Open Media Engagement Network (OpenMedia)
1424 Commercial Drive
P0 Box #21674
Vancouver|BC|V5L 5G3
https://openmedia.org

Written Inquiry Under Part 5 of the *Freedom of Information & Protection of Privacy Act ("FIPPA") of British Columbia*

In re: Vancouver Police Department

Submission of OpenMedia, Intervenor

BC OIPC File No: F15-63155 // Public Body File No: 15-2106A

March 23, 2016

Tamir Israel, Staff Lawyer, Canadian Internet Policy & Public Interest Clinic (CIPPIC)
Christopher Parsons, Post-Doctoral Fellow, Citizen Lab, Munk School of Global Affairs, University of Toronto

TABLE OF CONTENTS

INTRODUCTION

1. The Open Media Engagement Network (OpenMedia) is pleased to provide its intervention in BC OIPC File No F15-63155. This Inquiry concerns a Public Body, the Vancouver Police Department's ("VPD") refusal to respond to a request for records relating to the use of Cell Site Simulators, sometimes colloquially referred to as 'IMSI Catchers' and known by brand names such as 'Stingray' or 'King Fisher'. The Applicant in this matter has requested all records in VPD's control relating to IMSI Catchers. VPD has refused said request, invoking paragraph 8(2)(a) and section 15 of the British Columbia *Freedom of Information and Protection of Privacy Act* ("*BC FIPPA*"). The Applicant challenges this refusal, giving rise to the underlying inquiry that this intervention addresses. A Notice of Written Inquiry into this matter was issued on January 25, 2016, with the objective of determining whether VPD is authorized to refuse disclosure of responsive records or confirmation of the presence thereof, as per paragraph 8(2)(a) and section 15 of *BC FIPPA*.[1]

2. IMSI Catchers are a highly invasive mobile device surveillance tool that has witnessed significant growth in usage amongst law enforcement agencies in response to the decreasing costs of such devices and the modern-day ubiquity of mobile phones.[2] The invasiveness of IMSI Catchers arises from a number of features associated with the devices and their use. First, their capacity for self-deployment permits government agencies to intercept data without intermediation, excluding an important possible check on over-broad deployment.[3] Second, the collateral impact of IMSI Catchers is always high, as they are designed to intercept data from *all* devices in range, meaning that many innocent individuals' privacy will be affected

[1] *Re: Vancouver Police Department*, Notice of Written Inquiry, OIPC File No: F15-63155, January 25, 2016, (BC IPC), p 2.
[2] Robert Kolker, "What Happens When the Surveillance State Becomes an Affordable Gadget?", *Bloomberg*, March 10, 2016, http://www.bloomberg.com/news/articles/2016-03-10/what-happens-when-the-surveillance-state-becomes-an-affordable-gadget.
[3] Comparable information can generally be obtained directly from service providers, where over-broad requests can be challenged and safeguards can be inserted: *R v Rogers Communications*, 2014 ONSC 3853; *R v Rogers Communications*, 2016 ONSC 70.

alongside each legitimate surveillance target.[4] Finally, the data most commonly obtained by IMSI Catchers is sensitive, revealing anonymous activity and facilitating tracking of individuals.[5] These intrusive features of IMSI Catchers have led many internal policy-makers, legislatures and courts in other jurisdictions to conclude that IMSI Catcher use must be strictly regulated. However, such regulation – or even discussion of its need – cannot occur until government agencies confirm that they are using such devices.

3. This intervention argues that VPD must disclose any pertinent records in its control or confirm that no such records exist. VPD use of IMSI Catchers raises pressing public policy concerns that can only be addressed if information related to their use becomes public.

4. This intervention begins by outlining how IMSI Catchers function. Next, we demonstrate how the test for investigative necessity advanced by VPD simply does not apply to responsive records in light of the significant general information regarding IMSI Catcher use. Finally, we argue that even if disclosure of responsive records will, to some degree, undermine the utility of IMSI Catchers as an investigative tool, disclosure must still occur. Confirmation of IMSI Catcher use is a necessary precursor to informed public debate and to the proper legal constraint of an invasive surveillance tool and is therefore in the public interest.

I. IMSI Catchers in Context: Capabilities & Public Knowledge

5. There is significant information regarding the functionalities, capabilities and common uses of IMSI Catchers on the public record. However, this information emerges primarily from other

[4] See for example: *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div): "The concern over the collection of innocent third parties' information is not theoretical. It has been reported that the federal government collects telephone numbers, maintains those numbers in a database and then is very reluctant to disclose this information."
[5] *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212, para 43; Office of the Information and Privacy Commissioner of Ontario, "Surveillance Then and Now: Securing Privacy in Public Spaces", June 2013, https://www.ipc.on.ca/images/Resources/pbd-surveillance.pdf; *R v Rogers Communications*, 2016 ONSC 70, para 20; Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," A/HRC/23/40, April 17, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, para 36.

jurisdictions, where its publication has fueled robust public debate and the adoption of restrictions designed to limit the raw invasive capacities of IMSI Catchers, and variously imposed by legislatures, courts or directly by internal government policy-makers. In this section, we outline the invasive capabilities of IMSI Catchers, documented public sector uses of the devices, and some of the challenges that have delayed important policy changes abroad by frustrating transparency efforts.

IMSI Catcher Functionalities

6. IMSI Catchers, also known as Cell Site Simulators, are designed to impersonate cellular telecommunications towers. Mobile devices carried by individuals will connect to a cell site simulator, send information to it and accept instructions from it because they are designed to trust mobile cellular towers. IMSI Catchers are capable of a number of invasive activities, including the wholesale interception of communications and sending of executable instructions to a mobile device. However, IMSI Catchers are primarily used by law enforcement to intercept identification information transmitted by mobile devices.

7. The operator of an IMSI Catcher can set it to either 'identification' or 'camping' mode.[6] The former involves collecting identifiers such as the International Mobile Subscriber Identifier (IMSI) and International Mobile Equipment Identification (IMEI) numbers and subsequently passing the mobile device's communications to a legitimate cell tower. In identification mode, the IMSI Catcher will only interact with a mobile device long enough to identify the device and will then redirect the device to a legitimate cell tower, ending the interaction. In camping mode, by contrast, the IMSI Catcher retains the connection, continuously remaining in the 'middle' of all communications sent and received over the cellular network by proximate mobile devices. So

[6] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. (2014). "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," Conference Proceedings of the Annual Computer Security Applications Conference (ACSAC 2014), https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

while 'identification' mode entails interception of unique identifiers transmitted between mobile devices and service providers, 'camping' mode intercepts everything. Using IMSI Catchers in camping mode, operators can "deliver geo-targeted spam, send operator messages that reconfigure the phone … directly attack SIM cards with encrypted SMS … and can potentially intercept mobile two-factor authentication schemes (mTAN)."[7]

8. In identification mode, IMSI Catchers are limited to intercepting identifying information persistently associated with a particular device in a particular location at a particular time. Mobile devices such as cell phones communicate with neighbouring cellular towers, often a few times per second. Each communication will geo-locate the mobile device and send unique identifying information, including the IMSI and IMEI numbers.[8] IMSI numbers are bonded to the Subscriber Identity Module (SIM) that individuals place in their mobile devices to receive cellular service from a mobile telecommunications company.[9] The IMEI is bound to each handset device and as such is a persistent identifier that can be associated with the owner of that device. The heightened invasiveness of IMSI Catchers relative to other surveillance tools emerges from their capacity for self-deployment, their penchant for high collateral impact on the privacy of non-targets and the sensitive nature of the information their use can reveal.

9. Given the ubiquity of mobile devices today, the ability to intercept persistent mobile identifiers can facilitate a range of revealing activity, such as:

- Identifying a mobile device associated with a targeted individual using an unknown mobile device to facilitate a wiretap or other electronic surveillance power;[10]

[7] Dabrowski, *supra* 6.
[8] Citizen Lab, "The Many Identifiers in Our Pockets: A primer on mobile privacy and security," *Citizen Lab*, May 13, 2015, [Citizen Lab I], https://citizenlab.org/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/ .
[9] Citizen Lab I. *supra.* 8.
[10] See *Maryland v Taylor*, Case No 11410031, Suppression Hearing, November 21, 2014, TRANSCRIPT, [*Maryland v Taylor*, Transcript] https://assets.documentcloud.org/documents/2291303/md-v-shemar-taylor-stingray-hearing.pdf, p M-17: "[Detective Allen Savage |] A: I just called them up to see if they could ride by and see if the phone was in the house. [Joshua Insley, Counsel for the Defence |] Q: Okay.

- Locating a specific known device at an unknown location;[11]
- Identifying anonymous individuals at a specific location, in a specific interaction or association, or at a specific event;[12] or
- Tracking the physical movements of individuals pervasively.

A mobile identifier obtained for one of these objectives (identifying a mobile device for use of other powers) can later be used for another objective (tracking the movements of that device).

10. The geo-location capabilities of IMSI Catchers are a function of their ability to associate an intercepted identifier with the time of its interception, the known location and range of the IMSI Catcher at time of interception and the mobile device's signal strength upon interconnection. A single IMSI Catcher can yield quite specific geo-location information if strategically deployed – for example, if placed at the epicenter of a political protest, at a border crossing, or near the entry to a health clinic. Where multiple IMSI Catchers are deployed simultaneously, location can be determined with even greater precision by means of triangulation.[13] Dispersing multiple IMSI Catchers can also facilitate pervasive tracking, as individuals traverse from one IMSI Catcher's geographical range to the next, revealing their path and companions.[14]

11. Regardless of whether multiple or single IMSI Catchers are used, the devices operate in an indiscriminate and automated manner, affecting the communications of all devices within their proximity; they capture data through walls and over hedges, and penetrate spaces that attract heightened privacy expectations such as homes, public restrooms and change rooms.

So you asked them to do a ride by? A Yes, sir. Q Why would you ask them to do that? A Just to put in the application for the search warrant more probable cause to establish that the phone was active in that area."

[11] Brad Heath, "Police secretly track cellphones to solve routine crimes," *USA Today*, August 24, 2015, http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

[12] Fruzsina Eordogh, "Evidence of 'Stingray' Phone Surveilance by Police Mounts in Chicago", *Christian Science Monitor*, December 22, 2014, http://www.csmonitor.com/World/Passcode/2014/1222/Evidence-of-stingray-phone-surveillance-by-police-mounts-in-Chicago.

[13] Teresa Scassa and Anca Sattler, "Location-Based Services and Privacy", (2011) 9 *Canadian J of L & Tech* 99, https://ojs.library.dal.ca/CJLT/article/download/4848/4367, p 102.

[14] Ashkan Soltani and Craig Timberg, "Tech firm tries to pull back curtain on surveillance efforts in Washington," *The Washington Post*, September 17, 2014, https://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html

12. While the digital identifiers obtained by IMSI Catchers are relatively innocuous, in and of themselves, they are the key by which a rich biographical profile can be built. As noted in a recent report on IMSI Catcher use (footnotes preserved):

> [w]hile the identifiers intercepted by IMSI Catchers do not, in and of themselves, reveal the name or contact information of an individual being tracked, their status as persistent identifiers nonetheless renders their collection intrusive. Mobile devices are "intimately linked to … individuals", meaning that IMSIs/IMEIs (like other communication device identifiers) operate as digital footprints, left behind as we traverse the physical and digital world.[15] Such identifiers have significant invasive capacity because they allow for otherwise distinct, anonymous and unlinkable activity to be connected and compiled into a profile.[16] Detailed information can be gleaned from the locations we visit.[17] In addition, tracking IMSI/IMEI identifiers across mobile locations can act as a means of contact chaining, that is, the identifiers can be used to determine which individuals are associated with which other individuals.[18] This in turn implicates associational privacy.[19] IMSI/IMEI identifiers can also be used to identify digital activities such as web browsing.[20] All of this tracking and profiling can occur without any need to ever match a compiled profile to an individual's specific name or address. Yet it is in the collection of the IMSI/IMEI that the privacy invasion occurs, as a permanent record is created, which indicates that a particular person was at a particular location (digital or otherwise) at a particular time.[21]

Moreover, identifiers obtained by IMSI Catchers can be readily linked to real-world identities either by compiling subscriber data associated with mobile identifiers from telecommunications companies or by analyzing the geographic movements of the mobile device and its owner. Geo-location information is highly identifiable information – one study found that 95% of individuals

[15] Article 29 Data Protection Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices," European Commission, Adopted on May 16, 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, p 7.

[16] See examples in: Andrea Slane and Lisa M Austin, "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations," (2011) 57 *Criminal L Quarterly* 486, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2062404, p 501.

[17] Scassa, *supra* 13, pp 109-113.

[18] Washington Post. (2015). "How the NSA is Tracking People Right Now," retrieved November 27, 2015, https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-tracking-people-right-now/634/. Contact links are developed through a technique called 'co-traveler analytics'.

[19] *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 SCR 425, per La Forest, J, concurring, para. 141, ("It is for the individual to decide what persons or groups he or she will associate with...One does not have to look far in history to find examples of how the mere possibility of the intervention of the eyes and ears of the state can undermine the security and confidents that are essential to the meaningful exercise of the right to make such choices.").

[20] Adam Senft, Andrew hilts, Christopher Parsons, Jakub Dalek, Jason Q. Ng, John Scott-Railton, Katie Kleemola, Masashi Crete-Nishihata, Ron Deibert, and Sarah McKune, "A Chatty Squirrel: Privacy and Security Issues with UC Browser," *Citizen Lab*, May 21, 2015, https://citizenlab.org/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/.

[21] Tamir Israel & Christopher Parsons, "Going Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada", *Citizen Lab & Canadian Internet Policy & Public Interest Clinic*, January 2016, Tentative Discussion Draft, [Going Opaque], pp 6-7.

were unique based on four cell-tower obtained geo-spatial data-points alone.[22] Owners of devices can be permanently identified by process of visual elimination as well.[23]

13. The ability to self-deploy more generally renders IMSI Catchers more intrusive than other mechanisms for obtaining comparable information. Other tools for accessing cell tower-obtained information require the participation of a mobile service provider, which can then act as a check on more excessive requests, and even a pre-filter to move unnecessary information, an opportunity to impose additional safeguards, an external gauge of the appropriateness of advanced exigent circumstances, and an independent record of state search activities.[24] The ability to self-deploy IMSI Catchers bypasses all of these safeguards, making over-deployment of IMSI Catchers more likely. Individual detection of IMSI Catcher use is possible, with commonly available mobile applications designed to expose such devices. However, methods for doing so are in their infancy and remain imperfect.[25] Moreover, even where an IMSI Catcher can be identified, this will not reveal *who* has deployed or for *what* purpose, meaning any over-deployment will likely remain unchallenged.[26]

14. Finally, IMSI Catchers operate in a manner that is inherently overbroad with heavy collateral privacy impact on non-targets. Like cell towers, IMSI Catchers are designed to intercept all identifiers within range indiscriminately, and without regard as to whether the data is

[22] Yves-Alexandre de Montjoye, César A Hidalgo, Michel Verleysen, and Vincent D Blondel. (2013). "Unique in the Crowd: The Privacy Bounds of Human Mobility", (2013) 3(1376) *Scientific Reports*, http://www.nature.com/articles/srep01376.
[23] *Re Application*, *Illinois*, *supra* 4: "By activating the [cell-site simulator] device, the cell phones in a geographical area will send their signals to the device, which in turn captures the information. This process can be repeated at a later time and different location so that the target's cell phone [IMEI] or IMSI can be identified among all the other cell phone telephone information previously captured. (Basically, by process of elimination, the target's cell phone number is identified.)"
[24] See Gone Opaque, *supra* 21, Box 4: Direct & Unmediated Access to Data and in particular the reasoning in: *R v Rogers Communications,* 2014 ONSC 3853; *R v Rogers Communications*, 2016 ONSC 70 on ability of provider to challenge over-broad requests and present evidence that would not be present in *ex parte* applications.
[25] See in particular: *R v Rogers Communications,* 2014 ONSC 3853; *R v Rogers Communications*, 2016 ONSC 70.
[26] Soltani, *supra* 14, Ryan Gallagher, "Criminals May be Using Covert Mobile Phone Surveillance Tech for Extortion", *Slate*, Aug 22, 2012, http://www.slate.com/blogs/future_tense/2012/08/22/imsi_catchers_criminals_law_enforcement_using_high_tech_portable_devices_to_intercept_communications.html.

emerging from public or private spaces within range.[27] More powerful IMSI Catcher devices, often referred to as DRT Boxes, have amplified ranges that can be used to sweep entire cities.[28] Once obtained, there is no clear and direct obligation on state agencies to limit retention or secondary use of collaterally obtained identifiers.[29] This collateral privacy impact further heightens the intrusiveness of these devices.

State Agency Use of IMSI Catchers

15. There have been many documented and hypothetical examples of IMSI Catcher use by state agencies, providing a comprehensive picture of the devices' likely deployment scenarios:

- Confirming presence of a device in a target's home prior to a search thereof;[30]
- Identifying an individual responsible for sending harassing text messages;[31]
- Locating a stolen mobile device as a precursor to searching homes in the vicinity;[32]
- Locating specific individuals by driving around a city until a known IMSI is found;[33]
- Mounted on airplanes by the United States Marshall Service to indiscriminately sweep entire cities for a specific mobile device;[34]
- To monitor all devices within range of a prison to determine whether prisoners are

[27] *Re Application, Illinois*, *supra* note 4: "Although the operator of a cell-site simulator can use a directional antenna to direct the simulator's signal toward a certain area (sometimes referred to as "directional finding"), the cell-site simulator will still force many innocent third parties' cell phones to direct their signals to the simulator. … By activating the device, the cell phones in a geographical area will send their signals to the device, which in turn captures the information."

[28] Devlin Barrett, "Americans' Cellphones Targeted in Secret U.S. Spy Program," *The Wall Street Journal*, November 13, 2014, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

[29] Targeting, retention and secondary use obligations have been imposed where IMSI Catchers *have* been expressly examined in other jurisdictions and in comparable contexts in British Columbia: *Re Use of Automated License Plate Recognition Technology by the Victoria Police Department*, Investigative Report F12-04, November 15, 2012 (BC IPC) [BC IPC, ALPR]; *Re Application, Illinois*, *supra* note 4. But see, partially *contra*, *R v Rogers Communications*, 2016 ONSC 70.

[30] See *Maryland v Taylor*, Transcript, *supra* note 10, p M-17: "[Detective Allen Savage |] A: I just called them up to see if they could ride by and see if the phone was in the house. [Joshua Insley, Counsel for the Defence |] Q: Okay. So you asked them to do a ride by? A Yes, sir. Q Why would you ask them to do that? A Just to put in the application for the search warrant more probable cause to establish that the phone was active in that area."

[31] Heath, *supra* 11.

[32] *Maryland v Redmond*, (2013) 73 A.3d 385 (Maryland Court of Special Appeals), pp **403-404 (device later identified by a police log to be an IMSI Catcher: Heath, supra 11). See also: Kate Klonick, "Stingrays: Not Just for Feds!", Slate, November 10, 2014, http://www.slate.com/articles/technology/future_tense/2014/11/stingrays_imsi_catchers_how_local_law_enforcement_uses_an_invasive_surveillance.html: "The problem with Stingrays is twofold. Goldsberry's case illustrates the first: Stringrays simply don't provide reliable results—if a cellphone is located near a wall separating two apartments, it is nearly impossible to determine which apartment that phone is in."

[33] *Florida v Thomas*, Case No: 2008-CF-3350A, Suppression Hearing, August 23, 2010, TRANSCRIPT, pp 22-23, [*Florida v Thomas*, Transcript] See: https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf; Heath, supra 11: "'We're out riding around every day,' said one officer assigned to the surveillance unit, who spoke on the condition of anonymity because of the department's non-disclosure agreement with the FBI. 'We grab a lot of people, and we close a lot of cases.'"

[34] Barrett, *supra* 28.

using cell phones;[35]
- Reportedly at political protests to identify devices of individuals attending;[36]
- To monitor activity in the offices of an independent Irish police oversight body.[37]

Additional hypothetical usage scenarios can be advanced as common sense extensions of the generally known capabilities of the devices.

IMSI Catcher Transparency & Obfuscation

16. As with many other electronic surveillance tools, the surreptitious nature of IMSI Catchers renders their detection difficult. While their general use has been inferred in a number of jurisdictions, confirmation of such use has proven more difficult to achieve, due to persistent attempts to obfuscate this usage. These transparency challenges have delayed significant policy debates. Where transparency *has* been achieved it has led to the imposition of meaningful restraints on the use of such devices, with the object of curtailing their more intrusive potential.

17. In the United States in particular, significant initial obfuscation efforts were overcome, eventually leading to a rich and detailed public record and several legal and policy constraints. The obfuscation efforts in question have led law enforcement agencies to withhold disclosure of these devices' use from courts and defence attorneys,[38] and even to invent informants in order to place information gained from IMSI Catchers on the record without publicly disclosing

[35] Colin Freeze & Matt Braga, "Surveillance Device Used in Prison Sets Off Police Probe", *The Globe and Mail*, March 14, 2016, http://www.theglobeandmail.com/news/national/opp-launch-criminal-probe-into-use-of-surveillance-device-in-federal-prison/article29240374/.
[36] Eordogh, *supra* 12.
[37] Privacy International and Digital Rights Ireland, "The Right to Privacy in Ireland," *Digital Rights Ireland*, September 2015, https://www.digitalrights.ie/dri/wp-content/uploads/2015/12/Ireland_UPR-Stakeholder-Submission-DRI-and-Privacy-International_FINAL.pdf, para 54.
[38] Ellen Nakashima, "FBI clarifies rules on secretive cellphone-tracking devices," *The Washington Post*, May 14, 2015, retrieved November 16, 2015, https://www.washingtonpost.com/world/national-security/fbi-clarifies-rules-on-secretive-cellphone-tracking-devices/2015/05/14/655b4696-f914-11e4-a13c-193b1241d51a_story.html.

their use.[39] United States officials have gone so far as to drop important evidence[40] and enter into unfavourable plea agreements to prevent disclosure of IMSI Catcher use.[41] Entire cases have reportedly been dropped to avoid revealing the use of this technology.[42]

18. In time, however, these obfuscation efforts were overcome, leading to a robust and informed debate regarding the appropriate use of these invasive tools. Formal and official acknowledgement of IMSI Catcher use came slowly. Such acknowledgement was a precondition to the adoption of any legal or policy restraints. The rarity of judicial decisions referencing IMSI Catchers is indicative of the potential impact that ongoing obfuscation can have. There is evidence to suggest widespread IMSI Catcher use, however it appears that magistrates and courts in the United States were authorizing use of these devices without a clear understanding of their invasive capabilities.[43] In one indicative court case from Baltimore, counsel for the State was emphatic in its denials that no IMSI Catcher was used:

> … the crux of the Defendant's motion is that the police used a machine that the Defense is calling a StingRay machine. We have informed Defense that that was not used in this case. We've put that in writing in our response. … I can't turn over something that doesn't exist. And I can say until I'm blue in the face that the device wasn't used and that the … StingRay device [was not used for tracking].[44]

Both the prosecution and law enforcement, under direct questioning, testified that the mobile

[39] Maria Kayanan, "Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking," *American Civil Liberties Union*, June 19, 2014, https://www.aclu.org/blog/internal-police-emails-show-efforts-hide-use-cell-phone-tracking.
[40] Cyrus Farivar, "Prosecutors Drop Key Evidence at Trial to Avoid Explaining 'stingray' use", *Ars Technica*, November 18, 2014, http://arstechnica.com/tech-policy/2014/11/prosecutors-drop-key-evidence-at-trial-to-avoid-explaining-stingray-use/.
[41] Kayanan, *supra* 39; *Re Application, Illinois*, *supra* 4.
[42] Cyrus Farivar, "FBI would rather prosecutors drop cases than disclose stingray details," *Ars Technica*, April 7, 2015, http://arstechnica.com/tech-policy/2015/04/fbi-would-rather-prosecutors-drop-cases-than-disclose-stingray-details/.
[43] Stephanie K. Pell and Christopher Soghoian, "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy", (2014), 28(1) *Harvard J of Law & Tech* 1, http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf, pp 35-36 provide examples of this where IMSI Catcher authorization was sought under authorizations of general application – typically pen register authorization, comparable to a transmission data recorder application under s 492.2 of the Canadian *Criminal Code* – without any indication of the greater invasive capacity of these devices.
[44] *Maryland v Taylor*, *Transcript*, *supra* 10, pp M-5, M-87. Another police detective, John Haley, similarly testified that no IMSI Catcher was used in this case (p M-48): "That's a no, 'cause we did not."

device at issue was located using historical cell-site information obtained from the mobile provider as opposed to the more invasive IMSI Catchers.[45] Later, after the case ended, reporters discovered a surveillance log confirming that an IMSI Catcher was, in fact, used prompting defence counsel to seek reconsideration of the outcome.[46]

19. Following exposure through academic papers,[47] direct detection,[48] freedom of information requests,[49] extensive reporting, and rare judicial decisions,[50] transparency in the United States reached a tipping point in 2015, when a number of agencies officially confirmed IMSI Catcher use. This led to a proliferation of restraints, including state and municipal legislation,[51] policies adopted by the federal Departments of Justice and Homeland Security,[52] and judicial decisions.[53]

20. To date, there has been no comparable transparency in Canada. Freedom of Information requests and parliamentary queries have so far yielded no confirmation of IMSI Catcher use.[54]

---

[45] *Ibid*. For another case example, also from Maryland, see: *Maryland v Redmond*, *supra* 32, pp **403-404 ("to the extent that the averments in the search warrant application represent that the ATT detectives used 'sophisticated' means to locate the stolen cell phone while at the scene on the afternoon of March 2, 2010, they are simply inaccurate.").

[46] Nicky Woolf, "2,000 cases may be overturned because police used secret Stingray surveillance," *The Guardian*, September 4, 2015, http://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance. Re *Redmond*, see: Heath, *supra 11*.

[47] Pell & Soghoian, *supra* 43, being the most notable, comprehensive and widely effective example.

[48] Soltani, *supra* 14.

[49] For one example of a few: *ACLU of NC v Department of Justice*, (2014) 70 F.Supp.3d 1018, (N Dist California).

[50] Pell and Soghoian, *supra* 43 p 35 noted in 2014 that: "Despite the fact that U.S. government agencies have used cellular surveillance devices for more than twenty years, [a 2012 magistrate] opinion is one of only two known published magistrate opinions to address law enforcement use of this technology." In a more recent example, it has been demonstrated that at least two (but likely many more) State of Maryland courts expressly asked about IMSI Catcher use and were expressly told no such use was made, only to be contradicted by later developments (see discussion at *infra* footnotes 44 - 46.

[51] Hanni Fakhoury, "Stingrays Go Mainstream: 2014 in Review," *Electronic Frontier Foundation*, January 2, 2015, https://www.eff.org/deeplinks/2015/01/2014-review-stingrays-go-mainstream; Cyrus Farivar, "California cops, want to use a stringray? Get a warrant, governor says," *Ars Technica*, October 8, 2015, http://arstechnica.com/tech-policy/2015/10/california-governor-signs-new-law-mandating-warrant-for-stingray-use/; Christian Stork. (2015). "Alameda County becomes first in state to regulate cellphone surveillance tool," *Oakland North*, November 19, 2015, https://oaklandnorth.net/2015/11/19/alameda-county-becomes-first-in-state-to-regulate-cellphone-surveillance-tool/.

[52] "Use of Cell-Site Simulator Technology", Department of Justice Policy Guidance, September 3, 2015, [DOJ Policy] https://www.justice.gov/opa/file/767321/download; Department of Homeland Security, "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," October 19, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.

[53] *Re Application, Illinois, supra* 4.

[54] See *Gone Opaque*, *supra* 21, pp 14-16. One agency, the Canadian Border Services Agency (CBSA) did confirm that they do not use

Recently, the tide has begun to turn. One appeal of a Freedom of Information request was denied by the Ontario Office of the Information and Privacy Commissioner, however the Commissioner later noted, regarding the appeal: "it's not apparent … that the public interest was given full consideration … Were we to have another appeal, I think it could lead to a different conclusion…"[55] More recently, Corrections Services Canada (CSC) employees launched a judicial review of CSC's decision to install IMSI Catcher-like devices in a prison, highlighting concern over collateral impact on non-prisoners.[56] The incident also triggered a police investigation, as it appears the devices were deployed without lawful authorization in possible violation of criminal laws.[57] Further, the Québec Superior Court of Justice appears to have ordered the RCMP to disclose their use of an IMSI Catcher-like device in the course of a criminal trial — however this decision has been appealed.[58] Finally, journalists have discovered that the Canadian government has not yet authorized the use of IMSI Catchers in Canada, though it was concerned the RCMP or other agencies might be using them without seeking such authorization.[59]

21. In spite of all these efforts, there is still little confirmation of IMSI Catcher use by Canadian law enforcement and other agencies. That lack of knowledge has been an obstacle to meaningful debate regarding the use of these devices and whether such use should be regulated in a

"tracking products, infiltration software or interception hardware" in response to a parliamentary question: Minister of Public Safety and Emergency Preparedness's Responses to MP Charmaine Borg's Q-233 Order Paper Questions, March 24, 2014, https://www.christopher-parsons.com/Main/wp-content/uploads/2014/03/8555-412-233.pdf; *Toronto Police Services Board (Re)*, Order No MO-3236, [2015] OIPC No 168 (ON IPC).

[55] Robin Levinson King, "The cellphone spyware the police don't want to acknowledge," *Toronto Star*, December 15, 2015, http://www.thestar.com/news/canada/2015/12/15/the-cellphone-spyware-the-police-dont-want-to-acknowledge.html; *Toronto Police Services Board (Re)*, Order No MO-3236, [2015] OIPC No 168 (ON IPC); Further critique in *Gone Opaque*, *supra* 21, pp 16-27.

[56] Freeze & Braga, *supra* 35.

[57] *Ibid*.

[58] Colin Freeze, Matt Braga & Les Perreaux, "RCMP Fight to Keep Lid on High-Tech Investigation Tool", *Globe and Mail*, 13 March, 2016, http://www.theglobeandmail.com/news/national/rcmp-trying-to-keep-lid-on-high-tech-methods-used-to-fight-mafia/article29204759/. Information relating to what appears to have been an IMSI Catcher (referred to as an "Identification Dispositif Mobile") was ordered to be disclosed. See: *Mirarchi v R*, 2012 QCCS 7087, paras 63-64, for description of dispute. Decision regarding disclosure of IMSI Catchers is on appeal: *R v Mirarchi*, File No: 500-10-006048-159 (Québec Court of Appeal).

[59] Mathew Braga and Colin Freeze. "Agencies did not get federal authorization to use surveillance devices," *The Globe and Mail,* March 21, 2016, http://www.theglobeandmail.com/news/national/agencies-did-not-get-federal-authorization-to-use-surveillance-devices/article29322700/.

manner similar to that adopted by other agencies. The need for such debate creates a compelling public interest that, as we argue in the final section of this intervention, would override any potential risk to the effectiveness of IMSI Catchers that might result from disclosure of responsive records sought in this inquiry. Before turning to that analysis, however, we argue that disclosure of responsive records will do little to compromise the ongoing utility of IMSI Catchers as an investigative tool.

II. Disclosure of Records Poses No Threat to Investigative Techniques

22. Beyond VPD's facial invocation of the investigative techniques exception encoded in paragraph 15(1)(c), the record of this inquiry does not currently reflect any detail as to why VPD believes that disclosure of any responsive records or of their hypothetical non-existence would harm the effectiveness of IMSI Catchers as an investigative technique. As outlined below, no such argument can be successfully advanced in this context. The public record is already rich with general details as to the capabilities of IMSI Catchers and how law enforcement might use them. Confirmation that a particular agency – VPD – is using these tools does not pose a risk of harm that meets the investigative necessity test. Moreover, confirmation of a particular agency's IMSI Catcher use will eventually emerge through the criminal discovery process, meaning that refusal of this request will at best delay such confirmation.

The Test for Investigative Techniques

23. VPD invokes subsection 8(2) and paragraph 15(1)(c) of the *BC FIPPA* as justification for its with-holding of any records potentially responsive to the request in question.[60] Paragraph 15(1)(c) permits a public body to refuse disclosure of request-responsive records where it can be reasonably expected that disclosure would "harm the effectiveness of investigative techniques

[60] *Re: Vancouver Police Department*, Investigator's Fact Report, OIPC File No: F15-63155 (BC IPC).

and procedures currently used, or likely to be used, in law enforcement."[61] Further to paragraph 8(2)(a), a public body may refuse to confirm or deny the existence of a responsive record when invoking paragraph 15(1)(c).[62]

24. The investigative necessity exception is a 'harms-based exception'. The onus is on the agency invoking the exception to provide grounds demonstrating that releasing the information sought creates a risk of harm that is probable, not speculative.[63] It is insufficient to demonstrate that release of the responsive records would "increase the chances" that the harm will result by some factor.[64] Agencies must present "concrete factors" that "establish a clear and direct connection between the disclosure of withheld information and the alleged harm."[65] This can only be accomplished by "providing evidence 'well beyond' or 'considerably above' a mere possibility of harm"[66] and entails a level of specificity that excludes justifications based on generalized risks.[67]

[61] *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 [*BC FIPPA*].
[62] *Ibid.*
[63] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31, paras 48-54.
[64] *British Columbia (Minister of Citizens' Services) v British Columbia (Information and Privacy Commissioner)*, 2012 BCSC 875, paras 47, 49 and 58-59, citing with approval *Re British Columbia (Ministry of Citizens' Services)*, Order F10-39, [2010] BCIPCD No 59, paras 11 and 16.
[65] *British Columbia (Minister of Citizens' Services v British Columbia (Information and Privacy Commissioner)*, 2012 BCSC 875, para 58-59.
[66] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31, paras 48-54; *British Columbia (Minister of Citizens' Services v British Columbia (Information and Privacy Commissioner)*, 2012 BCSC 875; *Re British Columbia (Ministry of Aboriginal Affairs and Reconciliation)*, Order F16-05, [2016] BCIPC 4, (BC IPC), paras 23-24.
[67] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31, para 60; *Ontario (Community and Social Services) v Doe*, 2015 ONCA 727, para 27-29 (general evidence that some employees had received threats is not sufficient proof that releasing the names of specific employees proves well beyond a 'mere possibility' that disclosure will lead to threats); *Toronto Star Newspapers Ltd v Ontario*, [2005] 2 SCR 188, 2005 SCC 41, para 36: "In support of its application, the Crown relied exclusively on the affidavit of a police officer who asserted his belief, 'based on [his] involvement in this investigation that the release of the Warrants, Informations to Obtain and other documents would interfere with the integrity of the ongoing police investigation'. The officer stated that, should the contents of the information become public, witnesses could be fixed with information from sources other than their personal knowledge and expressed his opinion 'that the release of the details contained in the Informations to Obtain [the search warrants] has the potential to make it more difficult for the Ontario Provincial Police to gather the best evidence in respect of its investigation'"; *British Columbia (Minister of Citizens' Services v British Columbia (Information and Privacy Commissioner)*, 2012 BCSC 875, paras 49, 58-59: (disclosing names of internal system software and server locations may generally reduce practical barriers to an unauthorized breach of a computer system but does not amount to specific proof of risk): "I am satisfied the Adjudicator's finding that the Ministry failed to establish a clear and direct connection between the disclosure of the withheld information and the alleged harm, falls within a range of possible, acceptable outcomes which are defensible in respect of the facts and law… The Adjudicator informed the Ministry precisely what it lacked: concrete factors to demonstrate there was a reasonable expectation that sensitive government information would be "hacked" or otherwise compromised

25. Where general information regarding an investigative technique is already on the public record, the investigative techniques exception cannot typically be advanced to shield responsive records from disclosure, as the additional risk of disclosure to the effectiveness of such a technique is minimal.[68] If the responsive records contain information that can be derived by common sense inferences from public knowledge there can be no direct risk to the ongoing utility of the investigative technique in question that can result from disclosure of those records.[69] Put another way, merely confirming that a public body is making use of one of a range of publicly known techniques will not generally pose a sufficiently direct.

26. Finally, assessing whether the risk of harm in question rises to the level necessary to invoke the exception is, in part, a normative exercise. The sufficiency of the risk must be weighed internally against the public's interest in transparency and open government institutions.[70] (Our public interest arguments are made in Section III, applying section 25 of *BC FIPPA*). As a result, even where disclosure will lead to some degree of heightened risk to an investigative technique, the public interest in disclosure can render this risk insufficient to justify a refusal to disclose.

27. VPD has so far failed to meet this onus. Moreover, it is unlikely to be able to do so with respect

---

should the information in question be released."

[68] *R v Mentuck*, [2001] 3 SCR 442, 2001 SCC 76, para 43; *Re: Ontario (Ministry of Community Safety and Correctional Services)*, Order No PO-3421, [2014] OIPC No 262, paras 89-90; *Re: Ministry of Justice*, Order F15-12, 2015 BCIPC 12, para 67. The principle is clearly stated in: *Ministry of Community and Social Services*, Order PO-2034, [2002] OIPC No 119 (ON IPC), para 67, affirmed, to that extent, in *Ontario (Ministry of Community and Social Services) v Ontario (Information and Privacy Commissioner)*, [2004] 70 OR (3d) 680 (Ont Div Ct), para 12: "In order to constitute an 'investigative technique or procedure,' it must be the case that disclosure of the technique or procedure to the public would hinder or compromise its effective utilization. The fact that a particular technique or procedure is generally known to the public would normally lead to the conclusion that its effectiveness would not be hindered or compromised by disclosure and accordingly that the technique or procedure in question is not within the scope of [the investigative techniques exception]."

[69] *Re: Ministry of Justice*, Order F15-22, 2015 BCIPC 24, paras 26 *et seq*.

[70] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31, para 66: "In sum, the Commissioner's decision reasonably applied the appropriate evidentiary standard. However, she had to balance this concern with the public's interest in having transparent and open governmental institutions. In striking a balance between the two competing interests, the Commissioner decided that the risks suggested by the Ministry were too remote and not supported by the evidence to ground a reasonable expectation of probably harm."; *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23, paras 47-48: "In making the decision, the first step…is to determine whether disclosure could reasonably be expected to interfere with a law enforcement matter. If the determination is that it may, the second step is to decide whether, having regard to the significance of that risk and other relevant interest, disclosure should be made or refused."

to responsive records. To begin, significant public information is available regarding the capacities and law enforcement uses of IMSI Catchers. This mitigates any risk flowing from the incremental gain in information that might result from disclosure of responsive records. Even confirmation of IMSI Catcher use by specific police departments is likely to emerge in time, as evidence obtained by these techniques is inevitably included in the record of criminal proceedings. Moreover, this risk is low to begin with – such information will not notably help individuals frustrate or detect IMSI Catcher deployment. Finally, the public interest in disclosing any responsive records is high. IMSI Catchers are an invasive surveillance tool. Drawing on Canadian law and experiences of other jurisdictions it can be reasonably anticipated that their use may require regulation to mitigate this invasive capacity. However, without confirmation that the tools are being used by law enforcement in Canada, no such discussion – in the courts or otherwise – of the need for such mitigation can occur.

28. What is sought in this instance is confirmation that VPD is employing generally known techniques. That confirmation is integral to advancing public policy debates and to the transparent operation of policing services. Such confirmation would do little to compromise the utility of the investigative techniques in question.

Significant Information Already on the Public Record Mitigates Risk of Harm

29. Significant general information related to the technical capacities and public sector usage scenarios of IMSI Catchers is part of the public record. In addition, the fact of a given police agency's use of IMSI Catchers should ultimately become part of the public record if the resulting evidence contributes to criminal charges. The investigative techniques exception is unavailable where the investigative technique sought to be protected is already part of the

public record.[71] Any risk that individuals might compromise an investigative technique is already realized when such knowledge already exists; the disclosure of responsive records can do little to heighten that risk.

30. Broad public availability of general information relating to electronic surveillance capacities and equipment is not uncommon. For example, in the United States, the capacities and technical specifications of network interception devices are not only a matter of public record,[72] but of regulatory hearings.[73] These interception devices remain useful nonetheless.

31. There is a rich public record detailing the capacities of IMSI Catchers as well as general details concerning their deployment by government agencies comparable to VPD. As recently noted by a United States District Court:

> The ACLU has put forward substantial evidence--including evidence the DOJ itself had made public—that the techniques and procedures relating to the use of cell site simulators is generally known to the public. CSS and its use by the federal government has also been the subject of extensive news coverage. The public domain evidently contains enough information about the technology behind CSS that members of the public have actually created their own CSS devices. This evidence demonstrates that the public in general knows that the government possesses and utilizes such cell phone technology in its investigations to locate and obtain information about the cell-phone holder.[74]

[71] *R v Mentuck*, [2001] 3 SCR 442, 2001 SCC 76, para 43, "...with respect to general knowledge of techniques used by police to infiltrate criminal organizations: There are a limited number of ways in which undercover operations can be run. Criminals who are able to extrapolate from a newspaper story about one suspect that their own criminal involvement might well be a police operation are likely able to suspect police involvement based on their common sense perceptions or on similar situations depicted in popular films and books. While I accept that operations will be compromised if suspects learn that they are targets, I do not believe that media publication will seriously increase the rate of compromise. The media have reported the details of similar operations several times in the past, including this one. In spite of this publicity, Sgt. German, in his affidavit, was only able to positively identify one instance in which media reports arguably resulted in the compromise of an operation."

[72] Cisco, "Chapter 2 – Lawful Intercept and CALEA," Cisco, last revised March 24, 2011, http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/bts/5-0/feature/description/featdesc/fd5015li.html.

[73] Federal Communications Commission, "In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services: Second Report and Order and Memorandum Opinion and Order," Federal Communications Commission, Adopted May 3, 2006, https://apps.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf.

[74] *ACLU of Northern California v Department of Justice*, Docket No 13-cv-03127-MEJ, 2015 US Dist LEXIS 79340 (LexisNexis)(N Dist of California), pp *36 – 37 (references omitted).

These capabilities have been described in academic articles,[75] analyzed in technical papers,[76] news articles,[77] television show plot scenarios,[78] court cases,[79] documents obtained by freedom of information requests in other jurisdictions,[80] and even governmental policies.[81] The detailed capabilities, limitations and operational parameters of these devices are by no means secret, and are substantively described above. More public information about these capabilities will likely emerge in the future because transparency regarding these tools is a legal reality in neighbouring jurisdictions where government agencies use comparable equipment to achieve comparable objectives.[82]

32. The utility of these devices in a law enforcement capacity is equally a matter of public record. While it is not possible to definitively confirm from the public record that VPD is using IMSI Catchers, it *is* possible to infer how such devices might be used by VPD and to what effect (see para 15 above). Any individual seeking to avoid detection or surveillance will be able to surmise from the public record what steps might be taken to detect or defeat such surveillance.[83]

33. Moreover, as eponymously implied, IMSI Catchers effectively replicate the functions of cell towers operated by Wireless Service Providers (WSPs). The *Criminal Code* contains legal powers

[75] These include: Pell & Soghoian, *supra 43;* Stephanie Pell & Christopher Soghoian, "A Lot More Than a Pen Register and Less Than a Wiretap: What the StingRay Teaches About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities," (2014) *16 Yale J L & Tech* 134.
[76] Dabrowski, *supra* 6; Luca Bongiorni, "iParanoid: A Mobile Cell Networks Intrusion Detection System," *Bootcamp 2012 – University of Luxembourg*, September 20, 2012, http://www.slideshare.net/iazza/mobile-cell-networksintrusiondetectionsystemiparanoidlucabongiorni..
[77] Sean Gallagher, "This machine catches stingrays: Pwnie Express demos cellular threat detector," *Ars Technica*, April 20, 2015, http://arstechnica.com/information-technology/2015/04/this-machine-catches-stingrays-pwnie-express-demos-cellular-threat-detector/.
[78] For example, these are discussed in HBO's The Wire, as documented in Pell & Soghoian, *supra* 43
[79] For example, see: *Re Application, Illinois*, *supra* 4.
[80] For example, see *ACLU NC v DOJ*, 2014, *supra* 49.
[81] DOJ Policy, *supra* 52; DHS Policy, *supra* 52.
[82] *ACLU NC v DOJ,* 2014, *supra* 49.
[83] Pell & Soghoian, *supra* 43; Soltani, *supra* 14; *ACLU NC v DOJ* 2014, *supra* 49, p *1038: "the DOJ's declaration asserts that information about the specifics of when various investigatory techniques are used could alert law violators to the circumstances under which they are not used without addressing the fact that the public is already aware that minimizing vehicular or cell phone usage will allow them to evade detection. To the extent that potential law violators can evade detection by the government's location tracking technologies, that risk already exists."

that expressly let law enforcement agencies access the type of information that could be obtained by using IMSI Catchers.[84] It is a matter of public record that law enforcement agencies will obtain comparable information from service providers. Access to this type of historical cell-site data is colloquially referred to as a 'tower dump' and has been the object of court cases and news stories.[85] Real-time interception of mobile device traffic and tracking of movements of mobile devices through the installation of interception devices is also explicitly covered by the *Criminal Code*. An IMSI Catcher is one mechanism (albeit one that is highly intrusive) that enables such interception. IMSI Catchers operating in identification mode in particular obtain identifiers that *must* be transmitted to cell towers to facilitate mobile interactions. IMSI Catcher obfuscation thus entails comparable obfuscation to what would be required if an individual wished to avoid WSP-based interception further to these *Criminal Code* powers.[86]

34. IMSI Catcher obfuscation options are severely limited. While some encryption techniques might protect the content of communications from being decrypted by IMSI Catchers operating in 'camping mode' (discussed above) it will be functionally challenging, at best, to obfuscate a handset from an IMSI Catcher in 'identification mode' given that IMSI and IMEI numbers are transmitted without encryption. Both are a necessary precursor to any mobile communication.[87] One would need to power down one's phone to ensure a zero footprint,[88] but this would also be necessary to avoid normal network-operated cell towers and attendant production powers. It is also notable that a range of IMSI Catcher detection techniques are *already* widely and publicly

[84] Going Opaque, *supra* 21, from Section Three C i-ii.
[85] *R v Mahmood*, 2011 ONCA 693; *R v Rogers Communications*, 2016 ONSC 70; Christine Dobby, "Ontario Court Rules Police Orders Breached Cellphone Users' Charter Rights", *The Globe and Mail*, January 14, 2016, http://www.theglobeandmail.com/report-on-business/industry-news/the-law-page/court-sides-with-telecoms-in-landmark-cellphone-privacy-case/article28180968/.
[86] *Going Opaque*, *supra* 21, pp 20-21.
[87] Dan Goodin, "Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations," *Ars Technica*, October 28, 2015, http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/; Dabrowski, *supra* 6.
[88] See: *Florida v Thomas*, Transcript, *supra* 33, p 20: "[Daren Shippy, Counsel for the defendant |] Q: And as long as the cellphone is turned on and as long as there is power where the battery has power, I guess then you're able to track the cellphone? [Investigator Christopher Corbitt |] A: Generally speaking, yes. As long as the handset is on, then you know we have the ability to attempt to track it."

available and have been subjects of academic and news articles.[89] While these techniques have limits, further knowledge of VPD use would not impact on their effectiveness or availability. In summary, VPD responsive records relating to the public body's general use of IMSI Catchers can do little more to compromise the effectiveness of these tools.

VPD IMSI Catcher Use Likely to be Disclosed Through Eventual Discovery Process

35. The fact of VPD IMSI Catcher use will likely emerge on the public record in time. The investigative technique exemption is only available where disclosure can be reasonably expected to compromise the effectiveness of the technique in question. The effectiveness of IMSI Catchers is, however, closely tied to the device's ability to assist VPD investigate crimes. Consequently, evidence VPD gathers using IMSI Catchers will be used to bring criminal charges and subject to discovery obligations. In the criminal discovery context, law enforcement agencies may shield some investigative techniques from disclosure,[90] though law enforcement secrecy is balanced against the defendant's right to make full answer and defence and, subsequently, against the open court principle.[91] It is insufficient to demonstrate that the effectiveness of a particular

[89] These include: Pell & Soghoian, *supra* 43; Dabrowski, *supra* 6; Bongiorni, *supra* 76 See also: Gallagher, *supra* 77.

[90] *Canada Evidence Act*,. RSC 1985, c C-5, s 37 *et seq*.; *Carey v Ontario*, [1986] 2 SCR 637 (public policy privileges are far more qualified than was the case historically); *R v Toronto Star Newspaper Ltd*, [2005] 204 CCC (3d) 397 (ONSC), paras 14-16 (public policy privilege over investigative techniques "is a basis for secrecy that is…fairly narrow in its application"); *R v Meuckon*, [1990] 57 CCC (3d) 193 (BCCA) (police techniques for faking cocaine ingestion might be protected as it would endanger future undercover police officers, but only if non-disclosure does not unduly undermine ability to make full answer and defence); *R v Richards*, [1997] 34 OR (3d) 244 (CA), paras 2, 13, 17 (public policy privilege engaged, but not definitively, where it might reveal a surveillance post or commonly used undercover surveillance vehicle); *R v Lam*, 2000 BCCA 545 (some protection for locations of surveillance positions). Note the Supreme Court of Canada has never recognized a qualified privilege for investigative techniques, although a framework for making such information more broadly public has been addressed: *R v Kim*, 2003 ABQB 1025, paras 48-51 (Supreme Court of Canada decision in *R v Mentuck* offers publication ban as potential prophylactic to mitigate harm of disclosing investigative techniques to opposing counsel).

[91] *R v Meuckon*, [1990] 57 CCC (3d) 193 (BCCA) (…if the decision to uphold the claim of [investigative technique] privilege … would have the effect of preventing the accused from making full answer and defence … the trial judge may permit the introduction of the evidence though the trial judge may impose whatever safeguards are appropriate."); *R v Richards*, [1997] 34 OR (3d) 244 (CA), para 17 (location of observation post and type of car used engages right to make full answer and defence as it could assist in testing observational evidence of officer"); *R v Blair*, [2000] OJ No 3019 (CA) (investigative technique privilege upheld because "this was not a case where the accused had no information, or even very little information, about the police observation post…"); *R v Lam*, 2000 BCCA 545, paras 39, 42-45 (refusal to provide details regarding location of observation post, details of observation, supports judge's refusal to accept evidence obtained from said observation post as credible).

technique might be marginally undermined by its disclosure.[92]

36. With respect to surveillance equipment, courts have mandated disclosure of some details, while permitting law enforcement to withhold information that has only limited potential to assist in a defence.[93] Even in such instances, enough details regarding the nature of the surveillance device in question must be disclosed so that its use can be effectively challenged. The invasive nature of IMSI Catchers raises legal ambiguities about their authorization framework and related *Charter* implications.[94] As such, evidence obtained by the unconditioned use of these devices can arguably be challenged, making disclosure of IMSI Catcher use central to a defendant's ability to make full answer and defence.[95] While VPD can withdraw IMSI Catcher-derived evidence from any criminal trial where disclosure is anticipated,[96] doing so would greatly reduce the utility of these surveillance devices, especially as potential *Charter* issues will accompany most IMSI Catcher deployments. It is therefore likely that confirmation of VPD IMSI Catcher use will, in time, become part of the public record, decreasing any potential harm that can be attributed to the release of responsive records in this instance.

---

[92] *Toronto Star Newspaper Ltd v Ontario*, [2003] 67 OR (3d) 577 (CA), paras 26-27 ("Fundamental freedoms, like the freedom of expression and freedom of the press, cannot, however, be sacrificed to give the police a "leg up" on an investigation."), aff'd in [2005] 2 SCR 188, 2005 SCC 41, para 36-43; *R v Toronto Star Newspaper Ltd*, [2005] 204 CCC (3d) 397 (ONSC), para 10; *R v Mentuck*, [2001] 3 SCR 442, 2001 SCC 76, paras 42-45.

[93] *R v Gerrard*, [2003] OJ No 420 (ONSC), paras 39-40 ("the witness did have to testify to at least the general nature of the tracking device installed. … the evidence must disclose that the tracking device used was a GPS … the Crown has a right to refuse to disclose any further details … I am satisfied that requiring the Crown to disclose the exact details of what specific type of GPS was used, how it was installed, and where it was installed in the vehicle in no way will effect the ability of the accused to make full answer and defence")(emphasis added); *R v Guilbride*, 2003 BCPC 176, paras 1-3 and 40-42 ("A considerable amount of information about the location of the sat-trac was disclosed … the information…is, at best, of some very limited, peripheral and possible relevance to issues the Defence seek to pursue in this trial.").

[94] These legal ambiguities are canvassed in *Going Opaque*, *supra* 21, Section Three (C) (ii) – (iii).

[95] Contrast *R v Kim*, 2003 ABQB 2015, paras 45-47 (evidence relied upon to gain search warrant under heightened obligation to disclose in spite of qualified investigative techniques privilege) with *R v Anderson*, 2011 SKQB 427, para 36 (…it would be of little or no use to the defence."), aff'd in 2013 SKCA 92, paras 133-137 and *R v Guilbride*, 2003 BCPC 176, paras 1-3 and 40-42 (data relating to surveillance device need not be disclosed in part because it is at best peripheral to a *Charter* challenge of that device). Indeed, the Québec Superior Court of Justice appears to have recently made precisely such an order regarding RCMP use of such devices: Freeze, Braga & Perreaux, *supra* 58. Information relating to what appears to have been an IMSI Catcher (referred to as an "Identification Dispositif Mobile") was ordered to be disclosed. See: *Mirarchi v R*, 2012 QCCS 7087, paras 63-64, for description of dispute. Decision regarding disclosure of IMSI Catchers is on appeal: *R v Mirarchi*, File No: 500-10-006048-159 (Québec Court of Appeal).

[96] *R v Lam*, 2000 BCCA 545, paras 39, 42-45.

Conclusion

37. In summary, significant information on the general capacities and investigative uses of IMSI Catchers is already publicly available. Responsive records could add minimal details that are not derivable from public information supplemented by common sense, and even this would not enhance the ability to detect or evade IMSI Catcher use. Finally, IMSI Catchers are used by a number of United States-based agencies of comparable mandate to VPD who are not protected by secrecy and will be an ongoing source of related information. It is also clear that these devices' utility has *not* been compromised by such public disclosure. These agencies still use IMSI Catchers, and adoption of such policies would not be justified without anticipated ongoing.[97]

III. Public Interest in Disclosure Outweighs Any Residual Harm

38. In assessing whether the risk to investigative techniques is sufficient to justify refusal of the right to information, this risk must be balanced against the public's interest in transparency and open government institutions.[98] This means that even where revealing details of a surveillance tool might risk undermining its efficiency, the risk may not warrant invoking the investigative technique exception in the face of a cogent countervailing public interest. Moreover, freedom of expression, as protected by section 2(b) of the *Charter*, encompasses a derivative right to receive information without which "meaningful public discussion and criticism on matters of public interest would be substantially impeded" or where the information is related to the exercise of an individual's *Charter* rights.[99] Where section 2(b) is engaged in this manner, a government

[97] DOJ Policy, *supra* 52; DHS Policy, *supra* 52.
[98] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31, para 66; *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23, para 48.
[99] *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23, para 37; *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, [2013] 3 SCR 733, 2013 SCC 62, paras 28, 30 and 37: "*PIPA* prohibits the collection, use, or disclosure of personal information for many legitimate, expressive purposes related to labour relations. These purposes include ensuring the safety of union members, attempting to persuade the public not to do business with an employer and bringing debate on the labour conditions with an employer into the public realm. These objectives are at the core of protected expressive activity under s. 2(*b*). … Expressive activity in the labour context is directly related to the *Charter* protected right of workers to

institution must exercise its discretion accordingly. The public interest may thus justify disclosing requested information even where there is evidence to demonstrate it *is* sufficiently probable that disclosure will hinder the effective utilization of an investigative tool.[100]

39. With respect to IMSI Catchers, their invasive nature and penchant for high collateral impact on the privacy of non-targets requires a policy debate. Other jurisdictions, including Germany and the United States, have adopted specific policies to curtail the excesses of these devices. In Canada, however, the debate regarding the invasiveness of these tools cannot meaningfully advance if agencies do not take the basic step of acknowledging IMSI Catcher use.

40. In addition, disclosure of IMSI Catcher use will enhance trial fairness. There is no guarantee that discovery rules requiring disclosure of IMSI Catcher use will be respected. Indeed, experience abroad suggests that government agencies will not proactively disclose IMSI Catcher use, and defence counsel may not know to ask.[101] Even hypothetical knowledge of general police IMSI Catcher use may be insufficient to raise the prospect of discovery shortcomings.[102] It is all the more important that credible information regarding the devices' use in Canada enter the public domain as a safeguard for the discovery process.

41. However specific knowledge that an agency such as VPD is actively using the devices might provide the legal basis for such a challenge. Moreover, where investigative techniques pose a

---

associate to further common workplace goals under s. 2(*d*) of the *Charter*."; *Ruby v Canada (Solicitor General)*, 2002 SCC 75, paras 52-53; *Ruby v Canada (Solicitor General)*, [2000] 3 FC 589 (CA), paras 145-146.

[100] *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23, paras 47-48.

[101] Pell & Soghoian, *supra* 43, pp 35-37; Kolker, *supra* 2: "Soghoian's colleagues educated dozens of public defenders in Maryland about the police's favorite toy; in one case last summer, a detective testified that the Baltimore police have used a Hailstorm some 4,300 times. "That's why there are so many StingRay cases in Baltimore," Soghoian tells me. "Because the defense lawyers were all told about it."

[102] *R v Khan*, [2004] OJ No 3811 (SC), para 36 (defence must present more than speculation to support production order); *R v Guilbride*, 2003 BCPC 176, para 2 ("This claim for further disclosure is based on speculation by accused persons in this trial, and their Defence counsel, that the sat-trac must have been placed in the emergency inflatable life raft container or "pod" on the deck of the "Blue Dawn". This suggestion arises out of the testimony provided by Cpl. Saccomani of the RCMP on "the Greek voir dire" as to the approximate size of the sat-trac package and the fact it was installed on the vessel without incursion or intrusion into certain areas." See also: *Maryland v Redmond*, Transcript, *supra* 32; *Maryland v Taylor*, Transcript, *supra* 10.

heightened threat of excessive intrusiveness it is all the more important that such information be made public so as to facilitate debate, as noted in *R v Mentuck*:

> The improper use of bans regarding police conduct, so as to insulate that conduct from public scrutiny, seriously deprives the Canadian public of its ability to know of and be able to respond to police practices that, left unchecked, could erode the fabric of Canadian society and democracy.[103]

There are ambiguities relating to the legal authorization framework for use of such devices,[104] creating the potential for misuse. Refusing IMSI Catcher-related information requests delays important public debates regarding these ambiguities as well as those regarding the conditions under which IMSI Catchers should be deployed under current law. These debates cannot advance in more than a hypothetical manner without confirmation that the tools are being used by law enforcement in Canada.

42. Finally, the experience from abroad and particularly from the United States demonstrates that there are good reasons to restrain the use of IMSI Catchers proactively, and Canadian experience to date affirms this. For example, Corrections Services Canada appears to have installed IMSI Catchers in a prison without any safeguards and potentially in violation of criminal laws.[105] Federal agencies appear to be using these devices in violation of federal spectrum regulations.[106] It is likely that if judges new of the invasive potential of these devices, they would place adopt safeguards.[107] Finally, while privacy impact assessments are often required for new privacy-invasive programs,[108] and while IMSI Catcher use likely to has implications under federal and

[103] *R v Mentuck*, [2001] 3 SCR 442, 2001 SCC 76, para 51.
[104] Canvassed in *Going Opaque? supra 21*, Section Three C i-iii.
[105] Freeze & Braga, *supra* 35.
[106] Braga & Freeze, *supra 59*.
[107] *Re Application*, *Illinois*, *supra* 4; *R v Rogers Communications*, 2016 ONSC 70.
[108] Treasury Board of Canada, Directive on Privacy Impact Assessment, effective April 1, 2010, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308.The obligation is binding as it is a directive issued under paragraph 71(1)(d) of the *Privacy Act*, RSC 1985, c P-21.The obligation is implicated where a new or modified program "[c]ollects personal information which will not be used in decision-making process that directly affect and individual but which will have an impact on privacy." (https://www.priv.gc.ca/resource/fs-

provincial data protection laws,[109] it appears that no such privacy impact assessments have been undertaken.[110] Placing information relating to these invasive tools on the public record in Canada is therefore a necessary precursor to ensuring transparency in IMSI Catcher use, where there is tangible concern such use may not be consistent with the law.[111] Moreover, confirmation of IMSI Catcher use is integral to meaningful debate on a matter of public interest in Canada while being equally essential to the proper exercise of Canadian privacy rights.[112]

IV. Conclusion

43. In summary, IMSI Catchers are a surveillance tool with high invasive capacity. Much general information regarding their capacities, limitations and usage is publicly available already – more information from responsive records can pose minimal (if any) harm to the utility of these devices. However the refusal of Canadian agencies to confirm use of these devices has been a key impediment to any meaningful discussion – in the courts, in Canadian legislatures and in the public – of how to ensure these devices are used in a manner that is proportionate and properly restrained by law. The public interest in disclosure of responsive records therefore far outweighs any potential risk to the future utility of these tools that may result.

***** END OF DOCUMENT *****

---

fi/02_05_d_33_e.asp). As noted above, IMSI Catchers are specifically designed to operate in a manner that intercepts extensive information on non-targets, information that is not necessary for any decision-making process, as it is only captured collaterally. See also: Office of the Information & Privacy Commissioner, "Early Notice and Privacy Impact Assessments to the OIPC under the *Freedom of Information and Protection of Privacy Act*, updated July 2012, (BC IPC), https://www.oipc.bc.ca/guidance-documents/1434.

[109] *Going Opaque?*, *supra* 21, pp 65-67; BC IPC, ALPR, *supra* 29.

[110] Matthew Braga, "The covert cellphone tracking tech the RCMP and CSIS wont' talk about," *The Globe and Mail*, September 15, 2014, http://www.theglobeandmail.com/technology/digital-culture/the-covert-cellphone-tracking-tech-the-rcmp-and-csis-wont-talk-about/article20579947/: "According to Tobi Cohen, a spokesperson for the Office of the Privacy Commissioner of Canada, 'We have not been made aware by the RCMP of their use of this technology. If they were looking to use this type of technology, we would expect to be consulted.'"; Jordan Pearson, "A Canadian Prison Was Spying on Non-Inmates and Recording Their Calls and Texts", Motherboard, September 24, 2015, http://motherboard.vice.com/read/a-canadian-prison-was-spying-on-people-and-recording-their-calls-and-texts.

[111] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31, para 66; *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23, paras 47-48.

[112] *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23, para 37; *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, [2013] 3 SCR 733, 2013 SCC 62, paras 28, 30 and 37; *Ruby v Canada (Solicitor General)*, 2002 SCC 75, paras 52-53; *Ruby v Canada (Solicitor General)*, [2000] 3 FC 589 (CA), paras 145-146.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 23rd day of March, 2016

Tamir Israel

Samuelson Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

Tel: (613) 562-5800 x 2914
Fax: (613) 562-5417
Email: tisrael@cippic.ca

Counsel for the Intervener, Open Media

Canadian Authorities	
1.	*Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, [2013] 3 SCR 733, 2013 SCC 62
2.	*British Columbia (Minister of Citizens' Services) v British Columbia (Information and Privacy Commissioner)*, 2012 BCSC 875
3.	*Canada Evidence Act*, RSC 1985, c C-5
4.	*Carey v Ontario*, [1986] 2 SCR 637
5.	*Ministry of Community and Social Services*, Order PO-2034, [2002] OIPC No 119 (ON IPC)
6.	*Mirarchi v R*, 2012 QCCS 7087
7.	*Ontario (Ministry of Community and Social Services) v Ontario (Information and Privacy Commissioner)*, [2004] 70 OR (3d) 680 (Ont Div Ct)
8.	*Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31
9.	*Ontario (Community and Social Services) v Doe*, 2015 ONCA 727
10.	*Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23
11.	*Re British Columbia (Ministry of Aboriginal Affairs and Reconciliation)*, Order F16-05, [2016] BCIPC 4, (BC IPC)
12.	*Re British Columbia (Ministry of Citizens' Services)*, Order F10-39, [2010] BCIPCD No 59
13.	*Re: Ministry of Justice*, Order F15-22, 2015 BCIPC 24
14.	*Re: Use of Automated License Plate Recognition Technology by the Victoria Police Department*, Investigative Report F12-04, November 15, 2012 (BC IPC)
15.	*Re: Vancouver Police Department*, Investigator's Fact Report, OIPC File No: F15-63155 (BC IPC)
16.	*Re: Vancouver Police Department*, Notice of Written Inquiry, OIPC File No: F15-63155, January 25, 2016, (BC IPC)
17.	*Ruby v Canada (Solicitor General)*, [2000] 3 FC 589 (CA)
18.	*Ruby v Canada (Solicitor General)*, 2002 SCC 75
19.	*R v Blair*, [2000] OJ No 3019 (CA)
20.	*R v Gerrard*, [2003] OJ No 420 (ONSC)
21.	*R v Guilbride*, 2003 BCPC 176
22.	*R v Khan*, [2004] OJ No 3811 (SC)

Secondary Sources	
45.	Article 29 Data Protection Working Party. (2011). "Opinion 13/2011 on Geolocation services on smart mobile devices," European Commission, Adopted on May 16, 2011
46.	Cisco, "Chapter 2 – Lawful Intercept and CALEA," Cisco, last revised March 24, 2011
47.	Citizen Lab, "The Many Identifiers in Our Pockets: A primer on mobile privacy and security," *Citizen Lab*, May 13, 2015
48.	Devlin Barrett, "Americans' Cellphones Targeted in Secret U.S. Spy Program," *The Wall Street Journal*, November 13, 2014
49.	Matthew Braga, "The covert cellphone tracking tech the RCMP and CSIS wont' talk about," *The Globe and Mail*, September 15, 2014
50.	Mathew Braga and Colin Freeze, "Agencies did not get federal authorization to use surveillance devices," *The Globe and Mail,* March 21, 2016
51.	Luca Bongiorni, "iParanoid: A Mobile Cell Networks Intrusion Detection System," *Bootcamp 2012 – University of Luxembourg*, September 20, 2012
52.	Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. (2014). "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," Conference Proceedings of the Annual Computer Security Applications Conference (ACSAC 2014)
53.	Department of Homeland Security, "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," October 19, 2015
54.	Department of Justice, "Use of Cell-Site Simulator Technology", Department of Justice Policy Guidance, September 3, 2015
55.	Christine Dobby, "Ontario Court Rules Police Orders Breached Cellphone Users' Charter Rights", *The Globe and Mail*, January 14, 2016
56.	Fruzsina Eordogh, "Evidence of 'Stingray' Phone Surveillance by Police Mounts in Chicago", *Christian Science Monitor*, December 22, 2014
57.	Cyrus Farivar, "California cops, want to use a stringray? Get a warrant, governor says," *Ars Technica*, October 8, 2015
58.	Cyrus Farivar, "FBI would rather prosecutors drop cases than disclose stingray details," *Ars Technica*, April 7, 2015
59.	Cyrus Farivar, "Prosecutors Drop Key Evidence at Trial to Avoid Explaining 'stingray' use", *Ars Technica*, November 18, 2014
60.	Hanni Fakhoury, "Stingrays Go Mainstream: 2014 in Review," *Electronic Frontier Foundation*, January 2, 2015
61.	Colin Freeze & Matt Braga, "Surveillance Device Used in Prison Sets Off Police Probe", *The Globe and Mail*, March 14, 2016

62.	Colin Freeze, Matt Braga & Les Perreaux, "RCMP Fight to Keep Lid on High-Tech Investigation Tool", *Globe and Mail*, 13 March, 2016
63.	Ryan Gallagher, "Criminals May be Using Covert Mobile Phone Surveillance Tech for Extortion", *Slate*, Aug 22, 2012
64.	Dan Goodin, "Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations," *Ars Technica*, October 28, 2015
65.	Brad Heath, "Police secretly track cellphones to solve routine crimes," *USA Today*, August 24, 2015
66.	Tamir Israel & Christopher Parsons, "Going Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada", *Citizen Lab & Canadian Internet Policy & Public Interes Clinic*, January 2016
67.	Maria Kayanan, "Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking," *American Civil Liberties Union*, June 19, 2014
68.	Robin Levinson King, "The cellphone spyware the police don't want to acknowledge," *Toronto Star*, December 15, 2015
69.	Kate Klonick, "Stingrays: Not Just for Feds!", *Slate*, November 10, 2014
70.	Robert Kolker, "What Happens When the Surveillance State Becomes an Affordable Gadget?", *Bloomberg*, March 10, 2016
71.	Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," A/HRC/23/40, April 17, 2013
72.	Yves-Alexandre de Montjoye, César A Hidalgo, Michel Verleysen, and Vincent D Blondel. (2013). "Unique in the Crowd: The Privacy Bounds of Human Mobility", *Scientific Reports* 3
73.	Ellen Nakashima, "FBI clarifies rules on secretive cellphone-tracking devices," *The Washington Post*, May 14, 2015
74.	Office of the Information & Privacy Commissioner, "Early Notice and Privacy Impact Assessments to the OIPC under the *Freedom of Information and Protection of Privacy Act*, updated July 2012, (BC IPC)
75.	Office of the Information and Privacy Commissioner of Ontario, "Surveillance Then and Now: Securing Privacy in Public Spaces", June 2013
76.	Jordan Pearson, "A Canadian Prison Was Spying on Non-Inmates and Recording Their Calls and Texts", Motherboard, September 24, 2015
77.	Stephanie Pell & Christopher Soghoian, "A Lot More Than a Pen Register and Less Than a Wiretap: What the StingRay Teaches About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities," (2014) *16 Yale J L & Tech* 134
78.	Stephanie K. Pell and Christopher Soghoian, "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy", (2014), 28(1) *Harvard J of Law & Tech* 1
79.	Privacy International and Digital Rights Ireland. (2015). "The Right to Privacy in Ireland," *Digital Rights*

	Ireland, September 2015
80.	Teresa Scassa and Anca Sattler, "Location-Based Services and Privacy", (2011) 9 *Canadian J of L & Tech* 99
81.	Treasury Board of Canada, Directive on Privacy Impact Assessment, effective April 1, 2010
82.	Adam Senft, Andrew hilts, Christopher Parsons, Jakub Dalek, Jason Q. Ng, John Scott-Railton, Katie Kleemola, Masashi Crete-Nishihata, Ron Deibert, and Sarah McKune, "A Chatty Squirrel: Privacy and Security Issues with UC Browser," *Citizen Lab*, May 21, 2015
83.	Andrea Slane and Lisa M Austin, "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations," (2011) 57 *Criminal L Quarterly* 486
84.	Ashkan Soltani and Craig Timberg, "Tech firm tries to pull back curtain on surveillance efforts in Washington," *The Washington Post*, September 17, 2014
85.	Christian Stork, "Alameda County becomes first in state to regulate cellphone surveillance tool," *Oakland North*, November 19, 2015
86.	Washington Post, "How the NSA is Tracking People Right Now," retrieved November 27, 2015
87.	Nicky Woolf, "2,000 cases may be overturned because police used secret Stingray surveillance," *The Guardian*, September 4, 2015