data. Indeed, 99.9% of the individuals affected by

[40] Owsley, at 48.
[41] Keith Rose, "Phone Companies after R. v. Rogers: Constitutional Guardians or Agents of the State", January 20, 2016, online: http://www.canadiancybersecuritylaw.com/2016/01/phone-companies-after-r-v-rogers-constitutional-guardians-or-agents-of-the-state/?platform=hootsuite.

tower dumps are completely unconnected to the offence being investigated and are never made aware that their information was disclosed to law enforcement officials.

In the absence of any legislation directly addressing tower dumps, it has been left to the courts to regulate the use of this investigative power. The Canadian judicial response to the significant privacy concerns associated with tower dumps is a step in the right direction. However, legislative measures are required. Justice Sproat's guidelines should be endorsed by governments in legislation and legislative measures should be taken to ensure that all subscribers are notified when the police obtain their private information from the service provider. Further, regulations should be enacted to address the state's retention, use and disclosure of this information. These steps will ensure that privacy rights are adequately protected, while still advancing society's interest in effective law enforcement.