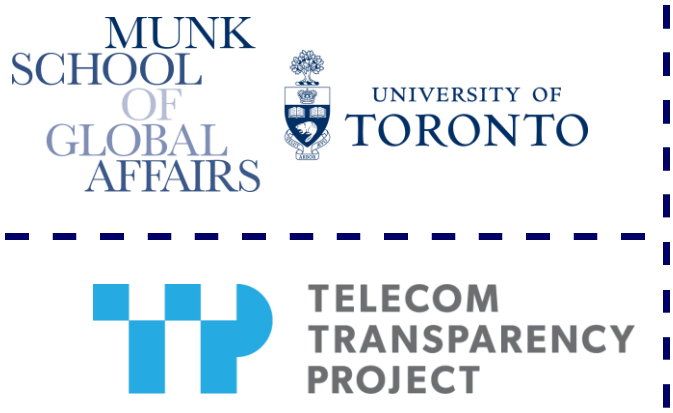

Gone Opaque?

An Analysis of Hypothetical IMSI Catcher Overuse in Canada

VER.2

August 2016

Report by Tamir Israel & Christopher Parsons

This page has intentionally been left blank.

Electronic version first published by the Telecom Transparency Project and the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic. The Telecom Transparency Project is associated with the Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto. The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is a legal clinic based at the Centre for Law, Technology & Society at the University of Ottawa, Faculty of Law.

Document Version 2.0

The authors would like to graciously thank a number of sources whose generous funding made this report possible: the Open Society Foundation, Frederick Ghahramani, a Social Sciences and Humanities Research Council (SSHRC) Postdoctoral Fellowship Award, and the Munk School of Global Affairs at the University of Toronto.

About Telecom Transparency Project and Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic

The **Telecom Transparency Project** investigates how telecommunications data is monitored, collected, and analyzed for commercial, state security, and intelligence purposes. The Project is associated with the Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto. The Citizen Lab focuses on advanced research and development at the intersection of information and communications technologies, human rights, and global security.

Core to the Telecom Transparency Project's work is interrogating the practices of telecommunications service providers (e.g. AT&T, Vodafone, and Bell Canada) that route data traffic between communicating parties and the mechanisms that third parties use to access the digital information that is endlessly flowing through telecommunications service providers' networks. Rendering telecommunications processes transparent will help citizens, politicians, and businesses understand how private or public, and how secure or vulnerable, their communications are to service provider-linked communications interferences and data disclosures.

The **Canadian Internet Policy & Public Interest Clinic (CIPPIC)** is a legal clinic based at the Centre for Law, Technology & Society (CLTS) at the University of Ottawa, Faculty of Law. Its core mandate is to ensure that the public interest is accounted for in decision-making on issues that arise at the intersection of law and technology. It has the additional mandate of providing legal assistance to under-represented organizations and individuals on law and technology issues, as well as a teaching mandate focused on providing law students practical training in a law and technology setting.

CIPPIC adopts a multi-lateral approach to advancing its mandate, which involves placing objective and comprehensive research and argumentation before key political, regulatory and legal decision makers. It seeks to ensure a holistic approach to its analysis, which integrates the socio-political, technical and legal dimensions of a particular policy problem. This regularly includes providing expert testimony before parliamentary committees, participating in quasi-judicial regulatory proceedings, strategic intervention at all levels of court and involvement in domestic and international Internet governance fora.

About This Report

The technical, legal and public policy analysis contained in this report were intended to contribute to an ongoing and evolving legal and political environment and, additionally, designed to seek input at formative stages of the analysis from other experts. The analysis herein has therefore significantly evolved over time as the authors received input from a number of sources.

An earlier version of this document, Discussion Draft, version 1, dated January 2016, was submitted on the record of a written inquiry into the refusal of a state agency to produce records responsive to requests for information relating to the use of IMSI Catchers, and was circulated widely for input.

Over the course of drafting this report, the 'on the ground' situation in Canada has dramatically evolved. At the outset, significant information on the use of IMSI Catchers had emerged in the United States, but very little was known about their operation in Canada. While much remains obscure, the past few months have seen a relative explosion of public information regarding the use of these devices by Canadian state agencies, largely due to sustained efforts of civil society organizations and journalists. This newly emerged information is largely reflected in this final version of the report, which has been updated to account for developments.

Along these lines, a series of 'Update Boxes' have been added to this document in order to incorporate the most recent series of developments and updates in a non-intrusive manner.

Finally, while the report remains squarely focused on IMSI Catchers, it is the hope of the authors that the historical and substantive narrative might elicit some inspire into transparency and control of surreptitious surveillance techniques more generally.

The authors are grateful for in-depth substantive input on the December 2015 draft of this document from Ronald Deibert and Sarah McKune, to Adrian Dabrowski and to participants of Citizen Lab Summer Institute 2016 for key input on technical questions raised by this paper and to Lex Gill for extensive substantive additions and edits. Responsibility for any errors or omissions remains with the authors.

Please send feedback to: **christopher@christopher-parsons.com** and **tisrael@cippic.ca**

About the Authors

This report was researched and written by Tamir Israel and Christopher Parsons.

Tamir Israel is Staff Lawyer at the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) at the University of Ottawa, Faculty of Law. He leads CIPPIC's privacy, net neutrality, electronic surveillance and telecommunications regulation activities and conducts research and advocacy on a range of other digital rights-related topics. He also lectures on Internet regulation at the University of Ottawa, Faculty of Graduate & Post-doctoral Studies.

Christopher Parsons received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D from the University of Victoria. He is currently a Research Associate at the Citizen Lab, in the Munk School of Global Affairs with the University of Toronto as well as the Managing Director of the Telecom Transparency Project at the Citizen Lab.

Acronyms

CBSA	Canada Border Services Agency
CDMA	Code Division Multiple Access
CSE	Communications Security Establishment of Canada
CSIS	Canadian Security Intelligence Service
DHS	Department of Homeland Security
DOJ	Department of Justice
EPS	Edmonton Police Service
ESN	Electronic Serial Number
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
GSM	Global System for Mobile Communications
GSOC	Garda Siochana Ombudsman Commission
IMEI	International Mobile station Equipment Identifier
IMSI	International Mobile Subscriber Identifier
MS	Mobile Station [mobile device, mobile phone]
MSID	Mobile Station ID
MSISDN	Mobile Station Integrated Services Digital Network-Number
mTAN	Mobile Two-Factor Authentication Scheme
NDA	Non-Disclosure Agreement
NSA	National Security Agency
RCMP	Royal Canadian Mounted Police
SIM	Subscriber Identification Module
SMS	Short Message Service
TPS	Toronto Police Services Board
VLR	Visitor Location Register
VPD	Vancouver Police Department

Table of Contents

Tables & Boxes

Executive Summary

This analytical report, *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada*, examines a class of surveillance devices called 'cell site simulators', and which are commonly referred to as 'IMSI Catchers', 'Digital Analyzers', 'cell grabbers', and 'mobile device identifiers' or by brand names such as 'Stingray', DRTBOX and 'Hailstorm'.

IMSI Catchers allow state agencies to intercept communications from mobile devices and are used primarily to identify otherwise anonymous individuals associated with a mobile device or to track them. These surveillance devices are not new – their use by state agencies spans decades. However, the ubiquity of the mobile communications devices in modern day life, coupled with the plummeting cost of IMSI Catchers, has led to a substantial increase in the frequency and scope of IMSI Catcher use. As the devices are highly intrusive in nature, their surreptitious and uncontrolled use poses an insidious threat to privacy.

Broadly, the report investigates the surveillance capabilities of IMSI Catchers, state efforts (and civil society counter-efforts) to prevent any information relating to IMSI Catchers from becoming public, and the legal and policy framework that governs the use of these devices in state surveillance contexts. While this report principally focuses on Canadian state agencies, it draws on comparative examples from other jurisdictions, notably the United States and to some degree Germany. The report concludes with a series of recommended transparency and control mechanisms (primarily legal) designed to properly constrain the use of these devices and to temper their more intrusive features. Structurally, the report is divided into four sections relating to technical capacities, transparency, policy controls and best practices.

In light of the evolving nature of the subject matter explored here, a series of recent developments have been incorporated into the report in the form of 'Update Boxes', with the intention of documenting these developments and contextualizing them against the analysis contained in the primary report.

Along these lines, **Section One** of the report provides an overview of capabilities of IMSI Catchers. As the devices are designed to emulate the functionality of cell phone towers, much regarding their capabilities and general operation can be determined based on the well-documented protocols and specifications that govern cellular communications. The report primarily focuses on the operation of these devices in 'identification mode', where the devices operate to intercept digital numbers such as the IMSI and IMEI numbers that identify mobile devices. IMSI Catchers exploit weaknesses in the design of mobile communications standards in order to trick mobile devices within range into

believing that the IMSI Catcher is a cell tower operated by an individual's mobile service provider. IMSI Catchers then induce these mobile devices to transmit unique digital identifiers that would typically only be transmitted to the mobile service provider. The section proceeds to explore how IMSI Catchers have and can be used, specifically by various state agencies. In an investigative context, IMSI Catchers are used primarily to identify or locate individuals, implicating anonymity and raising the potential of pervasive tracking. IMSI Catchers are operationally intrusive. Mobile devices tricked to interact with an IMSI Catcher are removed from the mobile communications network and, hence, are unable to send or receive calls, text messages or data. From a privacy perspective, the devices are inherently intrusive – by design, they capture mobile identifiers from all mobile phones in range, leading to significant collateral privacy impact that can affect the privacy of thousands of non-targets for each individual legitimate target.

Section Two examines efforts to identify and understand state use of IMSI Catchers in a number of jurisdictions. It begins by looking beyond Canada's borders by describing civil society efforts to uncover state IMSI Catcher use and the surprisingly robust obfuscation measures these efforts encountered. After highlighting some of the hard-fought successes in the United States, in particular, we examine comparable efforts to uncover IMSI Catcher use in Canada, and these efforts' comparative successes and failures. To exemplify some of the problems faced in attempts to uncover IMSI Catcher use by Canadian agencies, it analyzes a failed appeal of a refused freedom of information request as a case study. In this context, it critiques a number of the justifications that are frequently advanced by state agencies seeking to prevent any information relating to IMSI Catchers from becoming public. The case analysis concludes that providing some details of IMSI Catcher use will not undermine the investigative utility of these devices and that there is substantial public interest justifying authorities disclosing their use of these devices regardless. In part, disclosure is important so that the public can ensure that no laws are being violated by the use of IMSI Catchers – specifically in light of some suggestion that possession and use of these devices might be inconsistent with the *Radiocommunications Act*, the *Privacy Act* and perhaps the *Charter*. Importantly, refusing information IMSI Catcher-related requests delays public debates regarding the appropriate parameters for using these devices. Moreover, ongoing refusal to officially acknowledge IMSI Catcher use in the face of a growing public record documenting such use undermines public confidence that the devices are being used lawfully and in a manner that is proportionate and minimizes their impact on non-targeted members of the public.

Section Three examines the regulation of IMSI Catchers and avenues toward the lawful authorization of their use. We survey regulatory models in both Germany and

the United States to better understand potential gaps in the Canadian context. It then explores Canada's ambiguous statutory framework for electronic surveillance in order to better understand the legal avenues available to state agencies for authorization of IMSI Catcher use in practice. The report demonstrates how a range of overlapping powers might apply to IMSI Catcher authorization, and that this ambiguity might permit state agencies to deploy IMSI Catchers using powers that offer minimal privacy protection. This, in turn, could allow for IMSI Catchers to be used in a disproportionate manner. The section concludes by examining the *Charter* implications of IMSI Catcher use. It suggests that some stage agencies might believe they can use these devices without prior judicial authorization. However, such a belief is likely inconsistent with the *Charter*. The report reviews possible justifications for IMSI Catcher deployment in the absence of prior judicial authorization, rejecting each. IMSI Catchers effectively operate as identification and geo-location tools, and courts have held that electronic surveillance of digital identifiers and geo-location requires prior authorization. Section 8 of the *Charter* should therefore generally compel government agencies to obtain judicial authorization as precondition of IMSI Catcher use. This section of the report concludes by distilling safeguards and conditions on use that may be necessary to ensure IMSI Catcher use does not amount to a constitutionally impermissible search.

Section Four sets out a number of best practices that should be incorporated into a framework governing IMSI Catcher use. These best practices are distilled from the various controls placed on IMSI Catcher use by policy, legislation, and by courts in other jurisdictions, from mechanisms imposed on comparable types of invasive electronic surveillance in Canada, and on general best practices for electronic surveillance. The section **recommends** that IMSI Catcher use by state agencies be subject to comprehensive transparency mechanisms, including annual statistical reporting on use, an individual notice obligation so that affected individual can challenge violations of their privacy, and compliance with standard reporting obligations typically applied to radio devices owned by state agencies. It further argues that unauthorized IMSI Catcher use should be criminalized. In order to ensure IMSI Catcher use is only authorized in a proportionate manner, the report suggests that their use should be subject to a strict authorization regime as well as an investigative necessity obligation, and a "serious crimes" provision limiting their use to investigations of more severe offences. In addition to these proportionality measures, targeting and minimization measures should be imposed on IMSI Catcher use to limit the collateral impact of deployment on innocent third parties. This would include a prohibition, to the degree possible, on using IMSI Catchers at areas and times where it is known that many non-targeted individuals will be subject to this intrusive surveillance tool, an obligation to

expeditiously delete non-targeted data collaterally obtained by an IMSI Catcher, and limits on use such information exclusively to single out targeted information.

The report's **Conclusion** highlights some of the core findings and also emphasizes the importance of privacy in liberal democratic societies. Failing to properly render surveillance technologies transparent and unsuccessfully regulating their use can raise serious issues for basic freedoms of all persons. This is particularly so in light of the surreptitious nature of electronic surveillance tools. As such, the Government of Canada and its provincial counterparts ought to follow the example of other jurisdictions by developing, and publicizing, information on how IMSI Catchers can be used by state agencies and should draw on experiences abroad in strictly regulating any future use of these intrusive devices. Doing anything else threatens to place citizens under an unaccountable surveillance regime that may have serious chilling effects on Canadians' basic freedoms.

Introduction

While about 19% of Canadian mobile phone subscribers use 'feature' phones that largely lack app stores or mobile Internet access, the majority of Canadians (81%) now carry powerful mobile computing devices with them practically everywhere they go.[1] And while more and more Canadians prefer sending texts, emails, or other non-voice communications using their phone, all of their mobile devices - regardless of their sophistication - emit unique numbers that are used to route communications. The same numbers, however, can be captured in the course of surveillance operations conducted by state agencies or other parties using devices called 'cell-site simulators', and referred to variously as 'IMSI Catchers', 'Digital Analyzers', 'cell grabbers', and 'mobile device identifiers' or by brand names such as 'Stingray', DRTBOX and 'Hailstorm'. The ubiquity of mobile devices, in tandem with the low costs and consequent availability of IMSI Catchers, has meant that government agencies and other third-parties can track and intercept the mobile identifiers and communications of large volumes of people. Though IMSI Catcher-based surveillance has been used by some government agencies for over a decade, such surveillance is rarely rendered transparent through government reporting or explicit legislation that showcase the conditions under which IMSI catchers can be deployed.

Government agencies have frequently tried to obscure how they use these technologies. Civil liberties advocates, journalists, academics, and politicians have all tried to peel away some of this state imposed secrecy with varying degrees of success around the world, and to particularly little effect in Canada. Though there is no public evidence that IMSI Catchers are being used by Canadian agencies, their potential for invasiveness means it is nonetheless worthwhile to examine the framework under which such devices might be deployed as well as how their use might be uncovered.

This analytical report investigates the lawfulness of using IMSI Catchers in Canada and the failure of the federal and provincial governments to disclose agencies' policies or uses of IMSI Catchers. **Section One** provides an overview of how the devices work, how they can be configured to monitor communications traffic emitted from mobile devices, and how data collected using IMSI Catchers can be used to identify particular persons. **Section Two** focuses on efforts to understand how IMSI Catchers are used; we first outline international efforts and then turn to the corresponding activities in Canada. We focus, in particular, on the difficulties that Canadians who have used the freedom of

[1] ComScore. (2015). "Canada Digital Future in Focus," *ComScore*, May 27, 2015, retrieved December 1, 2015, https://www.comscore.com/Insights/Presentations-and-Whitepapers/2015/2015-Canada-Digital-Future-in-Focus.

information system to compel policy documents from government have experienced, and the dubiousness of existing rulings which authorize authorities to withhold documents. Section Three explores how IMSI Catcher use is regulated in other jurisdictions, notably Germany and the United States. It then examines how IMSI Catchers might be deployed in Canada, suggesting first that while some agencies might believe they are lawfully authorized to make use of IMSI Catchers without prior judicial authorization, such beliefs are likely inappropriate. It then proceeds to examine how changes to the *Criminal Code* powers relating to metadata and tracking information offers one potential legislative framework that state agencies might rely upon for authorizing IMSI Catchers. It argues that these powers establish ambiguity concerning what warranting regime is appropriate and, moreover, that the *Charter* likely requires a more privacy-protective mechanism than that offered by many of the potential powers offered by the *Criminal Code*. **Section Four** of the report offers a set of recommendations concerning the regulation of IMSI Catchers, and places emphasis on establishing a strict authorization regime that is linked with the Part VI regime, invoking data minimization policies, creating deletion requirements pertaining to non-targeted persons' data, and adopting statutory reporting requirements surrounding the use of IMSI Catchers by public agencies. The report's **Conclusion** highlights some of the core findings and also emphasizes the importance of privacy in liberal democratic societies.

Section One: IMSI Catcher 101

Cell-site simulators are devices that impersonate cell phone towers, convincing mobile devices to interact with them as they normally would only interact with a service provider's tower. While not a new technology – cell site simulators have been used by law enforcement for several decades – a dramatic reduction in their price coupled with the modern day ubiquity of mobile devices has made cell site simulators a commonly used investigative tool.[2] At their core, such devices exploit a feature of the Global System for Mobile Communications (GSM), that requires mobile devices to authenticate themselves to cell phone towers. This same feature does *not*, however, require cell phone towers to authenticate themselves to mobile devices even though the system as a whole requires mobile devices to *trust* cell towers.[3] This creates a situation where a properly configured simulator can impersonate a cell tower and devices will connect with it, trust instructions received from it, and send it information that is normally reserved for a service provider. IMSI Catchers are a subset of these tower impersonators that target the majority of today's mobile

[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] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, p 87-91.

devices. In this section we discuss how IMSI Catchers collect information that is emitted from mobile devices, that information's importance, and some actors which have deployed them.

IMSI Catchers can be used by third parties to carry out various tasks that service providers typically carry out by means of cell phone towers. Per A. Dabrowski et al., IMSI Catchers can:

> track handsets, deliver geo-target 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).[4]

A. Dabrowski et al. note there are two 'modes' in which IMSI Catchers can operate. On the one hand, they can operate in 'identification mode' where the device collects digital identifiers of each mobile device within range and then redirects those devices to connect to a legitimate cellular tower. On the other hand, they can operate in 'camping mode'. In this mode the mobile device is not redirected to a legitimate tower after its unique identifiers are obtained, but instead all traffic passes through the IMSI Catcher before it is forwarded on to a legitimate cellular base station. 'Camping mode' places whomever controls the IMSI Catcher in the middle of the communications flow, letting the controller capture and subsequently access the content of a person's communications. Camping mode therefore entails intercepting a person's communications in their entirety.

A. IMSI Catchers: General Functionality & Operation

Operation in camping mode raises challenges. Many elements of a modern communications flow are encrypted, some of which is applied by the mobile network itself, for the specific purpose of protecting interactions between the mobile device and the network from third parties. Sometimes, additional encryption will be applied by third parties – the website, email service or chat client may each apply their own layer of encryption in addition to that applied by the mobile network itself.[5]

Some IMSI Catchers are able to bypass encryption applied by the mobile network itself. However, to do this in real-time, an IMSI Catcher may need to carry out a downgrade attack. A downgrade attack entails the IMSI Catcher sending a signal to a

---

[4] 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), retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

[5] Ross Anderson (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems (Second Edition)* (Indianapolis: Wiley Publishing Inc, 2008), pp. 608-619.

mobile device that convinces that device to switch from an advanced communications protocol such as 3/4G to an older one such as 2G, which employs weaker encryption.[6] Specifically, older communications protocols employed ciphers (A5/1 and A5/2) that were purposefully weakened to facilitate lawful interception and because of historic export controls on cryptography and for which there are now publicly known techniques that can break the encryption in real time. In contrast, more recently developed communications protocols use A5/3 or A5/4, neither of which are publicly known to have been broken.[7] Mobile devices that are sold today still support the 2G protocol so that the devices can inter-operate with older towers that only support the older protocol sets, and are designed to accept requests from cell towers (and, by extension, IMSI Catchers) to switch to these older protocols. In addition, some older mobile communications protocols let cell towers disable encryption altogether; a functionality that is replicated by some IMSI Catchers.[8]

If higher layer encryption mechanisms, such as HTTPS/TLS (used to encrypt transmissions between applications on devices and website or email servers) or OTR (used to encrypt instant messaging between two individuals communicating using the XMP Protocol) are being used by third party services these will, of course, remain unaffected by such decryption attempts. Consequently, underlying content that has been encrypted independently of the encryption applied by the mobile network itself will remain generally inaccessible to an IMSI Catcher in camping mode (just as it remains inaccessible to cell towers in general) barring additional decryption capabilities.

IMSI Catchers operating in 'camping mode' (i.e. operating to capture the content of voice, text or data communications) offer some, but minimal, utility to law enforcement over other mobile interception capabilities which rely directly on network providers to carry out comparable interception. Their capacity for greater

---

[6] Ross Anderson. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems (Second Edition)*. (Indianapolis: Wiley Publishing Inc, 2008), pp 608-619.

[7] Fabian van den Broek, "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, p 7, see also sections 1.8 and 7.2: "Originally the internal designs of A5/1 and A5/2 was kept secret. It was only disclosed to GSM manufacturers under an NDA. However in 1999 Marc Briceno reverse engineered the design of both A5/1 and A5/2 from a GSM phone [7]. Both algorithms are stream ciphers, generating keystream from the current frame number and the session key (*Kc*) which is XOR-ed with the plain text. In 2002 an additional A5 algorithm was introduced: A5/3. Unlike with its predecessors, the internal designs of A5/3 where immediately published. It was based on the block-cipher KASUMI, which was already used in third generation networks, and which in turn was based on the block-cipher MISTY (KASUMI is the Japanese word for "mist"). A5/3 is currently considered unbroken and the best cryptographic alternative in GSM." See also: 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), retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf, section 4.7.

[8] 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), retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf, p 3.

intrusiveness over 'in network' wiretapping is also limited to certain situations. Mobile communications protocols only add encryption in 'over the air' communications, meaning that a wiretap authorization implemented by a network provider will be able to obtain the content of text or voice communications without the need to resort to potentially complicated decryption attacks such as those described above. In addition, as elaborated below, IMSI Catchers operating in 'camping mode' are more susceptible to detection and obfuscation than when operating in 'identification mode'. In this sense, in the absence of exigent conditions, traditional wiretapping techniques may be preferable to 'camping mode' for law enforcement. It is perhaps not surprising then that most reported instances of IMSI Catcher use have related to the 'identification mode' functionality of the devices, which does offer utility not easily replicated by traditional law enforcement capabilities (for example, the IMSI Catcher can identify a prepaid temporary device or 'burner' phone to facilitate a traditional wiretap). Indeed, many law enforcement and security agencies have agreed to restrain the use of these devices to identification mode alone.[9]

In addition, it is notable that much of the invasive capacity of IMSI Catchers arises uniquely from their operation in 'identification mode'. Their ability to track devices, to identify anonymous individuals in a specific locale or associated with a specific activity (see **Box 2** on p 84, below), and the manner in which they intercept all identifiers within range indiscriminately leading to high collateral privacy impact (see **Box 3** on p 91, below) are all features relating to the identification mode of the devices. Operating in camping mode, IMSI Catchers still pose a concern as state agencies (and others) can deploy these devices without the awareness, consent or assistance of an intermediary such as a service provider or a court (see **Box 4** on p 95, below). This lack of intermediary involvement can lead to potential misuse, particularly by law enforcement in borderline exigent contexts, by intelligence agencies, or by non-state agencies operating with criminal intent. However, the capacity of intelligence or criminal agencies to conduct excessive wiretapping of mobile devices is a problem with dimensions that extend beyond the use of IMSI Catchers. Additionally, as noted above, most reported uses of IMSI Catchers to date have related to the operation of these devices in identification mode. For this reason, the legal and policy analysis below largely focuses on the use of these devices in 'identification mode'.

[9] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, retrieved November 16 2015, http://www.justice.gov/opa/file/767321/download; Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.

IMSI catchers operating in identification mode principally capture three core identifiers: the International Mobile Subscriber Identity (IMSI) number, the International Mobile station Equipment Identifier (IMEI) and the Mobile Station Integrated Services Digital Network-Number (MSISDN). (Note: These identifiers are relevant to GSM, the dominant means of mobile communication. Comparable identifiers for the other major mobile communications system, Code Division Multiple Access (CDMA) include the Mobile Station ID (MSID), the Electronic Serial Number (ESN) and Mobile Directory Number (MDN), respectively. However, these are not treated at length in this analysis).

Mobile devices must possess a Subscriber Identification Module (SIM) card (a smart card that is transferrable from device to device) to connect to cellular networks.[10] The SIM "identifies and authenticates the phone and user to the network" and "has a unique serial number."[11] This module is identified to the network with an International Mobile Subscriber Identity (IMSI) number that, in turn, "identifies the mobile country code, network code, and mobile subscription identification number."[12] Functionally, the IMSI lets a service provider recognize a particular customer on its network to facilitate customer management tasks such as billing and control over access to particular services.[13] In addition to the IMSI, the mobile device itself (e.g. a specific Blackberry phone, or specific person's cellular-enabled iPad or Android tablet) possesses an International Mobile station Equipment Identifier (IMEI) that is used by network providers to determine whether the device is on a stolen device or other blacklist (for example, if the device lacks the ability to interact with the network).[14] A final identifier, the Mobile Station Integrated Services Digital Network-Number (MSISDN) more commonly referred to as a telephone number, is used to route specific calls to a specific destination device.[15]

---

[10] Fabian van den Broek, (2010) "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.1.2.

[11] Citizen Lab. (2015). "The Many Identifiers in Our Pockets: A primer on mobile privacy and security," *Citizen Lab*, May 13, 2015, retrieved November 16, 2015, https://citizenlab.org/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/.

[12] Citizen Lab. (2015). "The Many Identifiers in Our Pockets: A primer on mobile privacy and security," *Citizen Lab*, May 13, 2015, retrieved November 16, 2015, https://citizenlab.org/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/.

[13] ETSI, 2000. "Digital Cellular Telecommunications System (Phase 2): International Mobile Station Equipment Identities (IMEI)", November 2000, ETS 300 508/3GPP 02.16 v4.7.1: "As described in specification GSM 02.17, an MS can only be operated if a valid "International Mobile Subscriber Identity" (IMSI) is present. An IMSI is primarily intended for obtaining information on the use of the GSM network by subscribers for individual charging purposes."; Citizen Lab. (2015). "The Many Identifiers in Our Pockets: A primer on mobile privacy and security," *Citizen Lab*, May 13, 2015, retrieved November 16, 2015, https://citizenlab.org/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/.

[14] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, sections 2.3.6; 2.16.

[15] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.3.3.

The IMEI is unique to each mobile device, the IMSI is unique to each SIM card (but transferrable between different mobile devices), and an MSISDN is unique to each subscriber (network providers identify subscribers on the basis of IMSI, meaning that multiple telephone numbers can be associated with the same IMSI operating on different networks). The IMSI and IMEI appear to be the most frequent objects of IMSI Catcher use,[16] perhaps because obtaining the MSISDN may require a more intrusive process that involves initiating an actual phone call or text message (often referred to as a silent call or text) between the IMSI Catcher and the target mobile device.[17]

Identifiers such as IMSIs can be retained by cellular providers to identify customers as they traverse different parts of the providers' networks, and to track the times at which this has occurred. In essence, this generates a geo-locational record: the network provider becomes aware of the physical location of the device in question as mobile devices 'check in' with cell phone towers. Such 'check-in' activities (including the time and location of check-in) will be correlated by the network provider to the subscriber's IMSI. By linking this information along with its timestamps, the provider, or any other party with access to the information, can trace the physical movement(s) of the device and person(s) associated with it.

IMSI Catchers set to identification mode can be used in different configurations so as to achieve different objectives. A United States Department of Justice (DOJ) policy on such equipment describes these functionalities as follows:

> When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.[18]

---

[16] See, for example, *R v Mirarchi*, Case No: 540-01-063428-141, November 18, 2015, Québec Superior Court, leave to appeal granted, appeal discontinued: 2016 QCCA 597, para 22.

[17] SHOGHI, 2013. "Wideband GSM Monitoring System", July 2013, *Shoghi Quarterly Newsletter*, http://www.shoghicom.com/newsletter/july2013/latest_product1.html, "IMSI/TMSI identifying by known MSISDN number (silent call or hush SMS)"; and Security: PWNED, "Android-IMSI-Catcher-Detector – Glossary of Terms", last revised February 9, 2016, accessed July 28, 2016, https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/wiki/glossary-of-terms: "In terms of GSM interception, a silent call is a call originated from the GSM Interceptor [IMSI Catcher] to a specific IMEI/IMSI, in order to make correlations between IMEI/IMSI and MSISDN (Mobile Subscriber Integrated Services Digital Network-Number, which is actually the telephone number to the SIM card in a mobile/cellular phone). By using the silent call, an GSM Interceptor can find out a certain phone number allocated to a specific IMEI/IMSI. Silent calls are a result of process known as pinging. This is very similar to an Internet Protocol (IP) ping. A silent call cannot be detected by a phone user. Not to be confused with Spy Call, which mean listen to phone surroundings."

[18] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States

This latter use-case entails massively capturing the IMSI and IMEI numbers of all devices in a region where the IMSI Catcher is operating. By calculating signal strength and time, location can be determined. Where multiple IMSI Catchers are deployed simultaneously a device controller can triangulate the positioning of specific devices with even greater precision.[19] Even when set to identification mode these devices are immensely invasive; they capture surrounding device identifiers through walls and over hedges, and can be used to determine persons' relative proximity to the given IMSI Catcher. To some degree, operating in identification mode is *more* invasive than in camping mode as it interrupts the interaction between the device and the network.[20] In effect, IMSI Catchers are inherently mass surveillance instruments. After device controllers have collected a large volume of identifiers using their IMSI Catchers they can analyze that data and, subsequently, determine the presence of specifically targeted identifiers.

IMSI Catchers do not merely passively receive data from mobile devices, but tend to actively trigger such devices to identify themselves by disrupting standard mobile device operation.[21] In general operation, GSM mobile phones will register with their network service provider when activated or when joining a new network, which involves a one-time authentication process during which key identifiers such as the IMSI are transmitted.[22] They will also identify the closest cell tower, and notify the network of its location so that interaction between the mobile device and the network provider can be routed through that cell tower.[23] When an IMSI Catcher is 'turned on' in a given region, mobile devices within range will already be engaged with the network as well as with the 'closest' network cell tower.

The pre-existing interconnection between mobile devices and the network creates two hurdles to IMSI Catcher operation. First, the already-identified 'closest' tower will be the conduit through which the mobile device communicates with the network and, hence, the mobile device will not interact with the IMSI Catcher. Second, upon initial registration and confirmation of a subscriber by means of IMSI transmission,

---

Government, September 3, 2015, retrieved November 16 2015, http://www.justice.gov/opa/file/767321/download.

[19] Teresa Scassa and Anca Sattler. (2011). "Location-Based Services and Privacy", *Canadian Journal of Law and Technology* 9, https://ojs.library.dal.ca/CJLT/article/download/4848/4367, p 102.

[20] Colin Freeze, 2016. "RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals", *The Globe and Mail*, April 18, 2016, http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memo-reveals/article29672075/.

[21] *Maryland v Andrews*, (2016) *Md App LEXIS 33, File No 1496 (Md Ct of Special Appeals), pp *77-79.

[22] This is technically referred to as 'IMSI Attach', a process by which the mobile subscriber identifies itself to the network and the network determines which services the subscriber is eligible: Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf.

[23] Fabian van den Broek. (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.5.2.

the network will assign a 'Temporary Mobile Subscriber Identity' (TMSI) number to each subscriber on its network. The TMSI is subsequently used to identify the subscriber's device. The issuance of TMSI numbers is a security measure meant to ensure that the IMSI is not repeatedly transmitted each time that the network and the mobile device interact. Put another way, the IMSI is only generally sent to the first mobile tower that a mobile device interacts with on a given network for the purpose of authentically identifying the customer in question.[24] The IMSI is then stored deeper in the network, in the Visitor Location Registry (VLR), and most future cell towers the mobile device interacts with (including 'fake' cell towers like IMSI Catchers) will only receive the TMSI.[25] As elaborated by van den Broek, "subscriber identity (IMSI) confidentiality" is one of five security goals established by ETSI from the GSM system, and the TMSI is the means of approximating this goal:

> [The subscriber identity confidentiality] property states that the IMSI should not be made available or disclosed to unauthorized individuals, entities or processes. This feature should provide for identity privacy and location privacy of the subscriber and enhance other security features, like user data confidentiality.
>
> Subscriber identity confidentiality is achieved by allocating a TMSI to a MS and using the TMSI for all further communications.[26]

The TMSI, however, is of no assistance to a state agency seeking to persistently identify a mobile device (or the individual behind it) because it only exists locally and is even constantly re-assigned to other mobile devices within range once the initial device moves to a different location.[27]

To overcome these two hurdles the IMSI Catcher must first induce the mobile device to register with it as its new primary cell tower. This is carried out by triggering a 'location update', which occurs when a mobile device believes it has moved out of the range of

---

[24] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 8.1.1.

[25] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 8.1.1.

[26] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 8.1.1.

[27] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.5.2: "Location updates are always initiated by the MS [mobile device] and always result in a new TMSI being assigned to the MS." This means that the TMSI will not even persist a single change in location, making it an ineffective mechanism for tracking a particular mobile device or for 'wiretapping' it. Moreover, the TMSI is only "conditionally stored in the VLR" and is in fact re-allocated to another mobile device in a given area once the mobile device it had previously been allocated to moves outside of that region. It will only be retained if there is some issue with the mobile device, for example if the device has 'disappeared' from the network, the TMSI / mobile device correlation will be retained to avoid the mistaken allocation of the TMSI to two devices at one time: ETSI, (2016). "Digital Cellular Telecommunications System (Phase 2+) / Universal Mobile Telecommunications System (UTMS) / LTE; Location Management Procedures", January 2016, ETSI TS123 012 | 3GPP TS 23.012 ver 13.0.0 Rel 13, section 3.6.1.4.

one cell tower and into that of another. A GSM mobile device periodically polls all cell towers within range to identify that which is associated with its network provider and is emitting the 'strongest' signal.[28] When it identifies a cell tower with a stronger signal than the one with which it is currently registered, the mobile device presumes that it has moved into a new region and re-registers with the new tower by carrying out a 'location update'.[29] To induce the mobile device to interact with it more robustly, then, most IMSI Catchers are designed first to impersonate different network providers and then to 'trick' all phones within range from the particular network provider being impersonated into believing that they have moved into the range of a 'new' tower (the IMSI Catcher) by emitting a stronger signal than that of any other tower within range.[30] To speed up the process, some IMSI Catchers are further equipped with cell phone 'jammers', which interrupt existing interactions between mobile devices within range and the mobile network.[31] Such disruptions will force mobile devices to 'poll' local towers immediately.

Even once this more robust interaction is achieved and all mobile devices within range have updated their location so that they are interacting with the IMSI Catcher as the 'closest' tower, only TMSI identifiers will be obtained from most devices within range (excluding those that are re-activated post IMSI Catcher activation).[32] In order

[28] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdfGSM, section 2.5.2: "A [mobile device or "MS"] is always listening to all [cell towers or "BTSs"] it can receive, in order to judge which one has the best reception. When another BTS gives a better reception then the current BTS the MS will conclude that it has moved in a different cell area. … the MS will initiate a location update (via the new BTS)."

[29] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.5.2: ""A [mobile device or "MS"] is always listening to all [cell towers or "BTSs"] it can receive, in order to judge which one has the best reception. When another BTS gives a better reception then the current BTS the MS will conclude that it has moved in a different cell area. … the MS will initiate a location update (via the new BTS)."

[30] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, p 90: "If an attacker starts a fake base station, seemingly from the correct provider, in the neighborhood of his victim MS, then this MS will try to register to the fake base station. … Naturally the attacker would have to make sure that the reception from his fake base station is better than the reception of the current serving BTS. This attack, being an active attack, can be detected. This is typically how industrial IMSI catchers work." See also Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p 2: "Cell-site simulators…function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower."

[31] 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), retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

[32] ETSI, (2016). "Digital Cellular Telecommunications System (Phase 2+) / Universal Mobile Telecommunications System (UMTS) / LTE: Location Management Procedures", January 2016, ETSI TS 123 012 | 3GPP TS 23.012 v13.0.0 Rel 13, section 3.5: "The MS [mobile device] will identify itself by either the IMSI or the TMSI plus Location Area Identification of the previous VLR." Ie if the mobile devices has already authenticated with the network prior to its interconnection with the IMSI Catcher, only the TMSI will be sent whereas the IMSI will be retained deeper in the network, in the Visitor Location Registry. See also: section 2.4.1 (Explicit IMSI detach/attach to a network occurs when a mobile device is de-activated/activated, respectively).

to induce these devices to send their persistent IMSIs in lieu of the TMSI, the IMSI Catcher must disrupt the normal operation of these devices by sending out special identity requests that induce re-transmission of the IMSI (and IMEI). While the GSM communications protocols allow for this type of query, it contradicts the GSM system's security goals, as the GSM system tries to protect IMSIs by limiting their use to the rare network sign-on process rather than by encrypting it in transit. Inducing IMSI/IMEI transmission in this manner therefore interferes with the normal operation of such devices and exploits the intended functioning of the GSM system.[33]

Obtaining other device identifiers, such as the MSISDN (phone number) require even greater intrusion into the standard operation of mobile devices within range of the IMSI Catcher. This is because, much like the IMSI, the MSISDN is not stored in the cell tower, but deeper in the network in the Visitor Location Register (VLR).[34] However, unlike the IMSI, the MSISDN is not transmitted to the cell tower when a mobile device signs on or registers its location to a network and, instead, remains controlled and stored by elements deeper within the network.[35] A cell tower (including a fake cell tower) must undertake even more intrusive measures induce the mobile device to undertake interactions with the tower that *do* include transmission of the MSISDN.[36] This inducement could, for example, require the IMSI Catcher to initiate a fake (or 'silent') call with the mobile device.[37] In light of this greater level of intrusiveness, it is

[33] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 8.2.2.

[34] Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.3.4, indicates that the MSISDN for each IMSI within a given region is housed in the VLR which is located deeper in the network from cell towers (also see *ibid*. figure 2.1 on p 17). See also , section 2.1.2 (MSISDN is *not* stored in the cell tower).

[35] In the GSM network, the correlation between a mobile device's phone number (MSISDN) and a specific device is stored in the VLR and occurs from within the network, not from the device. The phone number for each IMSI is contained in, and populated from, the Home Location Register (HLR) deep within a given provider's network. The mobile device sends its IMSI to the 'tower' which then forwards it to the VLR. The VLR then queries the HLR for the appropriate MSISDN associated with the given IMSI. Once obtained, it is stored locally in the Visitor's Location Register. As the MSISDN is obtained by the VLR from the HLR, the local 'tower' is not involved in the interaction and does not gain access to the MSISDN at the authentication or location registration stages. See: Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.3.3, 2.3.4 and 2.5.2.

[36] For example, the MSISDN of the mobile device (MS) will often be transmitted to the 'tower' (BTS) in the call setup stage (see Fabian van den Broek, (2010). "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, Table 6.5, p 67).

[37] *Shoghi Quarterly Newsletter*, http://www.shoghicom.com/newsletter/july2013/latest_product1.html, "IMSI/TMSI identifying by known MSISDN number (silent call or hush SMS)"; and Security: PWNED, "Android-IMSI-Catcher-Detector – Glossary of Terms", last revised February 9, 2016, accessed July 28, 2016, https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/wiki/glossary-of-terms: "In terms of GSM interception, a silent call is a call originated from the GSM Interceptor [IMSI Catcher] to a specific IMEI/IMSI, in order to make correlations between IMEI/IMSI and MSISDN (Mobile Subscriber Integrated Services Digital Network-Number, which is actually the telephone number to the SIM card in a mobile/cellular phone). By using the silent call, an GSM Interceptor can find out a certain phone number allocated to a specific IMEI/IMSI. Silent calls are a result of process known as pinging. This is very similar to an Internet Protocol (IP) ping. A silent call cannot be detected by a phone user. Not to be confused with Spy Call, which mean listen to phone surroundings."

perhaps unsurprising, then, that while many IMSI Catchers technical *can* obtain identifiers such as the MSISDN, the device operators tend to focus on capturing IMSI numbers as their primary targets.

Even in their most basic operation, however, IMSI Catchers can have intrusive impacts. By convincing mobile devices within range that the IMSI Catcher is the 'closest tower' and inducing these devices to interact with it, an IMSI Catcher interferes with the ability of such devices to interact with the broader GSM network, rendering them temporarily unable to communicate. As noted above, an IMSI Catcher effectively 'tricks' a mobile device into believing that the IMSI Catcher is the closest cell tower to it and, hence, its avenue to the network. However, unless the IMSI Catcher enters 'camping mode', where the IMSI Catcher also impersonates the mobile device in a second connection initiated between itself and the network,[38] the IMSI Catcher cannot forward communications between the mobile device and the network. In essence, this means that when operating in 'camping mode' an IMSI Catcher is a fraudulent node on the network through which phone calls and other communications can transit back and forth. When operating in 'identification mode', however, the IMSI Catcher is a functional dead end that effectively removes the mobile device from the communications network and impedes its ability to receive or send communications, including emergency 911 calls.[39] The IMSI Catcher can receive outgoing calls from the device, but cannot forward them, nor can the IMSI Catcher receive incoming calls for the device, as the service provide will not know to forward these to the IMSI Catcher.

While operation in identification mode can occur in short 'bursts', engaging mobile devices within range and rapidly releasing them back to the network,[40] engagement can be for more extensive periods of time if the objective is to track a device or to identify a series of individuals at a given locale over time. When engaging mobile devices, an IMSI Catcher will interact with all mobile devices within range that are associated with a particular cellular network provider. When the operator of an IMSI Catcher does not know the network service provider their target is using (or has no specific target), the IMSI Catcher will repeatedly cycle through all known providers so that all mobile devices within range will eventually be 'captured'. An IMSI Catcher's

---

[38] Joseph Ooi, (2015). "Imsi Catchers and Mobile Security", *EAS 499 Senior Capstone Thesis*, April 29, 2015, https://www.cis.upenn.edu/current-students/undergraduate/courses/documents/EAS499Honors-IMSICatchersandMobileSecurity-V18F-1.pdf,

[39] Colin Freeze, (2016). "RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals", *The Globe and Mail*, April 18, 2016, http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memo-reveals/article29672075/.

[40] 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), retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf, p 2.

effective range is not only a function of its signal strength, but is also determined by the signal strength and density of surrounding towers. An IMSI Catcher will have a wider area of coverage in areas where there are fewer towers to overpower its signal and attract devices away from it than it will in an area with densely spaced high-powered towers. While some IMSI Catcher implementations are designed to immediately deactivate if any mobile device interacting with them initiates a 911 call, tests have shown that this process is ineffective, with over 50% of test devices failing to complete their 911 calls.[41]

B. In Operation: Capacity to Interfere with Devices & Privacy

A range of actors have deployed and used IMSI Catchers in identification mode to achieve varied objectives. Shopping mall operators have tested them to follow customers around as they shop by collecting unique identifiers at strategic locations inside the mall.[42] A criminal enterprise in South Africa used them track members of a tender committee in order to blackmail committee members with that information to win a multi-million dollar tender.[43]

Unknown parties, suspected to be intelligence agencies, or domestic policing or security agencies, have strategically placed IMSI Catchers around cities such as Washington, DC and across the Czech Republic.[44] Law enforcement agencies have used IMSI Catchers to locate specific individuals by driving around a city until the sought IMSI was located.[45] Canadian correctional services have deployed devices with IMSI Catcher-like capacities at some prisons, implicating the privacy of prisoners, employees and visitors alike.[46] The US Marshall Service has placed high-powered IMSI Catchers (referred to as 'Digital Receiver Technology' or 'DRT' Box) onto small airplanes in order to canvass cities for

---

[41] Colin Freeze, (2016). "RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals", *The Globe and Mail*, April 18, 2016, http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memo-reveals/article29672075/.

[42] Sean Gallagher. (2011). "We're Watching: malls track shopper's cell phone signals to gather marketing data," *Ars Technica*, November 25, 2011, retrieved November 16, 2015, http://arstechnica.com/business/2011/11/were-watching-malls-track-shoppers-cell-phone-signals-to-gather-marketing-data/.

[43] Solly Maphumulo. (2015). "Man in dock over R25m bugging device," *IOL*, August 4, 2015, retrieved November 16, 2015, http://www.iol.co.za/news/crime-courts/man-in-dock-over-r25m-bugging-device-1.1895186.

[44] Ashkan Soltani and Craig Timberg. (2014). "Tech firm tries to pull back curtain on surveillance efforts in Washington," *The Washington Post*, September 17, 2014, retrieved November 16, 2015, 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; Ryan Gallagher, "Criminals May be Using Covert Mobile Phone Surveillance Tech for Extortion", *Slate*, August 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.

[45] *Florida v Thomas*, Case No: 2008-CF-3350A, Suppression Hearing, August 23, 2010, TRANSCRIPT, pp. 23-24. See: https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf.

[46] Jordan Pearson, "A Canadian Prison Was Spying on Non-Inmates and Recording Their Calls and Texts", *Motherboard*, September 24, 2015, https://motherboard.vice.com/read/a-canadian-prison-was-spying-on-people-and-recording-their-calls-and-texts.

identifiers.[47] There are even suggestions that the US National Security Agency (NSA) has deployed airborne DRT boxes in combat zones and (potentially) in allied counties.[48]

From this list of activities, some likely state agency deployment scenarios can be distilled:

- Confirming presence of a device in a target's home prior to a search thereof;[49]
- Identifying an individual responsible for sending harassing text messages;[50]
- Locating a stolen mobile device as a precursor to searching homes in the vicinity;[51]
- Locating specific individuals by driving around a city until a known IMSI is found;[52]
- Mounted on airplanes by the United States Marshall Service to sweep entire cities for a specific mobile device;[53]
- To monitor all devices within range of a prison to determine whether prisoners are using cell phones;[54]
- Reportedly at political protests to identify devices of individuals attending;[55]
- To monitor activity in the offices of an independent Irish police oversight body.[56]

---

[47] Devlin Barrett. (2014). "Americans' Cellphones Targeted in Secret U.S. Spy Program," *The Wall Street Journal*, November 13, 2014, retrieved November 16, 2015, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

[48] Electrospaces, "DRTBOX and the DRT Surveillance System", *electrospaces.net* November 27, 2013, http://electrospaces.blogspot.ca/2013/11/drtbox-and-drt-surveillance-systems.html

[49] See *Maryland v Taylor, Case No 11410031, Suppression Hearing, November 21, 2014, TRANSCRIPT*, 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."

[50] 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/.

[51] *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: 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/). 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."

[52] *Florida v Thomas*, Case No: 2008-CF-3350A, Suppression Hearing, August 23, 2010, TRANSCRIPT, pp 22-23, See: https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf; 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/: "'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.'"

[53] Devlin Barrett. (2014). "Americans' Cellphones Targeted in Secret U.S. Spy Program," *The Wall Street Journal*, November 13, 2014, retrieved November 16, 2015, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

[54] Colin Freeze & Matt Braga. (2016). "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/.

[55] Fruzsina Eordogh. (2014). "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.

[56] Privacy International and Digital Rights Ireland, (2015). "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.

As implied, government agencies can use the IMSI Catchers to identify otherwise anonymous individuals at specific locations by, for example, setting up an IMSI catcher near a political protest or a conference, or at a border crossing.[57] Such placements let law enforcement or other government agencies generate comprehensive lists of all the mobile devices in the area, such as the protest participants or all the persons on a plane or below its flight path. With the IMSI numbers collected a government agency could identify people by associating the numbers with telecommunications companies' subscriber records.

While 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.[58] Such identifiers have significant invasive capacity because they allow for otherwise distinct, anonymous and unlinkable activity to be connected and compiled into a profile.[59] Detailed information can be gleaned from the locations we visit.[60] 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.[61] This in turn implicates associational privacy.[62] IMSI/IMEI identifiers can also be used to identify digital activities such as web browsing.[63] All of this tracking and profiling can occur without any need to ever match a compiled profile to an individual's

---

[57] Frank La Rue. (2013). "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," Human rights Council, Twenty-third session, April 17, 2013, retrieved February 26, 2016 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, para 36.

[58] Article 29 Data Protection Working Party. (2011). "Opinion 13/2011 on Geolocation services on smart mobile devices," European Commission, Adopted on May 16, 2011, retrieved December 1, 2015, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, p 7.

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

[60] Teresa Scassa and Anca Sattler. (2011). "Location-Based Services and Privacy," *Canadian Journal of Law & Technology* 9, https://ojs.library.dal.ca/CJLT/article/download/4848/4367, pp 109-113.

[61] 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'.

[62] *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 S.C.R. 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.").

[63] Adam Senft, Andrew hilts, Christopher Parsons, Jakub Dalek, Jason Q. Ng, John Scott-Railton, Katie Kleemola, Masashi Crete-Nishihata, Ron Deibert, and Sarah McKune. (2015). "A Chatty Squirrel: Privacy and Security Issues with UC Browser," *Citizen Lab*, May 21, 2015, retrieved December 1, 2015, https://citizenlab.org/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/.

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.

Moreover, geo-location information is highly identifying information.[64] Indeed, one comprehensive study of anonymous geo-location data sets found that 95% of individuals within it were unique, allowing for re-identification attacks based on correlation to publicly available location information sources:

> … in a dataset where the location of an individual is specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals. We coarsen the data spatially and temporally to find a formula for the uniqueness of human mobility traces given their resolution and the available outside information. This formula shows that the uniqueness of mobility traces decays approximately as the 1/10 power of their resolution. Hence, even coarse datasets provide little anonymity.[65]

As noted above, IMSI Catchers provide identifiers in association with a given geography. As they can be placed strategically for greater coverage than cell phone towers dispersed for optimal bandwidth coverage, the geo-locational information obtained by IMSI Catchers is likely to be even less coarse than the tower-site data equivalent used in the study.[66]

Finally, IMSI Catchers themselves provide an avenue for direct matching of permanent digital identifiers such as IMSI/IMSE to real world identities. This capacity includes the ability to combine visual verification with widespread IMSI Catcher deployment, or use of social engineering techniques such as telephoning mobile devices associated with collected IMSIs/IMEIs to determine device ownership. The United States District Court for the Northern District of Illinois described this identification capacity as such:

> 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

---

[64] Article 29 Data Protection Working Party. (2014). "Opinion 05/2014 on Anonymisation Techniques," *European Commission*, Adopted on April 10, 2014, retrieved December 2, 2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[65] 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, http://www.nature.com/articles/srep01376.

[66] For example, IMSI Catchers can be pointed at specific areas of interest to increase the precision of their field of capture: *In the Matter of the Application of the United States of America for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, https://www.unitedstatescourts.org/federal/ilnd/317964/. See also: *R v Mirarchi*, Case No: 540-01-063428-141, November 18, 2015, Québec Superior Court, leave to appeal granted, appeal discontinued: 2016 QCCA 597, para 39.

> 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.) According to the application submitted to the Court, with the ESN or IMSI, the United States can subpoena the service provider to obtain the cell phone's telephone number. However, according to the Department of Justice, a cell site simulator can collect a cell phone's telephone number directly; thereby eliminating this step.[67]

This demonstrates how easily IMSI/IMEI (and any information associated with them) can be linked to a known individual, confirming how grave a threat collection of such identifiers poses to anonymity.

C. Ability to Detect & Avoid IMSI Catchers

A growing number of tools, which are in their infancy, are available to detect IMSI Catchers. Two dominant tools to detect fake base towers are SnoopSnitch[68] and Android IMSI-Catcher Detector.[69] Both are only available for the Android mobile operating system. SnoopSnitch cannot certifiably assert that a mobile device is connecting to an IMSI Catcher. Android IMSI Catcher Detector is also in early development. This application monitors to ensure that mobile towers the Android device in question connects to have been seen before, that the identifiers emitted by the base station are normal, that information provided by neighbouring towers registers as normal, that applications are not being silently installed, that signal strengths are at expected levels, and that 'silent' SMS messages are not being sent by any given tower. The latter – silent SMS messages – is a mechanism sometimes used by IMSI Catchers to induce mobile devices in the area to send additional information or to send information more frequently to facilitate more fine-grained tracking.[70] As a development product Android IMSI Catcher Detector is not available for general use by the public at the time of publication.

Generally, a core function of the aforementioned, and equivalent, projects to detect IMSI Catchers relies on identifying suspicious changes to the cellular infrastructure to

---

[67] *In the Matter of the Application of the United States of America for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, https://www.unitedstatescourts.org/federal/ilnd/317964/.

[68] SnoopSnitch. (2015). Open source public repository. Last updated December 11, 2015, retrieved December 18, 2015, https://opensource.srlabs.de/projects/snoopsnitch/repository.

[69] Android IMSI-Catcher Detector. (2015). Github Repository. Last updated December 18, 2015, retrieved December 18, 2015, https://github.com/SecUpwN/Android-IMSI-Catcher-Detector/

[70] Jennifer Valentino-Devries, "How 'Stingray" Devices Work", *Wall Street Journal*, September 21, 2011, http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/. See also *infra*, footnotes 33-37 and accompanying text.

which a mobile device is connected.[71] Specifically, the applications will notify users of potential IMSI Catcher use after the applications detect changes in how communications are encrypted or if the cellular tower identifier changes or an unexpected tower identifier is encountered. Some of this 'suspicious' activity depends on collecting significant volumes of data about 'normal' cellular towers. For example, one method maps fixed cell tower sites in a given area and then identifies ephemeral towers that suddenly appear, disappear, or move, as suspect.[72] Others map mobile capabilities of cell sites in a geographic region. Departures from these capabilities (for example, an atypical reduction from 4G to 2G in an area known to contain extensive 4G coverage) might imply an encryption downgrade attack by an IMSI Catcher.[73] Some of these detection techniques will be more effective depending on how the IMSI Catcher is being deployed. For example, as noted above, IMSI numbers are sent without encryption during the authentication process, meaning that they can be obtained without a 'downgrade' attack (4G > 2G), whereas interception of the content of communications likely requires this more visible interference. Additionally, obtaining identifiers such as the MSISDN (the phone number) appears to require a greater level of interference with the device, such as the sending of potentially detectable 'silent' SMSs or calls.

The success of such projects often depends on crowd-sourced data collection and sharing such data with other users. However, attempts to create and improve IMSI Catcher detectors continue to proliferate and improve. One seemingly successful effort to date, for example, involved an application developed for a customized security phone. This application detected multiple likely IMSI Catchers of unknown ownership and purpose at various points throughout Washington, DC.[74] There are also commercial grade IMSI Catcher detectors that appear to promise greater levels of detection success, but the operation parameters and accuracy of these devices

[71] Luca Bongiorni. (2012). "iParanoid: A Mobile Cell Networks Intrusion Detection System," Bootcamp 2012 – University of Luxembourg, September 20, 2012, retrieved December 18, 2015, http://www.slideshare.net/iazza/mobile-cell-networksintrusiondetectionsystemiparanoidlucabongiorni; see also: Sean Gallagher. (2015). "This machine catches stingrays: Pwnie Express demos cellular threat detector," *Ars Technica*, April 20, 2015, retrieved December 18, 2015, http://arstechnica.com/information-technology/2015/04/this-machine-catches-stingrays-pwnie-express-demos-cellular-threat-detector/.

[72] 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), retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

[73] 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), retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

[74] 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.

has not been publicly verified.[75] These appear to replicate much of the functionality of an IMSI Catcher by, for example, "scanning for abnormalities in the spectrum", in order to facilitate better detection techniques.[76] However, all current detection techniques are subject to false positives as many of the indicia they rely upon to identify IMSI Catchers may be attributable to other factors, for example a downgrade from 4G > 2G may indicate a problem with a tower as opposed to an intentional downgrade attack perpetrated by an IMSI Catcher. Similarly, a high proportion of devices re-sending 'IMSI' numbers instead of 'TMSI' numbers might indicate IMSI Catcher use, as mobile devices are more likely re-authenticate (triggering IMSI transmission where the TMSI would normally be used: see **Section One: A**, above). However, network handovers, disruptions, or routing problems might also cause disproportionate IMSI to TMSI ratios in a given area, especially in areas where cellular base stations have not been densely deployed and many devices are roaming.

Avoiding an IMSI Catchers is an even more challenging proposition than detecting one. Because IMSI Catchers replicate a portion of the cellular network that most mobile devices have no capability to selectively block, even if successfully detected, avoiding interaction with an IMSI Catcher with standard mobile devices is challenging. If the IMSI Catcher in question is operating in camping mode some additional encryption might be deployed to render IMSI Catcher access to communications contents far more difficult, such as the use of an encrypted VoIP or instant messaging application. However, identification mode is far more difficult to avoid. The digital identifiers sought by IMSI Catchers constitute an integral component of cellular communications and currently there is no mechanism for encrypting their transmission so that a device's IMSI number is occluded from cell towers in the vicinity.[77] Even the use of a short term or 'burner' device is susceptible to detection because such devices also transmit IMSI/IMEI identifiers that can be intercepted and associated with the individual using the 'burner'. Moreover, unlike wireless network routers, mobile devices have no capacity to choose which towers (or 'fake' towers) to connect to and

[75] See for example DFCR AG, "IMSI Catcher Detector", last accessed July 14, 2016, http://www.dfrc.ch/solutions/imsi-catcher-detector/.

[76] DFRC AG's IMSI Catcher Detector, for example, monitors all IMSI numbers appearing within range and flags an abnormally high ratio of IMSI numbers to TMSI numbers as indicative of the presence of an IMSI Catcher: DFCR AG, "IMSI Catcher Detector: Smart Protection of Critical Infrastructure", last accessed July 14, 2016, http://www.dfrc.ch/wp-content/uploads/2015/08/BrochureA4IMSICatcherDetector.pdf, and screenshot (last accessed July 15, 2016): http://www.dfrc.ch/wp-content/uploads/2015/06/IMSI_catcher_detector_detail-e1434524833966.png, As noted in **Section One: A**, above, IMSI Catchers may compel mobile devices within range to re-send the rarely transmitted IMSI number instead of the more ephemeral TMSI. The IMSI is typically only transmitted when a mobile device 'logs on' to a new cellular network. A high proportion of IMSIs in a given area could therefore indicate that an IMSI Catcher has tricked a number of devices into believing they switched networks.

[77] Fabian van den Broek, Roel Verdult & Joeri de Ruiter, 2015. "Defeating IMSI Catchers", October 2015, *22nd ACM SIGSAC Conference on Computer and Communications Security CCS 15*, http://dx.doi.org/10.1145/2810103.2813615.

which to avoid.[78] The only certain way to avoid an IMSI Catcher operating in identification mode may be to simply turn off one's mobile device,[79] but this is unlikely to be a realistic proposition for most individuals.

Section Two: Uncovering IMSI Catcher Use – A Study in Obfuscation

Civil liberties advocates, journalists, academics, and politicians around the world have tried to understand how, why, and at what regularity state agencies use IMSI Catchers. This section first recounts efforts in the United Kingdom and United States to determine how the devices are used. It then examines the situation in Canada, showcasing ongoing efforts by state agencies to conceal information pertaining to IMSI Catcher use.

A. Revealing IMSI Catcher Use Abroad

State agencies' usage of IMSI Catchers in other jurisdictions has been difficult to discern due to a range of obfuscation techniques. In the United States, by contrast, more detailed information regarding the use of these devices is beginning to appear on the public record. Such revelations are only now occurring, however, after years of sustained efforts from journalists and civil society groups.

Accurate information regarding IMSI Catcher use in Europe has been difficult to uncover. In the United Kingdom, law enforcement procurement of IMSI Catchers has been publicly known, but not officially confirmed, since 2011.[80] However, despite attempts to obtain details regarding their use by journalists[81] and calls for enhanced transparency from civil liberties groups[82] the government has maintained a wall of obfuscation and, as a result, little is known about how these devices are deployed or used. Attempts to use right to information laws to learn about government agencies'

---

[78] Andrew Couts, 2013. "Meet the $250 Verizon Device That Lets hackers Take Over Your Phone", July 31, 2013, *Digital Trends*, http://www.digitaltrends.com/mobile/femtocell-verizon-hack/.

[79] *ACLU of NC v Department of Justice*, (2014) 70 F.Supp.3d 1018, (N Dist California), 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." See also: *Florida v Thomas,* Case No: 2008-CF-3350A, Suppression Hearing, August 23, 2010, TRANSCRIPT, https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf, 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."

[80] Ryan Gallagher and Rajeev Syal. (2011). "Met police using surveillance system to monitor mobile phones," *The Guardian*, October 2011, retrieved November 16, 2015, http://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance.

[81] Joseph Cox. (2014). "UK Police Won't Admit They're Tracking People's Phone Calls," *Motherboard*, August 7, 2014, retrieved November 16, 2015, http://motherboard.vice.com/en_uk/read/uk-police-wont-admit-theyre-tracking-peoples-phone-calls.

[82] Eric King and Matthew Rice. (2014). "Behind the curve: When will the UK stop pretending IMSI catchers don't exist," *Privacy International*, November 5, 2014, retrieved November 16, 2015, https://www.privacyinternational.org/node/454.

possession or operation of the devices were equally unsuccessful. Public acknowledgement in the media of IMSI Catcher use notwithstanding, London's Metropolitan Police Service first could not locate any records relating to IMSI Catcher use and subsequently refused to confirm or deny the existence of any such records on the basis that it might prejudice future theoretical use of such devices.[83]

In Ireland in 2014, the Garda Siochana Ombudsman Commission (GSOC), an independent body charged with overseeing the Irish police, discovered it had been targeted by a covert surveillance campaign.[84] In a subsequent inquiry into the matter, it emerged that an IMSI Catcher was used as part of the broader surveillance of GSOC's offices.[85] However, when asked, the Irish Minister of Justice and Equality advanced the view that IMSI Catcher use is effectively unregulated in Ireland and thus left significant uncertainty concerning how these devices were used by Irish law enforcement.[86] Somewhat belying claims that IMSI Catcher use cannot coincide with public transparency in the European system, Germany has openly and explicitly regulated IMSI Catcher use since 2001, including law enforcement and intelligence agency obligations that generate annual statistical reporting on the use of these devices.[87]

In the United States, general knowledge of IMSI Catcher use has been a matter of public record for over two decades. However, a range of obfuscation measures have prevented or significantly delayed important information from reaching the public record. This has led to comparably sparse public information regarding the use of these tools when compared to other electronic surveillance tools, as two authors concluded in 2014, regarding:

> (1) statutory authorities that may permit or preclude law enforcement use and how

[83] See Correspondence between Metropolitan Police Service and Eric King, Re Freedom of Information Request Reference No: 2011120002742, dated November 8, 2011, November 12, 2011 and January 24, 2012, archived at: WhatDoTheyKnow. (2011/2012). "IMSI Catcher Guidance," October 22, 2011 – January 24, 2012, retrieved February 26, 2016, https://www.whatdotheyknow.com/request/imsi_catcher_guidance.

[84] Richard Tynan. (2014). "€5,000 to compromise Ireland's mobile phone infrastructure," *Privacy International*, February 27, 2014, retrieved February 26, 2016,, https://www.privacyinternational.org/?q=node/163; Conor Lally. (2014). "Bugging found at offices of Garda complaints watchdog," *The Irish Times*, February 9, 2014, retrieved February 26, 2016, http://www.irishtimes.com/news/crime-and-law/bugging-found-at-offices-of-garda-complaints-watchdog-1.1685345.

[85] Privacy International and Digital Rights Ireland. (2015). "The Right to Privacy in Ireland," *Digital Rights Ireland*, September 2015, retrieved February 26, 2016, https://www.digitalrights.ie/dri/wp-content/uploads/2015/12/Ireland_UPR-Stakeholder-Submission-DRI-and-Privacy-International_FINAL.pdf, para 54.

[86] Privacy International and Digital Rights Ireland. (2015). "The Right to Privacy in Ireland," *Digital Rights Ireland*, September 2015, retrieved February 26, 2016, https://www.digitalrights.ie/dri/wp-content/uploads/2015/12/Ireland_UPR-Stakeholder-Submission-DRI-and-Privacy-International_FINAL.pdf, paras 55-56.

[87] Aidan Wills & Mathias Vermeulen, (2011). "Parliamentary Oversight of Security and Intelligence Agencies in the European Union," European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2011, PE 453.207, http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf; Daehyun Strobel, (2007). "IMSI Catcher", July 13, 2007, http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf.

> the DOJ interprets such authorities to permit or limit law enforcement use (to include any Fourth Amendment constraints); (2) the frequency or regularity with which such technology is used by federal, state, and local law enforcement; (3) the types of investigations or actual factual scenarios where law enforcement agencies have used the technology; and (4) any related prosecution-based and policy-driven considerations for the retention of data collected by an IMSI catcher.[88]

Additional secrecy has occluded attempts to determine whether specific agencies are operating IMSI Catchers, as well as whether they have been used in specific cases. This secrecy largely emerges from Non Disclosure Agreements which have allegedly barred state agencies from disclosing to anyone, including courts, whether the devices have been used in the course of intelligence gathering or investigations. A number of rationales have been advanced as justification for the secrecy that these agreements seek to enforce. First, some police agencies have asserted that IMSI Catchers are classified as regulated defense articles on the United States' munitions list.[89] Because of this, some agencies allegedly maintain that "technical details related to the technology are subject to the non-disclosure provisions of the [Arms Control Export Act and International Traffic in Arms Regulation]."[90] Second, the Federal Bureau of Investigation (FBI) has classified information relating to IMSI Catchers as "homeland security information" under the "Homeland Security Act", thus allowing the FBI to retain control of device-related information even where local and municipal agencies are the primary vehicles for its deployment.[91] Finally, some agencies have asserted that disclosing information pertaining to their use of IMSI Catchers would compromise the effectiveness of these investigative tools.[92]

To implement this secrecy the FBI has asserted its own authority over IMSI Catchers so as to retain control over information relating to their use by other state agencies. Devices which interact with radio spectrum must receive equipment authorizations from the Federal Communications Commission (FCC). The FCC provides such

---

[88] Stephanie K. Pell and Christopher Soghoian, (2014). "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 l of Law & Tech* 1, http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf, p 20 *et seq*.

[89] Jason Leopold. (2015). "DC Police, the FBI, and Their Secret Agreement to Hide Cell Phone Spying," *Vice News*, September 30, 2015, retrieved November 16, 2015, https://news.vice.com/article/dc-police-the-fbi-and-their-secret-agreement-to-hide-cell-phone-spying.

[90] Jason Leopold. (2015). "DC Police, the FBI, and Their Secret Agreement to Hide Cell Phone Spying," *Vice News*, September 30, 2015, retrieved November 16, 2015, https://news.vice.com/article/dc-police-the-fbi-and-their-secret-agreement-to-hide-cell-phone-spying.

[91] Stephanie K. Pell and Christopher Soghoian, (2014). "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 l of Law & Tech* 1, http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf, p 38.

[92] Bradley S Morrison, Chief, Tracking Technology Unit, Operational Technology Division, Federal Bureau of Investigation, Affidavit, sworn April 11, 2014, https://assets.documentcloud.org/documents/1208337/state-foia-affidavit-signed-04112014.pdf. Obtained by Ars Technica: Cyrus Farivar, 2015. "FBI Now Claims its Stingray NDA Means the Opposite of What it Says", May 15, 2015, *Ars Technia,* http://arstechnica.com/tech-policy/2015/05/fbi-now-claims-its-stingray-nda-means-the-opposite-of-what-it-says/.

authorizations to IMSI Catcher devices and, in doing so, requires authorized manufacturers of IMSI Catchers to notify the FBI whenever any other agency seeks to purchase an IMSI Catcher.[93] In addition, in order to protect federal interests, the FCC requires any law enforcement agency that makes use of such devices to coordinate such use with the FBI.[94] The FBI subsequently leverages this coordination role to place significant restrictions on other federal investigative agencies (such as the Internal Revenue Agency or the Secret Service)[95] as well as on state and municipal agencies' use of IMSI Catchers, including the following proviso:

> In order to ensure that such wireless collection equipment/technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including but not limited to: in press releases, in court documents, during judicial hearings, or during other public forums or proceedings.[96]

Identical language is found in comparable agreements between the FBI and other investigative organizations,[97] forming the rationales on which such organizations base their reluctance to disclose information pertaining to IMSI Catchers to the public in any forum.

The aforementioned agreements have operated to frustrate freedom of information requests and ultimately forced civil liberties organizations to sue the US government for IMSI Catcher-related documents.[98] The agreements have led law enforcement agencies

---

[93] United States Department of Justice, Federal Bureau of Investigation and Eerie County Sheriff's Office, "Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations", June 29, 2012, https://assets.documentcloud.org/documents/1727748/non-disclosure-agreement.pdf.

[94] Federal Communications Commission Chairman Tom Wheeler. (2015). Letter to Senator Bill Nelson," United States Government, April 13, 2015, retrieved January 11, 2016, https://apps.fcc.gov/edocs_public/attachmatch/DOC-333229A1.pdf.

[95] Julian Hattem. "IRS Confirms Use of Surveillance Tool", *The Hill*, October 27, 2015, http://thehill.com/policy/national-security/258209-irs-head-reassures-congress-about-use-of-phone-tracking-tech; Cyrus Farivar. (2015). "DHS now needs warrant for stingray use, but not when protecting president," *Ars Technica*, October 21, 2015, retrieved November 16, 2015, http://arstechnica.com/tech-policy/2015/10/dhs-now-needs-warrant-for-stingray-use-but-not-when-protecting-president/.

[96] Congressman F James Sensenbrenner, Jr & Congresswoman Sheila Jackson Lee, 2016. Correspondence to James B Comey, Director, Federal Bureau of Investigation, February 24, 2016, http://sensenbrenner.house.gov/uploadedfiles/stingray_technology_letter.pdf.

[97] United States Department of Justice, Federal Bureau of Investigation and Eerie County Sheriff's Office, "Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations", June 29, 2012, https://assets.documentcloud.org/documents/1727748/non-disclosure-agreement.pdf.

[98] Jason Leopold. (2015). "DC Police, the FBI, and Their Secret Agreement to Hide Cell Phone Spying," *Vice News*, September 30, 2015, retrieved November 16, 2015, https://news.vice.com/article/dc-police-the-fbi-and-their-secret-agreement-to-hide-cell-phone-spying; see also: *American Civil Liberties Union of Southern California v Anaheim Police Department*, Case No: 30-2015-0076141-CU-WM-CJC, Superior Court of California, County of Orange, Verified Petition for Peremptory Writ of Mandate, March 10, 2015, https://www.aclunc.org/sites/default/files/2015.03.10%20Verified%20Petition%20for%20Peremptory%20Writ%20of%20Mandate%20with%20Exhibits_0.pdf.

to withhold disclosure of these devices' use from courts and defence attorneys,[99] and even to invent informants in order to place information gained from IMSI Catchers on the record without publicly disclosing their use.[100] United States officials have gone so far as to drop important evidence[101] and enter into unfavourable plea agreements to prevent disclosure of IMSI Catcher use.[102] Entire cases have reportedly been dropped to avoid revealing the use of this technology.[103] However, as a result of ongoing efforts by American civil liberties groups and journalists, some details have emerged about the use of IMSI Catchers in the United States.[104]

These sustained efforts have culminated in the FCC creating a task force to examine how criminals or foreign intelligence agencies might use IMSI catchers[105] as well as more general examinations into how IMSI Catchers are used,[106] legislation and judicial decisions limiting IMSI Catcher use in multiple states and even municipalities,[107] a federal Department of Justice policy regulating their use by law enforcement agencies,[108] and a warranting requirement for the Department of

[99] Ellen Nakashima. (2015). "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.

[100] Maria Kayanan. (2014). "Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking," *American Civil Liberties Union*, June 19, 2014, retrieved November 16, 2015, https://www.aclu.org/blog/internal-police-emails-show-efforts-hide-use-cell-phone-tracking.

[101] Cyrus Farivar. (2014). "Prosecutors Drop Key Evidence at Trial to Avoid Explaining 'stingray' use", *Ars Technica*, November 18, 2014, retrieved December 2, 2015, http://arstechnica.com/tech-policy/2014/11/prosecutors-drop-key-evidence-at-trial-to-avoid-explaining-stingray-use/.

[102] Maria Kayanan. (2014). "Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking," *American Civil Liberties Union*, June 19, 2014, retrieved November 16, 2015, https://www.aclu.org/blog/internal-police-emails-show-efforts-hide-use-cell-phone-tracking; *In the Matter of the Application of the United States of America for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, https://www.unitedstatescourts.org/federal/ilnd/317964/.

[103] Cyrus Farivar. (2015). "FBI would rather prosecutors drop cases than disclose stingray details," *Ars Technica*, April 7, 2015, retrieved January 8, 2016, http://arstechnica.com/tech-policy/2015/04/fbi-would-rather-prosecutors-drop-cases-than-disclose-stingray-details/.

[104] For a discussion of the "known unknowns" and secrecy efforts by the United States government, see: Stephanie K. Pell and Christopher Soghoian, (2014). "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 l of Law & Tech* 1, http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf.

[105] Craig Timberg. (2014). "Fed to study illegal use of spy gear," *The Washington Post*, August 11, 2014, retrieved January 11, 2015, https://www.washingtonpost.com/news/the-switch/wp/2014/08/11/feds-to-study-illegal-use-of-spy-gear/.

[106] Federal Communications Commission Chairman Tom Wheeler. (2015). Letter to Senator Bill Nelson," United States Government, April 13, 2015, retrieved January 11, 2016, https://apps.fcc.gov/edocs_public/attachmatch/DOC-333229A1.pdf.

[107] Hanni Fakhoury. (2015). "Stingrays Go Mainstream: 2014 in Review," *Electronic Frontier Foundation*, January 2, 2015, retrieved November 16, 2015, https://www.eff.org/deeplinks/2015/01/2014-review-stingrays-go-mainstream; Cyrus Farivar. (2015). "California cops, want to use a stringray? Get a warrant, governor says," *Ars Technica*, October 8, 2015, retrieved November 16, 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, retrieved December 3, 2015, https://oaklandnorth.net/2015/11/19/alameda-county-becomes-first-in-state-to-regulate-cellphone-surveillance-tool/.

[108] Department of Justice. (2015). "Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators," United States Government, September 3, 2015, retrieved November 16, 2015, http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators.

Homeland Security's use of the devices.[109] We discuss the substantive requirements of some of these policies in **Section Three**. However for the purposes of this section it should be noted that the adoption of these policies greatly clarifies to the public the nature of IMSI Catcher use in the United States. Greater transparency measures, including reporting and individual notice requirements, which have been adopted by the German government, are also explored in **Section Three**.

B. IMSI Use in Canada: Many Questions, Few Official Responses

Efforts to pierce the veil of secrecy surrounding state agency use of IMSI Catchers in Canada have met with comparable resistance. More recently, some evidence of IMSI Catcher use has begun to emerge. In spite of these recent developments, however, it remains unknown how frequently evidence obtained by means of IMSI Catchers has been obtained, retained, or used unchallenged in criminal proceedings.

Update Box 1: The Long Road to Official Confirmation of Use

At the time that the majority of this report was written, government officials had yet to publicly and officially confirm IMSI Catcher use in Canada despite conclusive evidence of such use on the public record. This evidence (described in more detail below) included a lawsuit against Correctional Services Canada for deploying IMSI Catchers in a prison, launched by employees of that prison; newspaper reporting regarding two criminal trials (one in Ontario and one in Québec) where IMSI Catchers were known to be used and eventually challenged; and, eventually, the court record of one of these proceedings, with evidence of IMSI Catcher usage as reflected therein, including confirmation that the devices have been in use by the RCMP for over a decade.

In spite of all of this, public officials continued to refuse to officially confirm in public discussion any use of these devices. Agencies such as the Toronto Police Services Board (TPS) and, later, the Vancouver Police Department (VPD) initially implied that they have never used these devices, while maintaining in the context of freedom of information demands that they have no legal obligation to confirm or deny such use.

Eventually, some measure of official public confirmation has emerged from some state agencies. VPD has now acknowledged that they have made use of an IMSI Catcher (through collaboration with the RCMP, which retained control of the device) stating that its initial denial related to 'ownership' of a device, not to past use.[110] Additionally, Edmonton Police Service (EPS) initially confirmed that it has

[109] Cyrus Farivar. (2015). "DHS now needs warrant for stingray use, but not when protecting president," *Ars Technica*, October 21, 2015, retrieved November 16, 2015, http://arstechnica.com/tech-policy/2015/10/dhs-now-needs-warrant-for-stingray-use-but-not-when-protecting-president/.

[110] After initially refusing a Freedom of Information to confirm or deny whether it had possession or control over any records responsive to a Freedom of Information demand relating to IMSI Catchers (see: *In re: An Applicant and the Vancouver Police Department*, BC OIPC File No: F15-63155 & Public Body File No: 15-2106A, Information & Privacy Commissioner of British Columbia,: Intervention of OpenMedia, January 25, 2016, https://cippic.ca/uploads/BCOIPC_F15-63155_ReVPD-OM-Intervention.pdf. NOTE: the authors represented OpenMedia). Following the filing of written submissions from the initial requestor (Pivot Legal Society) and a number of interveners, VPD ultimately decided to respond to the request, indicating it had not records: Vancouver Police Department, Letter to Douglas C King, Pivot Legal Society, "Re: Your Access Request | IMEI Device / IMSI Catcher Records", May 25, 2016: https://cippic.ca/uploads/BCOIPC_F15-63155_ReVPD-VPD_Response.pdf: "As you noted in your Submission, since the filing of your complaint and review, information about

"used the device in the past during investigations" in response to queries from Motherboard (VICE), even indicating that it owned such a device.[111] However, EPS subsequently asserted that it did not own the device, while declining to confirm or deny whether it had 'borrowed' one from the RCMP.[112]

In response to similar queries, police agencies in Halifax, Calgary, Ottawa, Winnipeg and Montreal have maintained their refusal to confirm or deny any such usage.[113] TPS and the Ontario Ministry of the Attorney General similarly continue to refuse official confirmation, even following the release of court records indicating the use of an IMSI Cather in a comprehensive TPS investigation (albeit one where the RCMP were assisting).[114] This ongoing refusal to officially confirm usage in the face of documented instances (potentially motivated by non-disclosure agreements between policing agencies and IMSI Catcher device manufacturers)[115] continues to stall efforts for reasoned public debate on the appropriate use of these devices.

As of the publication of this document, there have been three publicly confirmed uses in Canada of devices believed to be IMSI Catchers. All confirmations emerged from judicial proceedings. The first involved a judicial review launched by employees of a correctional facility, challenging the warden's decision to deploy mobile interception devices believed to be IMSI Catchers.[116] The ongoing judicial review questions whether the deployment is justified given its high collateral impact on the privacy of non-prisoners, including correctional services employees, visitors to the facility, and passers-by who enter the IMSI Catcher's range.[117]

The second instance involved a criminal proceeding, wherein the Royal Canadian Mounted Police (RCMP) used an IMSI Catcher in the course of a criminal investigation into an organized crime-related murder. The secrecy surrounding the use of the

---

the device commonly referred to as an IMEI Device or IMSI Catcher has been accessed through court records in Canada and reported on by media organizations. In consideration of all the relevant circumstances, the Vancouver Police advises that it does not have this devices and does not hold records responsive to your access requests of July 23, 2015."

[111] Jordan Pearson, 2016, "Edmonton Police Admit to Owning Stingray Surveillance Device", August 11, 2016, *Motherboard (VICE)*, https://motherboard.vice.com/read/edmonton-police-admit-to-owning-stingray-surveillance-device.

[112] Jordan Pearson, 2016, "Edmonton Police Say They Didn't Mean it When They Said They Own a Stingray", August 12, 2016, *Motherboard (VICE)*, http://motherboard.vice.com/en_ca/read/edmonton-police-say-they-didnt-mean-it-when-they-said-they-own-a-stingray.

[113] Jordan Pearson, 2016, "Edmonton Police Admit to Owning Stingray Surveillance Device", August 11, 2016, *Motherboard (VICE)*, https://motherboard.vice.com/read/edmonton-police-admit-to-owning-stingray-surveillance-device.

[114] Colin Freeze, 2016. "Case Sheds Light on How Police in Toronto Use 'Stingray' Surveillance", May 17, 2016, *Globe and Mail*, http://www.theglobeandmail.com/news/national/case-involving-first-documented-use-of-stingray-technology-in-toronto-goes-to-trial/article30057813/.

[115] Matthew Braga, 2016. "New Documents Show How Canadian Cops Use Secret Phone Surveillance Technology", May 17, 2016, *VICE News*, https://news.vice.com/article/new-documents-show-how-canadian-cops-used-secret-phone-surveillance-technology.

[116] Colin Freeze and Matt Braga, (2016). "Surveillance Device Used in Prison Sets Off Police Probe", *The Globe and Mail*, March 14, 2016, retrieved March 15, 2016, http://www.theglobeandmail.com/news/national/opp-launch-criminal-probe-into-use-of-surveillance-device-in-federal- prison/article29240374/.

[117] Colin Freeze and Matt Braga, (2016). "Surveillance Device Used in Prison Sets Off Police Probe", *The Globe and Mail*, March 14, 2016, retrieved March 15, 2016, http://www.theglobeandmail.com/news/national/opp-launch-criminal-probe-into-use-of-surveillance-device-in-federal- prison/article29240374/.

device in question was challenged, leading the Québec Superior Court to appoint an *amicus curiae* and hold extensive hearings to determine whether the RCMP's claimed secrecy was justified or not.[118] As a result, the RCMP was ordered to disclose a range of information related to its use of IMSI Catchers and the capacity of the underlying devices. The decision was appealed to the Québec Court of Appeal, and ultimately discontinued as the RCMP was concerned it might be compelled to disclose additional information regarding its investigative techniques.[119] Through persistent efforts of investigative journalists, details from the record of this case entered the public domain and, eventually, the full record (with redactions) was made public.[120] A third instance involves a criminal trial before the Ontario Superior Court, ongoing at the time of this writing, where the use of IMSI Catchers (and secrecy surrounding said use) have similarly been challenged. Again, through the persistent efforts of journalists, some details of this trial (and the IMSI Catchers used therein) have emerged on the public record.[121]

More generally, journalist attempts to understand whether government agencies use IMSI Catchers have met with strong resistance and official public confirmation of IMSI Catcher use remains elusive in spite of a growing public record establishing such use. The RCMP has stated to the press that it "[does] not release information pertaining to capabilities/tools as that can have an impact on our investigations."[122] Parliamentary questions have produced similarly limited results. In January 2014, Charmaine Borg, a Member of Parliament, tabled a written question on the Order Paper asking all federal departments (including the RCMP, Canadian Security Intelligence Service (CSIS), and Canadian Border Services Agency (CBSA), which are most likely to make use of such

[118] As recounted in *R v Mirarchi*, 2016 QCCA 81, para 5-7 and first publicly disclosed in *Mirarchi v R*, 2012 QCCS 7087, paras 63-64. Colin Freeze, Matt Braga & Les Perreaux, "RCMP Fight to Keep Lid on High-Tech Investigation Tool", *The 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/. The IMSI Catcher in question is referred to as a « Mobile Device Identifier » ("Identification Dispositif Mobile").

[119] *Mirarchi v R*, 2016 QCCA 597; Colin Freeze, (2016). "Guilty Pleas End Risk of Revealing RCMP Surveillance Technology", March 30, 2016, *The Globe and Mail*, http://www.theglobeandmail.com/news/national/guilty-pleas-scuttle-hearing-that-risked-revealing-rcmp-surveillance-technology/article29430116/.

[120] Jordan Pearson, 2016. "The RCMP Surveilled Thousands of Innocent Canadians for a Decade", June 10, 2016, *Motherboard (VICE)*, https://motherboard.vice.com/read/the-rcmp-surveilled-thousands-of-innocent-canadians-for-a-decade; *R v Mirarchi*, File No 540-01-063428-141, Order of Mr Justice Michael Stober, November 18, 2015, Reasons accompanying Order, issued December 8, 2015, https://cippic.ca/uploads/R_v_Mirarchi-QCCS-18Nov2015.pdf.

[121] Colin Freeze, 2016. "Case Sheds Light on How Police in Toronto Use 'Stingray' Surveillance", May 17, 2016, *The Globe and Mail*, http://www.theglobeandmail.com/news/national/case-involving-first-documented-use-of-stingray-technology-in-toronto-goes-to-trial/article30057813/; Matthew Braga, 2016. "New Documents Show How Canadian Cops Use Secret Phone Surveillance Technology", May 17, 2016, *VICE News*, https://news.vice.com/article/new-documents-show-how-canadian-cops-used-secret-phone-surveillance-technology.

[122] Matthew Braga. (2014). "The covert cellphone tracking tech the RCMP and CSIS wont' talk about," *The Globe and Mail*, September 15, 2014, retrieved November 16, 2015, http://www.theglobeandmail.com/technology/digital-culture/the-covert-cellphone-tracking-tech-the-rcmp-and-csis-wont-talk-about/article20579947/.

devices) whether they had used IMSI Catchers. Responding March 2014, the RCMP did not disclose whether, and if so under what specific grounds, it does or could deploy IMSI Catchers. The organization informed MP Borg that:

> The RCMP uses technical solutions to track customers' usage of communications devices and services only when judicially authorized to do so and only in support of criminal investigations. Information about these solutions cannot be disclosed as it could reveal details that would compromise the RCMP's ability to conduct criminal investigations.[123]

The RCMP's response would suggest, at least, that if the agency is using IMSI Catchers, they rely on some form of prior judicial authorization to do so. Some more recent case law has suggested that the primary vehicle for obtaining IMSI Catcher authorization by the RCMP is through the use of the *Criminal Code*'s general warrant power,[124] although it remains unclear if this authorization is adequate, if lesser authorization is relied upon in some circumstances, and even whether IMSI Catcher deployment occurs at times without any authorization at all.

Update Box 2: Many Questions Still Unanswered

As noted in **Update Box 1**, some regional Canadian police agencies (namely VPD [Vancouver] and apparently EPS [Edmonton]) have now publically and officially confirmed past IMSI Catcher use (in coordination with the RCMP), while court files confirm that a special RCMP unit owns and has made use of such devices, at least once in partnership with TPS [Toronto police]. However, much remains unknown regarding the nature, scope and secrecy of IMSI Catcher usage.

No state agency has provided any details regarding how frequently these devices are deployed, in relation to how many investigations, or on how many individuals have been affected by their deployment to date. Nor is it known how many such devices are owned by Canadian agencies, a factor that can greatly affect the willingness of agencies to use these devices to achieve a wider range of investigative objectives. Court filings on one criminal case, now public, indicate high demand for the devices – in one investigation far outstripping the number of officers trained to use the device.[125] One RCMP officer also testified to having personally used an IMSI Catcher in over 30 different operations on over 50 different subjects.[126]

Qualitative data remains equally absent. The court cases where IMSI Catcher use has been confirmed both arose in the context of complex organized crime investigations. Use in these instances was

[123] Minister of Public Safety and Emergency Preparedness, Responses to MP Charmaine Borg's Q-234 Order Paper Questions, March 24, 2014, retrieved January 17, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/11/8555-412-234.pdf.

[124] *R v Mirarchi*, File No 540-01-063428-141, Order of Mr Justice Michael Stober, November 18, 2015, Reasons accompanying Order, issued December 8, 2015, https://cippic.ca/uploads/R_v_Mirarchi-QCCS-18Nov2015.pdf.

[125] Jordan Pearson, 2016. "The RCMP Surveilled Thousands of Innocent Canadians for a Decade", June 10, 2016, *Motherboard (VICE)*, https://motherboard.vice.com/read/the-rcmp-surveilled-thousands-of-innocent-canadians-for-a-decade.

[126] Jordan Pearson, 2016. "The RCMP Surveilled Thousands of Innocent Canadians for a Decade", June 10, 2016, *Motherboard (VICE)*, https://motherboard.vice.com/read/the-rcmp-surveilled-thousands-of-innocent-canadians-for-a-decade.

reportedly confined to the more limited functionality of an IMSI Catcher – identification of unknown devices in the possession of known persons and confirming the presence of known devices in connection with known persons.[127] Nothing, however, is yet known regarding the use of these devices to achieve other investigative objectives (such as real-world tracking or identification of anonymous individuals) which have animated the use of these devices by policing agencies in other jurisdictions.

Similarly, nothing is known about the use of these devices in other contexts. Are they used where less severe offences are at issue, as was eventually the case in other jurisdictions? Other than the RCMP, do any policing services own or operate these devices? It is known from yet another court case that Correction Services Canada attempted to deploy such IMSI Catchers at a Canadian prison, prior to facing a lawsuit from employees for the alleged unlawful nature of the deployment. Are any other agencies using these devices? Intelligence agencies such as CSIS and CSE have wide-ranging surveillance and information-sharing powers that might be used to justify broad deployment of IMSI Catchers. Even agencies such as Canada Revenue or Canadian Border Services might find a wide range of uses for the devices.[128] Finally, the breadth of secrecy conditions imposed by an NDA onto the RCMP remains unknown. In short, much remains unanswered.

In response to identical questions, CSIS also declined to confirm or deny use of IMSI Catchers, but was even more circumspect regarding what legal authorization would be operative if such devices were hypothetically used: "[for] reasons of national security and to protect CSIS' ability to collect intelligence and provide advice to Government, CSIS does not disclose details of its operations and tradecraft."[129] Unlike either the RCMP or CSIS, the CBSA did disclose information about its access to telecommunications data. The agency made 128 cell tower log requests between April 1, 2012, and March 31, 2013; as we discuss in **Section Three**, such requests might largely obviate the need to operate IMSI Catchers in some contexts as they can provide access to comparable data.[130] The Agency, when asked about its use of IMSI Catchers specifically, asserted that it did "not use tracking products, infiltration software or interception hardware."[131]

MP Borg's requests paralleled those included in public questions sent to Canadian telecommunications companies by Canadian academics and civil liberties organizations. The public letters asked the companies a number of questions, including questions relating to their knowledge concerning state agencies' use of IMSI

[127] *R v Mirarchi*, File No 540-01-063428-141, Order of Mr Justice Michael Stober, November 18, 2015, Reasons accompanying Order, issued December 8, 2015, https://cippic.ca/uploads/R_v_Mirarchi-QCCS-18Nov2015.pdf, para 10.

[128] Julian Hattem. "IRS Confirms Use of Surveillance Tool", *The Hill*, October 27, 2015, http://thehill.com/policy/national-security/258209-irs-head-reassures-congress-about-use-of-phone-tracking-tech.

[129] Minister of Public Safety and Emergency Preparedness, Responses to MP Charmaine Borg's Q-234 Order Paper Questions, March 24, 2014, retrieved January 17, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/11/8555-412-234.pdf.

[130] Minister of Public Safety and Emergency Preparedness, Responses to MP Charmaine Borg's Q-233 Order Paper Questions, March 24, 2014, retrieved January 17, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2014/03/8555-412-233.pdf.

[131] Minister of Public Safety and Emergency Preparedness, Responses to MP Charmaine Borg's Q-234 Order Paper Questions, March 24, 2014, retrieved January 17, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/11/8555-412-234.pdf.

Catchers.[132] The telecommunications companies did not reveal anything about the use of IMSI Catchers, though it is not entirely clear whether they would even have such knowledge, as one of the features of IMSI Catchers is that they can be deployed by law enforcement directly, without knowledge or assistance of network providers.[133]

Given agencies' unwillingness to respond to questions about their use of IMSI Catchers, various journalists and organizations have submitted freedom of information requests to federal and provincial agencies to force them to disclose documents about how the devices might be used or regulated. In all cases we are aware of, these requests have been refused by the agencies in question, forcing the requestors to appeal the refusals to federal and provincial information commissioners. This includes at least one appeal to the British Columbia Office of the Information and Privacy Commissioner concerning the Vancouver Police Department's (VPD) refusal to disclose information relating to IMSI Catchers.[134] VPD has rationalized its refusal on the basis that disclosing responsive records would be contrary to the public's interest.[135] A similar refusal, by the Toronto Police Services Board ("TPS"), was the object of a failed appeal to the Office of the Information and Privacy Commissioner of Ontario. While both TPS[136] and VPD[137] eventually confirmed on the public record that they do not make direct use of IMSI Catchers, ongoing questions remain regarding whether these agencies are able to make regular use of such devices through

[132] Christopher Parsons. (2014). "Towards Transparency in Canadian Telecommunications," *Citizen Lab*, January 22, 2014, November 16, 2014, https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/.

[133] Christopher Parsons. (2014). "The Murky State of Canadian Telecommunications Surveillance," *Citizen Lab*, March 6, 2014, retrieved November 16, 2014, https://citizenlab.org/2014/03/murky-state-canadian-telecommunications-surveillance.

[134] Vancouver Police Department. (2015). "Re: Records Access Request," Vancouver Police Department, September 11, 2015, retrieved December 3, 2015, http://d3n8a8pro7vhmx.cloudfront.net/pivotlegal/mailings/520/attachments/original/2015_09_11_VPD_-_Response_to_FOI_on_Stingray_Device.pdf?1447214666.

[135] David Christopher. (2015). "Is the Vancouver Police Department sweeping up your cell phone data?," *Open Media*, November 13, 2014, retrieved December 3, 2015, https://openmedia.ca/blog/vancouver-police-department-sweeping-your-cell-phone-data.

[136] Robin Levinson King, 2015, "The Cellphone Spyware the Police Don't Want to Acknowledge", December 15, 2015, *The Toronto Star*, https://www.thestar.com/news/canada/2015/12/15/the-cellphone-spyware-the-police-dont-want-to-acknowledge.html: "Following that ruling, Toronto police spokesperson Craig Brister told the Star that the force does not have a stingray. "I have made some inquiries and we do not use the Stingray technology and do not have one of the units," Brister said in an email."

[137] After initially refusing a Freedom of Information to confirm or deny whether it had possession or control over any records responsive to a Freedom of Information demand relating to IMSI Catchers (see: *In re: An Applicant and the Vancouver Police Department*, BC OIPC File No: F15-63155 & Public Body File No: 15-2106A, Information & Privacy Commissioner of British Columbia,: Intervention of OpenMedia, January 25, 2016, https://cippic.ca/uploads/BCOIPC_F15-63155_ReVPD-OM-Intervention.pdf. NOTE: the authors represented OpenMedia). Following the filing of written submissions from the initial requestor (Pivot Legal Society) and a number of interveners, VPD ultimately decided to respond to the request, indicating it had not records: Vancouver Police Department, Letter to Douglas C King, Pivot Legal Society, "Re: Your Access Request | IMEI Device / IMSI Catcher Records", May 25, 2016: https://cippic.ca/uploads/BCOIPC_F15-63155_ReVPD-VPD_Response.pdf: "As you noted in your Submission, since the filing of your complaint and review, information about the device commonly referred to as an IMEI Device or IMSI Catcher has been accessed through court records in Canada and reported on by media organizations. In consideration of all the relevant circumstances, the Vancouver Police advises that it does not have this devices and does not hold records responsive to your access requests of July 23, 2015."

collaboration with the RCMP.[138] The TPS refusal to disclose and subsequent appeal, however, remains instructive in highlighting weaknesses in justifications advanced by law enforcement agencies seeking to maintain secrecy surrounding IMSI Catcher use. The next sub-section explores this decision in greater detail.

C. Case Study: Anatomy of an IMSI Catcher Information Request Denial

An appeal from a Toronto Police Services Board (TPS) decision to refuse disclosing any information relating to TPS' use of IMSI Catchers was released in August of 2015.[139] TPS' rationale for refusal was premised on the claim that any disclosure:

> … could be used to enable suspects to circumvent the techniques and procedures put in place. It would assist in educating criminals on how to protect themselves against police surveillance, or even allow unauthorized persons to employ such techniques themselves; thus, spoiling its potential for effective use as an investigative tool.
>
> To require the police to disclose records affirming the use of electronic surveillance equipment would quickly lessen its effectiveness and, possibly jeopardize the safety of law enforcement officials operating such devices.[140]

Courts have acknowledged that this might be a problem in some contexts and have accepted a limited common law privilege protecting investigative techniques.[141] TPS' expansive premise, however, extends well beyond the scope of this protection so as to effectively insulate any and all surveillance tools from public knowledge, without any regard at all for the public interest in such information. Worse, its premise fails to balance any risk that revealing the availability of a particular surveillance tool might lead to its circumvention against the public's need to be able to challenge the legitimacy and use of such tools. Indeed, TPS does not even assess the risk that revealing the mere knowledge of a specific surveillance tool will undermine its use.

It is unclear how TPS and other agencies can defend such categorical statements without any reference or analysis of the underlying surveillance tool in question. These agencies' positions presume, in essence, that generalized knowledge of the very use of a surveillance tool will permit criminals to circumvent it. Such positions

---

[138] Indeed, such usage has since been confirmed for both policing agencies. An Ontario criminal case confirmed that an IMSI Catcher was used in a TPS organized crime investigation, whereas VPD later confirmed that they had used such a device in a suspected kidnapping case, under exigent circumstances that generated no written records. In both instances, the RCMP appears to have been involved in the operation of the device: (see **Update Box 1**).

[139] *Toronto Police Services Board (Re),* Order No MO-3236, [2015] OIPC No 168 (ON IPC), para 9.

[140] *Toronto Police Services Board (Re),* Order No MO-3236, [2015] OIPC No 168 (ON IPC), para 9.

[141] *Toronto Police Services Board (Re)*, Order No MO-3236, [2015] OIPC No 168 (ON IPC), para 9.

fundamentally disregard the nature of surveillance tools, the public policy implications of adopting such an expansive premise, and the law.

To avoid disclosing documents, TPS invoked the 'investigative techniques' exception. This is a harms based exception, meaning it only applies where an agency can demonstrate that actual harm will follow from the disclosure.[142] To invoke this exception in the context of investigative techniques police must provide grounds demonstrating that the risk (although not the actual harm) in question is probable, as opposed to speculative, by "providing evidence 'well beyond' or 'considerably above' a mere possibility of harm".[143] This is a relatively exacting standard because it requires demonstrating the presence of specific, "detailed and convincing" evidence demonstrating that disclosure "could reasonably be expected to hinder or compromise [the investigative tool's] effective utilization."[144] Adopting a blanket exception that categorically equates disclosure of "the use of any electronic surveillance devices" with "maintaining their effectiveness, and thus upholding the police's ability to continue to successfully carry out its policing mandate"[145] is antithetical to either of these approaches because it discards the need to demonstrate that knowledge of a particular surveillance tool will actually compromise its effectiveness and/or threaten personal safety.

Regrettably, the Adjudicator appears to have accepted TPS' broad framing of the 'investigative techniques' exception. The Adjudicator found that that the request "would by definition reveal the fact that the police have access to surveillance devices for intercepting mobile phone traffic and tracking the movements of mobile phone users."[146] This finding seems to simply flow, directly and without elaboration, from TPS' assertion that knowledge of "*any* electronic surveillance device" undermines its "effectiveness".[147]

Confirmation of state agencies' use of investigation and intelligence gathering tools does not inherently reduce their utility as surveillance techniques. Government agencies are required to report on the frequency at which they request and receive interception warrants, and such reporting has not diminished the investigative utility

---

[142] *Re: Ministry of Community Safety and Correctional Services*, Order PO-2751, [2009] OIPC No 4 (OIPC), para 89.

[143] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner),* [2014] 1 SCR 674, 2014 SCC 31, paras 48-54.

[144] *Re: Ministry of Community Safety and Correctional Services*, Order PO-2751, [2009] OIPC No 4 (ON IPC), para 97; *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31, para 48.

[145] *Toronto Police Services Board (Re)*, Order No MO-3236, [2015] OIPC No 168 (ON IPC), para 12.

[146] *Toronto Police Services Board (Re*), Order No MO-3236, [2015] OIPC No 168 (ON IPC), para 13.

[147] *Toronto Police Services Board (Re),* Order No MO-3236, [2015] OIPC No 168 (ON IPC), para 12.

of telecommunications interceptions. In the United States, network interception capacities are a matter of legislation as well as of detailed regulatory policies. These policies provide extensive details regarding the interception requirements and associated technical capabilities that network equipment must meet if service providers are to incorporate it into their networks.[148] Moreover, network equipment vendors provide detailed public information regarding the interception capabilities of such equipment.[149] It is, therefore, not unusual to have knowledge regarding specific surveillance equipment capabilities on the public record that has not, in the past, unduly undermined the utility of such equipment.[150]

Moreover, as noted above, reliance on the 'investigative techniques' exception requires the presentation of *specific facts* that harm would result in the *specific* situation at issue – a generalized risk is not sufficient.[151] The Adjudicator's decision only presents a generalized risk that knowledge of electronic surveillance tools will undermine their effectiveness in support of his finding "that knowledge of the existence of this investigative tool would enable those who are subject to an investigation to take steps to avoid detection or surveillance by the police."[152] No specific details are provided as to what specific risk the knowledge that TPS is using IMSI Catchers might pose or of how such knowledge might compromise the effectiveness of these surveillance tools.

---

[148] *In Re Communications Assistance for Law Enforcement Act and Broadband Access and Services*,, Second Report and Order and Memorandum Opinion and Order, (2006) FCC 06-56, https://apps.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf.

[149] Cisco. (2011). "Chapter 2 – Lawful Intercept and CALEA," Cisco, last revised March 24, 2011, retrieved December 3, 2015, http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/bts/5-0/feature/description/featdesc/fd5015li.html.

[150] *In the Matter of New York Civil Liberties Union, Petitioner, against Erie County Sheriff's Office*, 47 Misc.3d 1201(A), (2015) (Supreme Court of New York, Erie County): "Even if it was, its disclosure would not interfere with or prejudice a particular law enforcement investigation or criminal prosecution, nor would it identify a particular confidential source or disclose particular confidential information, nor would it reveal other than "routine" — which to the Court merely means somewhat regularly resorted to — "criminal investigative techniques".

[151] *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 should the information in question be released."

[152] *Toronto Police Services Board (Re),* Order No MO-3236, [2015] OIPC No 168 (ON IPC), para 14.

i. Confirming Use Will Not Compromise IMSI Catcher Utility

Putting aside the general over-breadth of TPS' justification – that knowledge of *any* surveillance tool would facilitate circumvention of that tool – its application to IMSI Catchers is particularly difficult to defend. The same argument was advanced by law enforcement agencies in the United States and ultimately rejected in early attempts to prevent disclosure of IMSI Catcher use.[153]

The Eerie County Sheriff's Office, for example, advanced this argument to try and avoid disclosure obligations under freedom of information laws.[154] A New York State court rejected this, finding there was "no reasonable basis for denying access" to IMSI Catcher related records as these records would only reveal "routine" or "regularly resorted to" investigative tools and will "not interfere with…any particular…investigation or…prosecution."[155] Other courts have similarly held that disclosing records confirming a given agency's use of IMSI Catchers, and even details of such use, would not compromise their effectiveness.[156] Indeed, it is difficult to imagine what specific "detailed and convincing" facts *could* be presented to demonstrate that disclosure of TPS' use of IMSI Catchers would undermine the effectiveness of the technique. Nor is there much prospect that personal safety could be threatened by revealing their use. Public disclosure of IMSI Catcher-related records can only risk compromising the effectiveness of these tools if it is likely to greatly improve the ability of individuals to detect or evade surveillance by means of IMSI Catchers. Yet this is unlikely to occur.

As discussed in **Section Three: B**, below, there are legal powers in the *Criminal Code* that expressly authorize law enforcement to access the type of information that could be

---

[153] Nathan Freed Wessler. (2014). "VICTORY: Judge Releases Information about Police Use of Stingray Cell Phone Trackers," *American Civil Liberties* Association, June 3, 2014, retrieved December 3, 2015, https://www.aclu.org/blog/victory-judge-releases-information-about-police-use-stingray-cell-phone-trackers.

[154] New York Civil Liberties Union. (2015). "Stingrays," *New York Civil Liberties Union*, last updated September 15, 2015, retrieved December 3, 2015, http://www.nyclu.org/stingrays. *In the Matter of New York Civil Liberties Union, Petitioner, against Erie County Sheriff's Office*, 47 Misc.3d 1201(A), (2015) (Supreme Court of New York, Erie County): "Even if it was, its disclosure would not interfere with or prejudice a particular law enforcement investigation or criminal prosecution, nor would it identify a particular confidential source or disclose particular confidential information, nor would it reveal other than "routine" — which to the Court merely means somewhat regularly resorted to — "criminal investigative techniques"". See also: *ACLU of Northern California v Department of Justice*, Docket No 13-cv-03127-MEJ, 2015 US Dist LEXIS 90672 (LexisNexis)(N Dist of California), p 19.

[155] New York Civil Liberties Union. (2015). "Stingrays," *New York Civil Liberties Union*, last updated September 15, 2015, retrieved December 3, 2015, http://www.nyclu.org/stingrays. *In the Matter of New York Civil Liberties Union, Petitioner, against Erie County Sheriff's Office*, 47 Misc.3d 1201(A), (2015) (Supreme Court of New York, Erie County): "Even if it was, its disclosure would not interfere with or prejudice a particular law enforcement investigation or criminal prosecution, nor would it identify a particular confidential source or disclose particular confidential information, nor would it reveal other than "routine" — which to the Court merely means somewhat regularly resorted to — "criminal investigative techniques"". See also: *ACLU of Northern California v Department of Justice*, Docket No 13-cv-03127-MEJ, 2015 US Dist LEXIS 90672 (LexisNexis)(N Dist of California), p 19.

[156] *ACLU of NC v Department of Justice*, (2014) 70 F.Supp.3d 1018, (N Dist California); *In Re Order Authorizing Prospective and Continuous Release of Cell Site Location Records*, 31 F.Supp.3d 889, (2014)(S Dist Texas), (sealed, obtained by Electronic Privacy Information Center (EPIC) Freedom of Information Act request. see: https://epic.org/foia/fbi/stingray/In-re-US-Application-06022012.pdf).

obtained by using IMSI Catchers. With the appropriate authorization, this information can be obtained directly from network providers in the form of a production order or through the authorized installation of a wiretapping device (e.g. an IMSI Catcher, number dialing recorder, or other interception device). As such, "the fact that the police have access to surveillance devices for intercepting mobile phone traffic and tracking the movements of mobile phone users"[157] is already a matter of public record that any individual is deemed to be aware of and there are only "a limited number of ways" in which such interception can occur.[158] If TPS (or any other Canadian law enforcement agencies) is making use of IMSI Catchers that fact "is not unexpected."[159]

As an IMSI Catcher essentially operates by mimicking a service provider's own equipment, "avoid[ing] detection or surveillance" by an IMSI Catcher entails the same obfuscation techniques as would be required to avoid detection by one's own network provider. Even use of encryption or a throwaway 'pay per use' mobile device would be revealed by records held by telecommunications carriers, and which are accessible to law enforcement with the proper authorization, as such devices interact with the providers' cell tower. As these data access powers are on the public record there is little further obfuscation that can result from knowledge that TPS might be using IMSI Catchers.[160]

Further, as recounted above, there is significant, detailed, and public information concerning how law enforcement agencies around the world use IMSI Catchers.[161] Any individual seeking to avoid surveillance would be negligent to disregard the possibility that Canadian law enforcement use such tools as well. Further, the rich public record regarding IMSI Catcher use includes comprehensive details regarding their capacities and limitations (for an overview, see **Section One**, above). As a District Court in the United States, where comparable state agencies make comparable uses of IMSI Catchers, found in 2015:

---

[157] *Toronto Police Services Board (Re)*, Order No MO-3236, [2015] OIPC No 168 (ON IPC), para 13.

[158] *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."

[159] *In Re Ministry of Justice*, Order F15-12, 2015 BCIPC 12, (BC IPC), https://www.oipc.bc.ca/orders/1768.

[160] *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.

[161] *ACLU of NC v Department of Justice*, (2014) 70 F.Supp.3d 1018, (N Dist California); *ACLU of Northern California v Department of Justice*, Docket No 13-cv-03127-MEJ, (N Dist of California), p 19.

> … the techniques and procedures relating to the use of cell site simulators [are] 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.[162]

Indeed, tools are available for individuals to detect the presence of IMSI Catchers[163] and there is a growing academic discourse surrounding the detection of IMSI Catchers.[164] It is difficult to imagine how officially confirming TPS' use of these devices could have affected the ongoing development of these detection tools. Moreover, an individual trying to avoid detection by an IMSI Catcher is limited in their options for doing so. While some encryption techniques might be deployed against IMSI Catchers operating in 'camping mode' (i.e. operating to capture voice or text communications), obfuscating a handset from an IMSI Catcher in 'identification mode' is difficult given that IMSI and IMEI numbers are transmitted without encryption.[165] Regardless, these obfuscation techniques are as widely known and publicly discussed as evolving IMSI Catcher detection mechanisms and their availability is not contingent upon confirmation that a particular agency is operating IMSI Catchers.[166]

---

[162] *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).

[163] 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)*, retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

[164] These include: Stephanie Pell & Christopher Soghoian, 2014. "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; Stephanie K. Pell and Christopher Soghoian, (2014). "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 l of Law & Tech* 1, http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf; 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), retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf; Luca Bongiorni. (2012). "iParanoid: A Mobile Cell Networks Intrusion Detection System," Bootcamp 2012 – University of Luxembourg, September 20, 2012, retrieved December 18, 2015, http://www.slideshare.net/iazza/mobile-cell-networksintrusiondetectionsystemiparanoidlucabongiorni; see also: Sean Gallagher. (2015). "This machine catches stingrays: Pwnie Express demos cellular threat detector," *Ars Technica*, April 20, 2015, retrieved December 18, 2015, http://arstechnica.com/information-technology/2015/04/this-machine-catches-stingrays-pwnie-express-demos-cellular-threat-detector/.

[165] Dan Goodin. (2015). "Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations," *Ars Technica*, October 28, 2015, retrieved December 3, 2015, http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/; 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)*, retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

[166] See **Section One**, above, and: *ACLU of NC v Department of Justice*, (2014) 70 F.Supp.3d 1018, (N Dist California), 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

It is notable that general knowledge of IMSI Catcher use has been a matter of public record for two decades in the United States. Even after more specific and significant details regarding the use and capacities of these devices, including explicit confirmation of their use by specific agencies, became a matter of public record, United States agencies continue to recognize the utility of these devices. In fact, in the wake of disclosures regarding the use of IMSI Catchers, several United States agencies have adopted detailed policies to govern future use. In this regard, even if disclosure of IMSI Catcher use could undermine the use of such tools *to some minor degree* the devices clearly continue to enjoy significant utility after knowledge of their use is made public. As the 'investigative techniques' exemption entails a risk assessment this ongoing utility must be accounted for in assessing whether the risk in question is sufficient to truly 'undermine or compromise' the investigative technique in question.[167] Yet neither TPS nor the adjudicator took account of this rich public record when refusing the freedom of information request in question.

Indeed, the Federal Communications Commission which, as noted above, is responsible for overseeing spectrum usage in the United States, requires IMSI Catcher vendors to register all IMSI Catcher devices prior to commercial sale or use by non-federal government agencies. The list of these devices is publicly available on the FCC's website, subject to minor redactions intended to protect trade secrets, as explained by FCC Chairman Tom Wheeler:

> Equipment certification is required to ensure that products that use radio spectrum comply with the Commission's technical rules. Certification is required before such a product can be imported or marketed in the United States, except that equipment marketed to or used solely by the federal government is not subject to the Commission's rules or certification. Placing conditions on the equipment certification is intended to ensure that use of such equipment is constrained to law enforcement. …
>
> Harris Corporation has applied for and been granted certification for several devices, all of which are posted on the Commission's web site. A list of the certified devices and the links to the grants of certification are attached. Portions of the applications are withheld from public inspection as permitted under the Commission's rules because they include trade secrets. Digital Receiver Technology, Inc. applied for and was granted certification

---

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."

[167] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31, para 66: "In striking a balance between those 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 probable harm. This finding was reasonable.", para 29; *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.

> for similar devices which are also included in the attached list. The same conditions are included on the grants of certification for these devices.[168]

Canadian agency claims that they cannot even acknowledge the existence of such devices without compromising their utility stands in direct contrast to the situation in the United States, as shown above.

It is true that public confirmation of IMSI Catcher use in the United States *has* led to judicial and policy constraints designed to temper their potential for excessive privacy intrusion. However, concern over the latter is not a valid basis for refusing information requests – quite to the contrary, where the information sought is an essential precursor to a public debate concerning the legitimacy of a government or law enforcement practice, the right to information is engaged even more strongly.[169] Worryingly, arguments to conceal the use of contemporary surveillance techniques, such as IMSI Catchers, appear at times more prominently linked to concerns over potential public outcry regarding the presence or operation of such tools and the potential for resulting regulation of their use. While there is no direct evidence that such concerns provide the underlying rationale for resisting IMSI Catcher-related right to information requests, such rationales are antithetical to freedom of information regimes, whose object is to facilitate the "public interest in open government, public debate and the proper functioning of government institutions."[170]

ii. Will Enter Public Record Through Discovery Process

The adjudicator also failed to account for the likelihood that IMSI Catcher use should, in time, be revealed in court as prosecutors rely on evidence gained by these devices to bring criminal charges against individuals. As a result, refusal to acknowledge IMSI Catcher use is at best a short term delay in disclosure of information that *should* eventually be on the public record in any resulting case. Rules of discovery accommodate some level of protection for investigative techniques that might be compromised if made public (partially encoded in section 37 of the *Canada Evidence Act*).[171] However, in the context of a trial, the threat of harm to such techniques must

---

[168] Federal Communications Commission Chairman Tom Wheeler, (2015). Letter to Senator Bill Nelson," United States Government, April 13, 2015, retrieved January 11, 2016, https://apps.fcc.gov/edocs_public/attachmatch/DOC-333229A1.pdf.

[169] *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23.

[170] *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.

[171] *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

be balanced against the defendant's right to make full answer and defence.[172] Additionally, while TPS (like its United States counterparts) may be bound by a non-disclosure agreement, such agreements do not supersede discovery obligations.[173] Moreover, the open court principle is engaged in judicial proceedings, meaning that police procedures placed on the record of a proceeding will be made public unless it poses a serious threat to police techniques – it is not sufficient to demonstrate that the 'effectiveness' of these techniques might be marginally undermined.[174]

With respect to discovery obligations and IMSI Catchers, at least some courts in the United States have already held that constitutional privacy protections should, or could, play a role in regulating the use of IMSI Catchers.[175] The same potential constitutional implications are likely to arise in Canada.[176] In addition, and as explained in the final section of this report, the authorization framework for IMSI Catcher use is both legally and constitutionally ambiguous. It is at least arguable, then, that law enforcement relied upon insufficient legal authorization as a basis for gathering evidence against a defendant by means of an IMSI Catcher. IMSI Catcher use could even amount to a violation of the *Criminal Code*'s Part VI authorization framework, which offers high protection to invasive wiretapping activities. If IMSI Catcher activity is deemed to fall within Part VI and law enforcement failed to seek appropriate Part VI authorization, any evidence obtained thereby may run afoul of sub-section 188(5) of the *Criminal Code*. Even ancillary details, such as the level of interference that resulted from a given IMSI Catcher deployment, its conditions of deployment, the number of affected 'non-targets', data retention policies – all of

---

(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).

[172] *R v Meuckon*, [1990] 57 CCC (3d) 193 (BCCA); *R v Richards*, [1997] 34 OR (3d) 244 (CA); *R v Lam*, 2000 BCCA 545

[173] *R v Toronto Star Newspaper Ltd*, [2005] 204 CCC (3d) 397 (ONSC) para 30.

[174] *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.

[175] See: *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div); *In Re Order Authorizing Prospective and Continuous Release of Cell Site Location Records*, 31 F.Supp.3d 889, (2014)(S Dist Texas), (sealed, obtained by Electronic Privacy Information Center (EPIC) Freedom of Information Act request. see: https://epic.org/foia/fbi/stingray/In-re-US-Application-06022012.pdf). *In the Matter of an Application for Cell Tower Records Under 18 USC 2703(d)*, 90 F.Supp.3d 673, (2015)(S Dist Texas, Houston Div), pp 12-13 (IMSI Catchers are more invasive than tower dump production orders); *In the Matter of New York Civil Liberties Union, Petitioner, against Erie County Sheriff's Office*, 47 Misc.3d 1201(A), (2015) (Supreme Court of New York, Erie County) ("Clearly, even apart from any concerns about the "dragnet" or general search capabilities of the device, its employment by law enforcement officers to acquire information of the foregoing type, even if not especially within the context of a specifically targeted criminal investigation, has implications under the Fourth Amendment…").

[176] See in particular *R v Rogers Communications*, 2016 ONSC 70.

these factors might affect the legality or constitutionality of a given employment.

Update Box 3: IMSI Catcher Details Emerge in Trial

As mentioned in **Update Box 1**, Québec Superior Court Justice Michael Stober has, in fact, ordered the disclosure of details relating to IMSI Catcher usage in the context of a criminal investigation where the devices were used. This disclosure order followed an extensive and heavily contested hearing on the nature and impact of the devices, with a court appointed *Amicus Curiae* present to ensure the impact of these capabilities was fully canvassed so that the court could properly determine whether to disclose details of IMSI Catcher usage or not.

The Québec court held that disclosure of the fact of use, as well as details of its usage and impact, while withholding some specific details regarding the technical capacities of the devices as it was viewed these specific details could be used to develop improved IMSI Catcher detection tools and techniques.[177] Much of these details entered the public record when the publication ban in place for the duration of the trial expired. The order to disclose additional details (including the manufacturer, make, model and practical range of the device) was appealed, however, and the appeal was discontinued upon settlement of the underlying criminal trial.[178]

Knowledge of IMSI Catcher use then becomes relevant to mounting of a fair defence, as the admissibility of that evidence could be challenged if obtained unconstitutionally or in violation of Part VI. A court cannot properly assess whether such constitutional or legal considerations exist if it is unaware of the nature, functionalities or usage of an IMSI Catcher, as noted by the Maryland Court of Special Appeals:

> To undertake the Fourth Amendment analysis and ascertain "the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security," it is self-evident that the court must understand why and *how* the search is to be conducted. The reasonableness of a search or seizure depends "on a balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers." The analytical framework requires analysis of the functionality of the surveillance device and the range of information potentially revealed by its use.[179]

Along the same lines, knowing that these devices were used in the course of an investigation would be integral to making full answer and defence to any charges that relied on the evidence gained from these devices. This, in turn, suggests a

[177] *R v Mirarchi*, File No 540-01-063428-141, Order of Mr Justice Michael Stober, November 18, 2015, Reasons accompanying Order, issued December 8, 2015, https://cippic.ca/uploads/R_v_Mirarchi-QCCS-18Nov2015.pdf.

[178] Colin Freeze, Matthew Braga & Les Perreaux, 2016. "RCMP Fight to Keep Lid on High-Tech Investigation Tool", March 13, 2016, *Globe and Mail*, http://www.theglobeandmail.com/news/national/rcmp-trying-to-keep-lid-on-high-tech-methods-used-to-fight-mafia/article29204759/.

[179] *Maryland v Andrews*, (2016) *Md App LEXIS 33, File No 1496 (Md Ct of Special Appeals), citations omitted.

heightened need for disclosure.[180]

Canadian courts have specifically held that information related to surveillance devices must be disclosed so as to enable a meaningful defence.[181] This does not necessarily mean that police must disclose the specific location that IMSI Catchers have been placed, the specific model or make that is being used, or details relating to installation techniques.[182] Even withholding of such information, however, has only been approved by courts where sufficient details are already available to assess the overall constitutionality of the technique in question.[183] For example, with respect to tracking devices, in *R v Gerrard* the Ontario Superior Court of Justice required disclosure of significant salient details regarding the tracking device in question, including details relating to the general nature of the device (GPS, in that instance, IMSI Catcher, here) and its installation (the vehicle it was installed in was surreptitiously removed to facilitate the installation), but not the specific make and model of the device or the place in which it was concealed in the vehicle, as the latter would add little to the defence while tipping off future objects of investigation on where to look for such devices.[184] Here, TPS refused to even acknowledge the use of IMSI Catchers and thus denying a basic level of detail needed to assess the constitutionality of the search.

In summary, if TPS had made lawful use of IMSI Catchers in the course of its duties, disclosure obligations are such that this usage *should* eventually have formed part of the public record in some criminal trial. From this perspective, for the purposes of assessing the risk of harm posed by FOI disclosure to investigative techniques, it should be deemed that the information will eventually enter the public domain. By extension, refusal to disclose *cannot* be said to preserve an investigative technique. It only delays an important public debate that should occur sooner, rather than later.

iii. No Consideration of the Public Interest

Finally, in upholding TPS' refusal to disclose any details relating to its hypothetical use of

---

[180] 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); and *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.

[181] *R v Gerrard*, [2003] OJ No 420 (ONSC), paras 39-40; *R v Guilbride*, 2003 BCPC 176, paras 1-3 and 40-42.

[182] *R v Richards*, [1997] 34 OR (3d) 244 (CA); *R v Lam*, 2000 BCCA 545; *R v Guilbride*, 2003 BCPC 176; *R v Gerrard*, [2003] OJ No 420 (ONSC).

[183] *R v Gerrard*, [2003] OJ No 420 (ONSC), para 39 ("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 affect the ability of the accused to make full answer and defence"); *R v Guilbride*, 2003 BCPC 176, para 41 ("the information…is, at best, of some very limited, peripheral and possible relevance…"); *R v Lam*, 2000 BCCA 545, paras 29, 42-44 (where evidence of the location of a surveillance post is sparse but relied upon heavily, its probative value is low). See also: Stephanie K. Pell and Christopher Soghoian, (2014). "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 l of Law & Tech* 1, http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf, pp 33-34.

[184] *R v Gerrard*, [2003] OJ No 420 (ONSC), paras 4, 39-40 and 45-46.

IMSI Catchers, the Adjudicator wholly failed to consider any countervailing public interest considerations.[185] In assessing whether the risk to investigative techniques is sufficient to justify refusal of the general right to information, that risk must be balanced against the public's interest in "open government, public debate and the proper functioning of government institutions."[186] This means that even where revealing details of a surveillance tool may undermine its efficiency to *some* degree, the risk may not be sufficiently probable to 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.[187] Where section 2(b) is engaged in this manner a government institution must exercise its discretion accordingly. The public interest may therefore justify disclosing requested information even where there is sufficient evidence to demonstrate it *is* sufficiently probable that disclosure will hinder the effective utilization of an investigative tool.[188] Yet neither the TPS (in rendering its decision to refuse disclosure) nor the Adjudicator (in assessing the validity of that decision) accounted for the public interest in evaluating whether the documents sought should be disclosed in spite of any risk to investigative techniques this might pose.[189]

In this instance, the actual risk that IMSI Catchers would be undermined if knowledge of their use is negligible or non-existent, as explained above. It is already known that police can intercept and track mobile devices, many details regarding IMSI Catcher capacities are on the public record, and any probative information obtained by

---

[185] The Information & Privacy Commissioner of Ontario, Brian Beamish, has since indicated that the decision does, in fact, appear to be deficient for its failure to consider the public interest: Robin Levinson King, 2015, "The Cellphone Spyware the Police Don't Want to Acknowledge", December 15, 2015, *The Toronto Star*, https://www.thestar.com/news/canada/2015/12/15/the-cellphone-spyware-the-police-dont-want-to-acknowledge.html.

[186] *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.

[187] *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 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.

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

[189] *R v Mentuck*, [2001] 3 SCR 442, 2001 SCC 76, para 38 (court is obligated to consider freedom of expression implications of refusing disclosure of investigative techniques to the public even where this is not explicitly raised by parties); *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23, paras 66, 73-74; *Toronto Police Services Board (Re*), Order No MO-3236, [2015] OIPC No 168 (ON IPC).

Canadian law enforcement from IMSI Catcher use should eventually be subject to disclosure obligations. Moreover, given the nature of IMSI Catchers and mobile devices, obfuscation is difficult even where it is known these devices are in use. On the other hand, the public interest in verifying whether Canadian agencies are using these devices is high. Underpinning this high public interest in disclosure is legitimate concern that IMSI Catcher use may not conform to the legal requirements.

Risk that Use Violates Privacy Impact Assessment Obligations

There is a reasonable risk that, if TPS were using IMSI Catchers, such use might be without obtaining the proper level of legal authorization, implicating the *Charter*. In addition, TPS IMSI Catcher use may not conform to a range of other legal obligations. For example, most government agencies are obligated to disclose the adoption of invasive surveillance tools to a privacy commissioner and carry out a privacy impact assessment to ensure that such tools are used appropriately. For federal agencies, this obligation is triggered wherever 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."[190] IMSI Catchers are an inherently intrusive surveillance tool, which is noted for its collateral impact on the privacy of non-targets (see **Box 3** on p 91, below). This means that, by definition, they collect significant amounts of personal information that is untargeted and therefore cannot be legitimately used in any decision-making process associated with the surveillance operation at hand. The privacy impact is significant (see **Box 2** on p 88, below). Moreover, all tracking technologies have potential for high invasiveness, which is why the International Working Group on Data Protection in Telecommunications recommends that private sector organizations conduct a privacy impact assessment prior to adopting any mobile location tracking technology.[191] Yet, when asked by reporters whether the RCMP uses IMSI Catchers, the Office of the Privacy Commissioner of Canada responded by stating that it had not been consulted about the use of such technology, indicating no such privacy impact assessment had occurred.[192]

---

[190] The obligation to carry out privacy impact assessments is made binding by a directive issued under paragraph 71(1)(d) of the *Privacy Act*, RSC 1985, c P-21: 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. Guidance on the implementation of this directive from the Office of the Privacy Commissioner of Canada indicates that it is engaged whenever a new or altered program entails the collateral collection of personal information: Office of the Privacy Commissioner of Canada. (2011). "Fact Sheets: Privacy Impact Assessments," Government of Canada, retrieved November 16, 2015, https://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp. Provincial privacy laws impose comparable obligations: 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.

[191] International Working Group on Data Protection in Telecommunications, "Working Paper on Location Tracking from Communications of Mobile Devices", (2015) 675.51.12, https://datenschutz-berlin.de/attachments/1161/WP_Location_Tracking_675.51.12.pdf, para 20.

[192] Matthew Braga. (2014). "The covert cellphone tracking tech the RCMP and CSIS wont' talk about," *The Globe and Mail*, September 15, 2014, retrieved November 16, 2015, http://www.theglobeandmail.com/technology/digital-culture/the-covert-cellphone-tracking-

Risk that Possession & Use Violates Radiocommunication Act

In addition, the *Radiocommunication Act*, RSC 1985, c R-2, prohibits the use of uncertified radio devices and radio interference-causing equipment in Canada, yet no devices have been certified for IMSI Catcher use in Canada.[193] While there are exceptions to the certification requirement, IMSI Catchers do not appear to meet these. Such devices are not, for example, "capable only of the reception of broadcasting" as they intercept signals that are not "intended for direct reception by the general public" but rather for an individual's service provider.[194]

IMSI Catchers are also not appropriately categorized as "jammers", which the RCMP is permitted to use without certification further to an exception issued by regulation in 2015.[195] At face value, the definition of 'jammer' appears sufficiently broad to include IMSI Catchers, as it includes:

> … any device or combination of devices that transmits, emits or radiates electromagnetic energy and that is designed to cause, causes or is capable of causing interference or obstruction to radiocommunication, other than a device or combination of devices for which standards have been established under paragraph 5(1)(d) or 6(1)(a) or for which a radio authorization has been issued.[196]

IMSI Catchers operating in identification mode are, in fact, capable of interfering with the normal operation of a mobile device – while a mobile devices is sending information to an IMSI Catcher, it will not receive signals from other cell towers, rendering it incapable of sending or receiving calls, SMS or data as it will not be able to interact with its network provider.[197] There has even been some evidence that IMSI Catchers operating in identification mode can frustrate important mobile device functionality, such as the ability to call 911 in an emergency.[198]

Ultimately, however, the regulatory exception applies to "jamming", which is defined as

---

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.'"

[193] *Radiocommunication Act*, RSC 1985, c R-2, section 4. Matthew 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/.

[194] *Radiocommunication Act*, RSC 1985, c R-2, section 2 "broadcasting" and paragraph 4(1)(b).

[195] Matthew Braga & 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/; *Radiocommunication Act (Subsection 4(4) and Paragraph 9(1)(b)) Exemption Order No 2015-1*, SOR/2015-36.

[196] *Radiocommunication Act*, RSC 1985, c R-2, section 2 "jammer".

[197] See **Section One**, above.

[198] Colin Freeze, 2016. "RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals", *The Globe and Mail*, April 18, 2016, http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memo-reveals/article29672075/.

signals interference *by emission*. This is evident from the definition of a 'jammer', which is a device that emits signals that are capable of interfering with radiocommunication, and is a subset of all "interference-causing equipment", defined to include "any device ... that causes or is capable of causing interference to radiocommunication", whether by signals emission or otherwise.[199] Other jurisdictions similarly define 'jammers' as devices that block radiocommunication by emission, not functionality. For example, the United States Federal Communications Commission's Enforcement Bureau describes the devices as follows:

> Generally, "jammers" — which are also commonly called signal blockers, GPS jammers, cell phone jammers, text blockers, etc. — are illegal radio frequency transmitters that are designed to block, jam, or otherwise interfere with authorized radio communications.
>
> .... Jamming technology generally does not discriminate between desirable and undesirable communications. A jammer can block all radio communications on any device that operates on radio frequencies within its range (i.e., within a certain radius of the jammer) by emitting radio frequency waves that prevent the targeted device from establishing or maintaining a connection.[200]

By contrast, IMSI Catcher interference occurs by functionality, not by emission. The signals emitted by IMSI Catchers do not jam or saturate mobile frequencies in a manner that interferes with the operation of a mobile device – they operate on the basis of accepted mobile data transmission protocols.[201] Instead, the functional content of the signals tricks a mobile device into believing that it is already communicating with a mobile tower so that it ignores other signals and only interacts with the IMSI Catcher.[202] While some IMSI Catchers are equipped with a distinct frequency 'jammer' that saturates mobile frequencies in order to force mobile devices within range to interconnect more rapidly with the IMSI Catcher, this jamming capability is distinct and severable from the IMSI Catcher's core functionality.[203] Overall, an IMSI Catcher's

---

[199] *Radiocommunication Act*, RSC 1985, c R-2, section 2, "interference-causing equipment". An interpretation of "jamming device" that is not limited to interference by emission would effectively conflate "jamming device" with "interference-causing equipment", yet the Act treats each independently, with distinct obligations applying to each.

[200] Federal Communications Commission Enforcement Bureau, "GPS, Wifi, and Cell Phone Jammers: Frequently Asked Questions," https://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf.

[201] See description in **Section One: B**, above.

[202] See description in **Section One: B**, above. This interference will only occur if the IMSI Catcher is operating in 'identification mode'. If it is acting in 'camping mode' (that is, if it is operating as a conduit between engaged mobile devices and the mobile network) then there should not be any interference.

[203] See description in **Section One: B**, above. 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), retrieved November 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

capacity to interfere with mobile communications does not arise from frequency interference but from its removal of mobile devices from interacting with the broader mobile communications network.

Update Box 4: Skirting (or Ignoring?) the *Radiocommunication Act*?

As noted in **Update Box 1**, two regional policing services (VPD [Vancouver] and EPS [Edmonton]) have now confirmed that they have used IMSI Catchers, while court records confirm the use of these devices by a third (TPS [Toronto]). It is also clear from court records that the RCMP uses the devices. It is not yet clear on what basis this can occur in the clear absence of certification for any such devices under the Canadian *Radiocommunication Act*.

One theory suggests that the RCMP believes it is using these devices under an exception to the general certification requirement which permits the RCMP to use 'jamming device' for specific purposes. This report argues that the exception would not apply to IMSI Catchers as they do not meet the definition of a 'jamming device'. Even if they did meet this definition, however, the regulation was only enacted in 2015, whereas RCMP use of IMSI Catchers demonstrably predates its introduction by close to a decade. Moreover, the regulation only applies to the RCMP, meaning that other policing agencies could not rely on it. It is possible that other policing agencies are merely 'borrowing' these devices, or using them in joint investigations, and examples from VPD and TPS appear to confirm this arrangement. In such instances, RCMP officers would have to maintain control over the devices at all times, as the 'jammer' exception only exempts RCMP employees and specifically obligates these employees to "at all times prevent access to it by a person who is not exempt."

One officer's claim seemingly implies that limiting the operation of these devices to "restricted ranges and in short bursts" can in some manner avoid the certification obligations imposed on radio devices such as IMSI Catchers by the *Radiocommunications Act*.[204] As the certification obligations are not limited in application to use of such devices, extending to the possession, manufacturing, importation, distribution, lease, sale or offer to sell of any radio device or radio-interference causing device such as an IMSI Catcher, restricting usage could not somehow avoid the certification obligations.[205] More likely, these use limitations refer to obligations imposed onto the use of 'jamming devices' by the RCMP regulatory exemption, which obligates use of such devices to undertake "[e]very reasonable effort...to restrict the jammer's interference with or obstruction of radiocommunications to the smallest physical area, the fewest number of frequencies, the appropriate power level and the minimum duration required to accomplish the intended purpose".[206]

The exception granted to the RCMP regarding the use of jamming devices thus should not authorize the department's use of IMSI Catchers.[207] Moreover, the exception is

[204] Colin Freeze, 2016. "Case Sheds Light on How Police in Toronto Use 'Stingray' Surveillance", May 17, 2016, *Globe and Mail*, http://www.theglobeandmail.com/news/national/case-involving-first-documented-use-of-stingray-technology-in-toronto-goes-to-trial/article30057813/.

[205] *Radiocommunication Act*, RSC 1985, c R-2, sub-sections 4(1)-(2).

[206] *Radiocommunication Act (Subsection 4(4) and Paragraph 9(1)(b)) Exemption Order No 2015-1*, SOR/2015-36, sub-section 3(2).

[207] *R v Mirarchi*, 2016 QCCA 81, para 6, ("These disclosure requests dealt with the investigation techniques the police used that led to the charges against the respondents, and in particular the methods that were used to intercept and decode PIN to PIN Blackberry communications, as well as the means used to identify the cell phone devices in question.")(appeal discontinued, 2016 QCCA 597). Colin Freeze, 2016. "Guilty Pleas End Risk of Revealing RCMP Surveillance Technology", *The Globe and Mail*, March 30, 2016,

only available to the RCMP, and not to any other state agencies such as regional policing services, or Correctional Services Canada,[208] and expressly obligates any RCMP officer possessing a jammer to "at all times prevent access to it by a person who is not exempt" and not to any other state agencies such as regional policing services, or Correctional Services Canada.[209] It is therefore unclear to what extent the 'jamming' exception can be relied upon to justify use of IMSI Catchers by TPS specifically (or other local policing agencies more generally) and, as no such devices have been certified under the *Radiocommunications Act*, their use would likely be in violation.

Confusing Authorization Framework Raises Risk of Disproportionate Use

Additionally, questions remain regarding the appropriate framework for legal authorization of IMSI Catcher use, as well as the appropriate scope of that use. Without confirmation of Canadian agencies' use of such devices, however, there is no opportunity to ensure that the appropriate framework for their use is adopted. Moreover, examples of use from abroad (summarized above) imply that state agencies seeking to use IMSI Catchers will not always proactively disclose the more privacy invasive nature of such devices to the courts when seeking legal authorization for their operation.[210] One Canadian agency has already been shown to operate IMSI Catchers without any authorization, leading to a criminal investigation into the legality of the agency's action.[211] Similarly, Canadian policing agencies will occasionally frame cell-site record requests in over-broad terms. In one recent investigation (of a single crime), law enforcement requested service providers to provide cell-site records relating to over 40,000 individuals.[212] The two Canadian service providers through which the request was mediated noticed it was the broadest request they had seen to date, and were able to successfully challenge this overbreadth in court.[213] However, IMSI Catchers are self-deployed which lets their operators, such as government agencies, bypass the possibility

---

http://www.theglobeandmail.com/news/national/guilty-pleas-scuttle-hearing-that-risked-revealing-rcmp-surveillance-technology/article29430116/.

[208] Matthew Braga and Colin Freeze, "Agencies Did Not Get Federal Authorization to use Surveillance Devices", *The Globe and Mail*, March 21, 2016, retrieved March 22, 2016, http://www.theglobeandmail.com/news/national/agencies-did-not-get-federal-authorization-to-use-surveillance-devices/article29322700/.

[209] *Radiocommunication Act (Subsection 4(4) and Paragraph 9(1)(b)) Exemption Order No 2015-1*, SOR/2015-36: The exception only applies to "employees of the Royal Canadian Mounted Police who are required, as part of their duties or training, to install, use, possess, manufacture or import a jammer…" (section 2) and any employee "who possesses a jammer must … (b) at all times prevent access to it by a person who is not exempt from the application of subsection 4(4) of the Act." (section 6).

[210] 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/; *US v Rigmaiden*, (2012) 844 F.Supp.2d 982 (Dist of Arizona).

[211] Matthew Braga and Colin Freeze, "Agencies Did Not Get Federal Authorization to use Surveillance Devices", *The Globe and Mail*, March 21, 2016, retrieved March 22, 2016, http://www.theglobeandmail.com/news/national/agencies-did-not-get-federal-authorization-to-use-surveillance-devices/article29322700/

[212] *R v Rogers Communications Partnership*, 2014 ONSC 3853, para 12.

[213] *R v Rogers Communications*, 2016 ONSC 70.

of any comparable challenge by service providers.[214] Publicly confirming the use of such devices would at minimum allow for a discussion of that use in a context where such use is highly insulated.[215]

A related concern is that ongoing IMSI Catcher secrecy will undermine trial fairness. As outlined above, discovery rules likely compel the state to disclose information necessary for defendants to challenge the legality and *Charter* compliance of IMSI Catcher use, as well as the admissibility of any evidence obtained by means of inappropriate IMSI Catcher deployment. However, there is no guarantee that the state will respect such discovery obligations and proactively disclose IMSI Catcher use. Indeed, the experience from the United States suggests that government agencies might undertake expansive measures to avoid doing so proactively, and defence counsel may not know to ask.[216] Moreover, hypothetical claims of general police IMSI Catcher use may be insufficient to raise the prospect of discovery shortcomings in order to convince a court to compel disclosure.[217] However specific knowledge that an agency such as TPS uses the devices might provide the legal basis for such a challenge. It is all the more important, then, that credible information regarding IMSI Catcher use in Canada enter the public domain sooner rather than later because public disclosure may facilitate trial fairness.

---

[214] *In the Matter of an Application for Cell Tower Records Under 18 USC 2703(d)*, 90 F.Supp.3d 673, (2015)(S Dist Texas, Houston Div), pp12-13 (IMSI Catchers are more invasive than tower dump production orders because device is deployed by law enforcement directly, not the provider; information obtained is transmitted in real time directly to law enforcement; the device allows continuous real-time tracking). See also: Stephanie Pell & Christopher Soghoian, 2014. "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.

[215] *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16, pars 84-86: "In those exceptional cases in which prior authorization is not essential to a reasonable search, additional safeguards may be necessary, in order to help ensure that the extraordinary power is not being abused. Challenges to the authorizations at trial provide some safeguards, but are not adequate as they will only address instances in which charges are laid and pursued to trial. … In our view, Parliament has failed to provide adequate safeguards to address the issue of accountability in relation to s. 184.4. Unless a criminal prosecution results, the targets of the wiretapping may never learn of the interceptions and will be unable to challenge police use of this power. There is no other measure in the Code to ensure specific oversight of the use of s. 184.4. For s. 8 purposes, bearing in mind that s 184.4 allows for the highly intrusive interception of private communications without prior judicial authorization, we see that as a fatal defect. In its present form, the provision fails to meet the minimum constitutional standards of s. 8 of the Charter."

[216] Stephanie K. Pell and Christopher Soghoian, 2014. "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 l of Law & Tech* 1, http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf, pp 35-37; 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.: "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."

[217] *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."

Where, as here, there are legitimate and feasible questions relating to whether state agencies are making appropriate use of investigative techniques, it is all the more important that information relating to such techniques are made public so as to facilitate debate. This public interest is protected by section 2(b) of the *Charter*, 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.[218]

In this context, examples of police conduct from abroad establish the basis and legitimacy for such questions, as do broader ambiguities relating to the appropriate legal framework for authorizing IMSI Catcher use. Section 2(b) is additionally engaged where individuals are prevented from collecting information necessary for expressive debate that "is directly related to [a] *Charter* protected right".[219] In this instance, important public debates – even the meaningful exercise – of the right to be free from unreasonable search and seizure are impeded by the Government's refusal to detail, or even confirm, its use of IMSI Catchers.[220]

It is therefore critical that such information relating to such use be made public so that the lack of such information does not impede important public debates from proceeding in more than a hypothetical manner.[221] As the next section highlights, transparency regarding the use of IMSI Catchers in other jurisdictions has led to the imposition of important and specific safeguards. Similarly, the next section examines significant ambiguities in the legal framework that might be used by Canadian state agencies to justify IMSI Catcher use. These ambiguities might well lead to insufficient privacy safeguards.

---

[218] *R v Mentuck*, [2001] 3 SCR 442, 2001 SCC 76, para 51.

[219] *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 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.

[220] *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16, pars 84-86.

[221] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner),* [2014] 1 SCR 674, 2014 SCC 31, para 66.

Section Three: Regulating IMSI Catcher Use

Despite considerable attention from civil liberties groups, journalists, academics, and politicians there is little known about the frequency or efficacy of IMSI Catcher surveillance practices. There is, however, some information concerning their regulation by law and policy in the United States and Germany, as well as some recent information regarding the conditions under which such devices are deployed in the United States. These will be explored in the first sub-section, below.

There is no equivalent public documentation that explains how IMSI Catchers could be lawfully used in Canada. The Canadian legal framework offers a number of potentially overlapping powers that might be relied upon by state agencies seeking to deploy IMSI Catchers, each with different safeguards and protections. These will be explored below, with the strengths, weaknesses and potential applicability of each to IMSI Catcher use assessed. However, this alone does not explain which of varying options state agencies will use in different investigative circumstances. The final segment of this section, then, explores what minimum standards the *Charter* might impose on the use of these devices.

A. Lessons from Abroad: Regulation in Other Jurisdiction

Governments in the United States and Germany have established laws and policies which limit how state agencies can lawfully use IMSI Catchers. Courts in the United States have imposed additional restrictions.

In the United States, a Department of Justice policy ("DOJ Policy") adopted in 2015 imposes a number of safeguards and establishes limits on how law enforcement agencies can use IMSI Catchers in the context of criminal investigations. The policy imposes accountability and use controls by:

- mandating internal supervision of their use;
- limiting their use to identification purposes and thus ruling out functionality associated with 'camping mode'. This limitation follows from the DOJ's assertion that IMSI Catchers "must be configured as pen registers and may not be used to collect the contents of any communication";[222]
- obligating the adoption, in any court order sought, of some safeguards for non-targeted information incidentally collected by them and;
- requiring probable cause warrants as a precondition to using IMSI Catchers in

[222] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download, p 2.

non-emergency or -exceptional circumstances.[223]

This last requirement is particularly meaningful because the United States government has historically operated IMSI Catchers under ambiguous legal footing. While conceding that such devices implicated constitutional protections 'in some instances', the Department of Justice's (DOJ) earlier formal policies treated IMSI Catchers as pen registers or trap and trace devices.[224] Such devices have historically operated in the United States with no constitutional, and minimal legal, constraint. They have done so under the presumption that such devices do not infringe on reasonable expectations of privacy because they only capture metadata used by phone companies for routing purposes and do not capture the 'content' of communications like a wiretap does.[225]

Pen/Trap devices, which capture dialing, routing or signaling information associated with a communication, but not the content of the communication itself, are regulated primarily by the *Pen Register Statute*, codified at 18 USC 3121 *et seq.*[226] Historically, the United States government treated IMSI Catchers as pen/trap devices in many, if not most, instances, only conceding the need for more rigorous authorization in rare instances, such as where deployment would intentionally reach into 'private spaces'.[227] Use of this more rigorous authorization appears to have been the exception rather than the rule; prior to the 2015 DOJ Policy, the DOJ's guidance expressly noted that pen/trap authority was sufficient for using any device that obtained unique device identifiers, including where such devices were used for tracking purposes.[228] Indeed, while

---

[223] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download.

[224] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download. This has been the case since the passage of the USA PATRIOT Act, which expanded the definition of Trap and Trace Devices to include all signals. For a comprehensive overview of the Department of Justice's historical treatment of IMSI Catchers, see: Stephanie K. Pell and Christopher Soghoian, 2014. "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, generally and specifically pp 20-27.

[225] *In re Application for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, (1995) 885 F.Supp 197 (Central Dist, California), for example. However, US jurisprudence on the issue of metadata protection has significantly evolved since that decision.

[226] *Pen Registers and Trap and Trace Devices*, codified at 18 USC 3121 *et seq*. Defined in 18 USC 3127 (4) See: https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206.

[227] Chuck Grassley. (2014). "Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program," United States Senate, December 31, 2014, retrieved November 16, 2015, http://www.grassley.senate.gov/news/news-releases/leahy-grassley-press-administration-use-cell-phone-tracking-program; Stephanie K. Pell and Christopher Soghoian, (2014). "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 l of Law & Tech* 1, http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf, pp 31-33.

[228] Stephanie K. Pell and Christopher Soghoian, 2014. "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, footnote 132.

adopting more rigid protections, the 2015 DOJ Policy continues to assert that pen/trap authority remains 'appropriate', as a matter of legal imperative, even while imposing stricter conditions as a matter of policy.[229] There is a measure of irony in this persistent DOJ stance insofar as there are no publicly available US court decisions that have positively affirmed the use of pen/trap authority as a basis for IMSI Catcher deployment.[230] While it appears that many courts *have* authorized IMSI Catcher use on the basis of pen/trap authorization such authorizations were issued without knowledge of the nature of the device being used or its capacities.[231] (As explained below, since the issuance of the DOJ Policy some courts have explicitly rejected pen/trap authorization as an adequate basis for IMSI Catcher use.)

The implication of this historical reliance on pen/trace authority is that IMSI Catchers are likely to have been frequently deployed without adequate safeguards, as the pen/trace regime provides only minimal protections. The statute typically permits interceptions wherever the evidence sought is likely to be relevant to an ongoing criminal investigation – a lower standard than the constitutional minimum which requires proof of 'articulable facts' or 'probable cause' that an anticipated privacy invasion will yield evidence of an offence.[232] Moreover, judges presented with law enforcement pen/trap authorization requests play a largely administrative role; they include minimal discretion to refuse such requests if the formal requirements of the statute are met.[233] Some have

---

[229] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download, p 3.

[230] As is thoroughly reviewed in: Stephanie Pell & Christopher Soghoian, 2014. "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. See: *In re Application for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, (1995) 885 F.Supp 197 (Central Dist California)(pre-amendment pen/trap statute authority only available where interception device is 'attached' to a telephone line. Authorization would also not be available because phone or other identifying number of target devices not known); *In re Application for an Order Authorizing Installation and use of a Pen Register and Trap and Trace Device (In re Stingray)*, (2012) WL 2120492, 890 F.Supp.2d, (South Dist Texas)(Pen/Trap authority to deploy IMSI Catcher in order to discover a known suspect's telephone number denied because authorization only available where court is provided with "a telephone number or some similar identifier" of the targeted device); *US v Rigmaiden*, (2012) 844 F.Supp.2d 982 (Dist of Arizona)(government does not concede reasonable expectation of privacy, but relied on probable cause based warrant in addition to pen/trace order, which would be sufficient had there been a reasonable expectation of privacy); *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div)(government obtains probable cause warrant to justify use of IMSI Catcher).

[231] Stephanie K. Pell and Christopher Soghoian, 2014. "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; Hanni Fakhoury, "When a Secretive Stingray Cell Phone Tracking ' Warrant' Isn't a Warrant", *Eff.org*, March 28, 2013, https://www.eff.org/deeplinks/2013/03/when-stingray-warrant-isnt-warrant, with respect to comparable obscurity but in the context of a full search warrant authorization for deployment of an IMSI Catcher.

[232] *Tracey v State*, 152 So 3d 504, (2014) (Supreme Court of Florida), See: http://www.floridasupremecourt.org/decisions/2014/sc11-2254.pdf; *In re: Application for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, (2010) 620 F.3d 304 (3rd Circuit); *In re: Application for Historical Cell Site Data*, (2013) 724 F.3d 600 (5th Circuit).

[233] See *US v Hallmark*, (1990) 911 F.2d 399, (10th Circuit)("the extremely limited judicial review required by [the pen/trace authorization regime] is intended merely to safeguard against purely random use of this device by ensuring compliance with statutory requirements…"); and discussion in: *In re: Application for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, (2010) 620 F.3d 304 (3rd Circuit)(stored communications act provides judges with discretion whether to

even suggested that a court cannot assess whether the information provided meets the 'relevancy' requirement when reviewing an application for pen/trace authorization and must instead accept any self-certification to that effect made by the officer seeking the order at face value.[234] Finally, the statute offers few remedies for violations and, notably, there is no evidence exclusion provision. As some US courts have held that evidence suppression is not available under the pen/trap regime,[235] it is unclear whether any remedy would be available at all if, for example, state agencies deployed an IMSI Catcher without any pen/trap authorization at all under the mistaken conclusion that emergency circumstances justified such deployment.[236]

To some degree, the DOJ Policy mitigates these shortcomings by requiring a 'probable grounds' based search warrant while retaining many of the procedural safeguards present in the pen/trap regime.[237] However, there are ongoing concerns relating to available remedies. For example, if in a given instance law enforcement agencies ignore the policy and decline to seek a search warrant it is unclear what remedy is available in the absence of a clear constitutional violation.[238]

Similar to DOJ, the United States Department of Homeland Security (DHS) published a policy ("DHS Policy") directive for using cell-site simulators on October 19, 2015. As

---

issue order even if statutory conditions are met, but pen/trap regime does not) but see contra: *In re: Application for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, (2010) 620 F.3d 304 (3rd Circuit); *In re: Application for Historical Cell Site Data*, (2013) 724 F.3d 600 (5th Circuit).

[234] See: *In re United States*, (1993) 10 F.3d 931 (2nd Circuit)(a general description of the pen/trap authorization regime includes the following statement: "The provision was not intended to require independent judicial review of relevance; rather, the reviewing court need only verify the completeness of the certification"); but also see: *US v Hallmark*, (1990) 911 F.2d 399, (10th Circuit)(but see also FN 3 "we express no opinion as to whether the court may…inquire into the government's factual basis for believing pen…trace information to be relevant to a criminal investigation"). Some state pen register statutes explicitly require a court to independently confirm that the 'relevance' standard has been met prior to issuing a pen/trap authorization. See for example: *US v Wilford*, (2013) 961 F.Supp.2d 740 (District of Maryland); (Louisiana pen register statute requires certification of relevance, as well as "recital of facts or information" constituting basis for that conclusion. FN3: "This requirement…differs from its federal counterpart"); *State v Fakler*, (1993) 503 N.W.2d 783 (Supreme Court of Minnesota).

[235] See for example *US v Forrester*, (2007) 512 F.3d 500 (9th Circuit), pp 512-513.

[236] Such occurrences are not unlikely. For example, a report issued by the Office of the Inspector General of the FBI on the agency's use of National Security Letters (NSL) to acquire account identifiers associated with customers from various service providers (including predominantly telecommunications providers) found a high incidence of unreported possible violations of the underlying statutory regime (22% of a random selection of files examined) and, also, the use of emergency procedures to bypass the NSL authorization regime in non-emergency circumstances: United States, Department of Justice, Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of National Security Letters", March 2007, https://oig.justice.gov/special/s0703b/final.pdf, pp 85-86 (unreported possible violations), 96-99 (misuse of emergency powers).

[237] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download, p 3, ("as a matter of policy, law enforcement agencies must now obtain a search warrant supported by probably cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure … As a practical matter … prosecutors will need to seek authority pursuant to Rule 41 *and* the Pen Register Statute" emphasis in original).

[238] *US v Forrester*, (2007) 512 F.3d 500 (9th Circuit)(suppression is not available as a remedy for violations of the pen/trap regime); *US v Stefanson*, (1981) 648 F.2d 1231 (9th Circuit)("unless a clear constitutional violation occurs, noncompliance with Rule 41 requires suppression of evidence only where…" the violation results in prejudice or the disregard was intentional or deliberate).

with the DOJ Policy, the DHS Policy acknowledges that IMSI Catchers had historically been deployed without a search warrant or probable cause further to the *Pen Register Statute*, at 18 USC 3121 *et seq*.[239] Moreover, the DHS Policy maintains the constitutionality of this historical approach just like the DOJ policy, but holds that moving forward IMSI Catcher deployment will only occur if a probable cause-based warrant is first obtained.[240] It also retains safeguards already in the *Pen Register Statute* in relation to trap and trace devices, prohibits the retention of collaterally captured IMSI/IMSE identifiers, and limits IMSI Catcher use to identification mode. Limiting collection to identification mode prevents the use of IMSI Catchers to obtain "emails, texts, contact lists" or any other content stored on or transmitted from a device.[241] Finally, any use of IMSI Catchers on aircraft "must be approved either by the executive-level point of contact for the jurisdiction … or by a branch or unit chief at the agency's headquarters."[242] DHS Officers must notify the court about how IMSI Catchers generally operate, that they might interfere with mobile service proximate to the devices, and how data not associated with the targeted phone will be deleted. Policies are also set to address how data is collected and disposed of post-collection.

A central weakness in both the DOJ Policy and the DHS Policy is their adoption of a questionably broad definition of exceptional situations capable of justifying deviation from its search warrant requirement. The policies derive their definition of such exceptional circumstances from the more permissive *Pen Register Statute* as opposed to the more protective constitutional standard of exigent circumstances.[243] This creates more latitude for IMSI Catcher use without any court supervision, a concern given the invasive capacity of these devices.

---

[239] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p. 4.

[240] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p. 4.

[241] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, pp 2-3 and 7. See also 18 USC 3127(3). .

[242] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p 3.

[243] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, pp 3-4.

In addition to these federal policies which are designed to curb the potential excesses of IMSI Catcher use, some states and even municipalities have adopted further restrictions.[244] As more becomes known regarding IMSI Catchers in the United States, US Courts have begun to impose restrictions on their use. A Maryland appellate court, for example, has found that deploying an IMSI Catcher in identification mode always implicates the Fourth Amendment and must therefore generally be premised on probable cause and subject to prior authorization.[245] And the US District Court for the Northern District of Illinois recognized that "a process must be created to reasonably ensure that innocent third parties' information collected by the use of a cell-site simulator is not retained by the United States or any government body."[246] The court imposed three minimization obligations to further this objective:

- agencies must make reasonable and demonstrable efforts to minimize the capture of non-targeted individuals when deploying IMSI Catchers by localizing the IMSI Catcher more closely around the targeted individuals, where possible, and by refraining from deploying IMSI Catchers where significant numbers of innocent people will be present alongside the specific target(s) in question;
- all data captured by an IMSI Catcher other than data identifying the mobile device used by the target of the deployment must be destroyed "immediately" and, regardless, no less than within 48 hours of capture. This destruction must be explicitly verified to the Court that authorized use of the IMSI Catcher; and
- a categorical prohibition on any law enforcement use of data acquired from use of an IMSI Catcher beyond what is necessary to identify and isolate the mobile phone information of the target.[247]

In explaining its rationale for imposing these conditions, the Illinois court noted that "[a] cell-site simulator is simply too powerful of a device to be used and the information captured by it too vast to allow its use without specific authorization from a fully informed court."[248] While the decision in question did not directly address whether IMSI Catcher use implicated US Fourth Amendment constitutional protections, as this was conceded by the government, it did hold that imposing these minimization obligations "reasonably balances the competing interests of effective

[244] Alameda County District. (2015). "Alameda County District Attorney's Policy for Use of Cell-Site Simulator Technology (Draft)," *Alameda County,* November 17, 2015, retrieved December 3, 2015, http://www.alcoda.org/files/DA_Stingray_Policy_Final_11102015.pdf. The Alameda County Board of Supervisors passed this policy on November 17, 2015.

[245] *Maryland v Andrews*, (2016) *Md App LEXIS 33, File No 1496 (Md Ct of Special Appeals). See also: *United States v Lambis*, (2016) 1:15-cr-00734-WHP, 2016 US Dist LEXIS 90085 (Sth Dist NY).

[246] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

[247] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

[248] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

law enforcement and people's Fourth Amendment privacy interests."[249]

In Germany, IMSI Catchers have been explicitly regulated by federal law since 2002, when their use was authorized in the wake of the 9/11 attacks in the United States.[250] Section 100i of the German Code of Criminal Procedure (*Strafprozessordnung*, StPO)[251] lets German courts authorize law enforcement agencies' deployment of IMSI Catchers only where there are grounds indicating that a specific serious crime has been or is going to be committed by an individual, and only to the extent necessary to determine that individual's mobile device identifier or whereabouts (sub-sections 100i (1), (3) and 100a (3)). The law includes additional safeguards, including:

- the obligation to limit collection of third party data to what cannot be technically avoided in capturing the targeted IMSI;
- a categorical prohibition on using any third party data incidentally captured for any reason other than to confirm it is, indeed, an untargeted third party; and
- the obligation to delete such incidentally captured third party data without delay (sub-section 101i (2)).[252]

In addition, targeted individuals must be notified that an IMSI Catcher has been used as soon as it is possible to do so without endangering the purposes of the investigation or the life, physical integrity, significant assets or personal liberty of another (section 101). This is another key safeguard. Given the surreptitious nature of IMSI Catchers, individuals who have been spied on will only be aware of this spying if criminal charges are brought against them or the government is statutorily required to notify individuals their devices and communications have been monitored. German law demands that individuals who are not notified of the surveillance in a court proceeding could press challenges about the use of an IMSI Catcher. The German regime stands in contrast to jurisdictions which lack notification requirements; in such jurisdictions innocent people whose device information is spied upon will never know of the surveillance and, thus never be able to challenge the legitimacy of the surveillance. Another German law imposes a reporting obligation on intelligence agencies, which must report on IMSI Catcher use to the Parliamentary Control Panel.[253] This Panel,

---

[249] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

[250] Daehyun Strobel, (2007). "IMSI Catcher", July 13, 2007, http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf.

[251] *Criminal Procedure Code (Strafprozessordnung)*(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, section 100i.

[252] *Criminal Procedure Code (Strafprozessordnung)*(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf.

[253] Aidan Wills & Mathias Vermeulen, (2011). "Parliamentary Oversight of Security and Intelligence Agencies in the European Union," European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2011, PE 453.207,

subsequently, reports to the Bundestag.

In aggregate, the information now provided by US federal agencies as well as provided in Germany for over a decade clarify how, exactly, IMSI Catchers are regulated by some of the agencies that utilize them. In the American case, however, there are no requirements to publicly report on the regularity at which the devices are used or the numbers of persons affected, and no notification is provided to individuals monitored by IMSI Catchers save through court proceedings. Canada's regulatory situation concerning IMSI Catchers is worse than either Germany or the United States; though there is now evidence that Canadian agencies are using IMSI Catchers, there are few corresponding details on the regulations that constrain how the devices are utilized.

B. Canada's Ambiguous Electronic Surveillance Framework

The Canadian *Criminal Code* offers no explicit authorization framework for IMSI Catchers of the type found in its German counterpart. However, the *Criminal Code* does contain a patchwork of overlapping electronic surveillance powers that could potentially apply to IMSI Catcher use, each with varying levels of safeguards. It remains ambiguous what element of this electronic surveillance framework would apply to IMSI Catcher use, a question which is explored in this sub-section.

For many decades, the *Criminal Code*'s electronic surveillance framework centred primarily on its Part VI prohibition on the interception of private communications. In the early 1990s, a number of judicial decisions established the need for prior judicial authorization as a constitutional necessity for a range of electronic surveillance techniques.[254] The resulting framework included specific powers for tracking devices (section 492.1), telephone number dialing recorders (section 492.2), consensual wiretapping (184.2) and video surveillance (487.01(4)).[255] In addition, in recognition that future electronic surveillance techniques will likewise require some form of authorization, a general warrant power was introduced that could be relied upon to authorize "use of any device or investigative technique or procedure or do any thing described in the warrant" (section 487.01).[256] These powers were updated in 2015 by

---

http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf.

[254] *R v Wise*, [1992] 1 SCR 527 (prior judicial authorization required for tracking vehicles in public by electronic means); *R v Wong*, [1990] 3 SCR 36 (prior judicial authorization required for video surveillance); *R v Fegan*, [1993] 13 OR (3d) 88, (CA), para 33 (implied that prior judicial authorization might be required where a digital number recorder is installed at the behest of a state agency, as opposed to a private company).

[255] See summary in *R v Noseworthy*, [1997] 33 OR (3d) 641 (CA); *R v Edwards*, 2014 ONSC 6323, para 25.

[256] *Criminal Code*, RSC 1985, c C-46, section 487.01.

Bill C-13, *Protecting Canadians from Online Crime Act*),[257] and supplemented with a number of production powers to compel the disclosure of various types of digital data from third party service providers. This overall electronic surveillance framework offers a number of options that might be used to authorize use of IMSI Catchers.

Update Box 5: Vehicle of Authorization?

As described in **Update Box 3**, court records from a criminal case in Québec where the use of an IMSI Catcher was challenged have emerged on the public record. These court records have revealed that the RCMP in that case relied on the use of a general warrant (assessed in more detail in **sub-section ii**, below) as a means of authorizing their use of an IMSI Catcher.[258]

Unfortunately, this does not resolve ongoing ambiguity relating to the authorization framework of these devices. The case in question involved the use of many more traditional surveillance mechanisms including wiretaps, which already require law enforcement to meet rigorous authorization obligations. Under such conditions state agencies might not challenge the need for a general warrant, as obtaining one would add minimally to the existing process. However, the use of a general warrant in one case is not confirmation that the state views such authorization as mandatory, nor does it prevent state agencies from using lesser authorization in future instances or under differing circumstances. Indeed, one officer's affidavit in a second organized crime case indicates his belief that IMSI Catchers do not implicate any reasonable expectation of privacy, implying that the *Charter* does not require police to obtain any judicial authorization at all before using these devices.[259]

Further confusing matters, the case in question occurred prior to the adoption (by the coming into force of Bill C-13 in 2015) of comprehensive amendments to the *Criminal Code*'s metadata and tracking recorder provisions described in **Table 1**. Subsequent to these amendments, the RCMP may now view these new powers as more a more appropriate vehicle for IMSI Catcher authorization (discussed in the next sub-section). The Québec decision also revealed RCMP usage of IMSI Catchers in non-investigative circumstances where a general warrant would not be available, as no criminal offence had been committed (this includes 'testing' of the devices and their use in order to locate a missing person). It is not clear what, if any, authorization was sought in these circumstances, or what targeting and minimization safeguards were in place.

One option arises from the *Criminal Code*'s metadata interception mechanisms, which are comprised of a tracking interception power and a transmission data interception power (comprising sections 492.1 and 492.1 as updated by Bill C-13). Another option can be found in Part VI of the *Criminal Code*, which regulates interception of private communications and may apply to at least some IMSI Catcher use. Finally, it is possible

[257] Bill C-13: Protecting Canadians from Online Crime Act. (2014). First reading November 20, 2013, royal assent December 9, 2014. Parliament of Canada. See: http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&Bill=C13&Parl=41&Ses=2.

[258] *R v Mirarchi*, File No 540-01-063428-141, Order of Mr Justice Michael Stober, November 18, 2015, Reasons accompanying Order, issued December 8, 2015, https://cippic.ca/uploads/R_v_Mirarchi-QCCS-18Nov2015.pdf.

[259] Colin Freeze, 2016. "Case Sheds Light on How Police in Toronto Use 'Stingray' Surveillance", May 17, 2016, *Globe and Mail*, http://www.theglobeandmail.com/news/national/case-involving-first-documented-use-of-stingray-technology-in-toronto-goes-to-trial/article30057813/: Excerpts of [Toronto Police Detective Shingo] Tanabe's sworn 'information to obtain' ... said he did not know of any "reasonable expectation of privacy" that would attach itself to identifying data broadcast by mobile phones..."

that Canadian state agencies might rely on the *Criminal Code*'s general warrant provision, available as an authorization mechanism of final resort, if no other criminal code authorization powers exist. This sub-section explores the availability and implications of each of these options, while the following sub-section examines what minimal requirements are imposed on IMSI Catcher use by the *Charter*.

i. Conflicting *Criminal Code* provisions for metadata acquisition

The *Criminal Code* provides two categories of electronic surveillance powers (updated for digital information by Bill C-13, *Protecting Canadians from Online Crime Act*)[260] that create a framework for metadata acquisition. Metadata is information 'about' a communication that is not the content of the communication itself. It can be used to identify or geolocate the origin or destination of a communication. The information obtained by IMSI Catchers can, in some contexts, be classified as metadata making the *Criminal Code*'s metadata authorization framework relevant to this analysis.

The first category of metadata interception recognized by the *Criminal Code* relates to the broader collection of information that is released by a mobile device to mobile base stations for the purpose of facilitating the routing of digital interactions, defined by the *Criminal Code* as 'transmission data'. The second category relates to the interception of 'tracking data', which is defined as information that can locate either an individual or a thing. This tracking power is further sub-divided into tracking associated with an individual and tracking associated with an object such as a vehicle. These respective powers and their distinct features are summarized in **Table 1**:

Type of Authorization	***Grounds to Issue***	***Target of Authorization***
Object Tracking 492.1(1)	Suspicion privacy invasion will assist in investigation of an offence	Data that can help locate a transaction or thing that is not closely associated with an individual, such as a car
Individual Tracking 492.1(2)	Belief privacy invasion will assist in investigation of an offence	Data that can help locate an individual or a thing that is usually carried or worn by an individual
Transmission Data 492.2	Suspicion privacy invasion will assist in investigation of an offence	Data that is transmitted for the purpose of identifying a device in order to facilitate telecommunications

Table 1: Authorizing IMSI Catchers as Metadata or Tracking Recorders

[260] Bill C-13: Protecting Canadians from Online Crime Act. (2014). First reading November 20, 2013, royal assent December 9, 2014. Parliament of Canada. See: http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&Bill=C13&Parl=41&Ses=2.

IMSI Catchers exploit mechanisms that are integral components of the mobile communications routing protocols in order to induce the transmission of data that identifies and locates devices. As such, both of these powers are potentially implicated in IMSI Catcher use, and their potential application is explored below. At the outset, it should be noted at the outset that Bill C-13 recently amended both of these powers with the intention of channeling activities aimed at tracking the location of individuals into the more protective 'Individual Tracking' power. IMSI Catcher use that undermines this ability would similarly undermine this legislative intent.

Mobile Digital Identifiers as Transmission Data?

Further to section 492.2 of the *Criminal Code*, law enforcement may seek authorization to deploy a 'transmission data recorder' (historically referred to as a 'dialing number recorder') in order to obtain 'transmission data', defined as:

> *transmission data* means data that
>
> (a) relates to the telecommunication functions of dialing, routing, addressing or signaling;
>
> (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
>
> (c) does not reveal the substance, meaning or purpose of the communication.
>
> *transmission data recorder* means a device, including a computer program within the meaning of subsection 342.1(2), that may be used to obtain or record transmission data or to transmit it by a means of telecommunication.[261]

This provision applies to data that is transmitted for the purpose of facilitating communications. Assessing its application to IMSI Catcher use requires an analysis of the key identifiers intercepted by IMSI Catchers – the IMSI, IMEI and, to a lesser extent, the MSISDN.

Transmission of the International Mobile Subscriber Identity (IMSI) number is integral

[261] *Criminal Code*, RSC 1985, c C-46, sub-section 492.2 (6), "Transmission Data".

to the general GSM mobile communication process.[262] However, the IMSI numbers' primary function is to "obtain[] information on the use of the GSM network by subscribers for individual charging purposes"[263] and *not* to "identify, activate or configure a device" (paragraph (b)). Teleologically, the IMSI number is for identifying subscribers, not devices, and to facilitate subscriber management functions such as billing and ensuring customers only access subscribed services; the number is not for routing.[264] Indeed, routing of calls to a mobile device can occur *without* use of the IMSI in situations where customer-to-service provider or billing relations are not a factor, such as where an emergency call is made.[265] The IMSI is not even *unique* to a given device, as it is housed in the SIM card, which can follow a subscriber from mobile phone to mobile phone, and even to other devices such as laptops. It can, however, only be associated with a single mobile device at one time, barring an illegal technique called SIM cloning, by which an attacker copies a target's IMSI and installs it on another device.[266] SIM cloning allows the attacker to then make phone calls that will be charged to the target's subscriber account. However, in some instances (where the attacker's and target's devices are both within the same cell location area), SIM cloning will affect routing and the attacker will also be able to receive communications sent to the target.

Courts have held that information used by providers for the purpose of identifying their subscribers (as opposed to identifying the devices that they use) and for managing the customer relationship is not 'transmission data' as defined by section 492.2:

> Subscriber Information relates to non-technical issues. It relates to the information which the telecommunication company needs for the purpose of facilitating billing and collection of fees arising from use of the cell phone network or for other

[262] See Fabian van den Broek, 2010. "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.1.2: "Note that the IMSI is not equal to the Mobile Subscriber ISDN Number (MSISDN), the phone number belonging to this SIM. Both numbers are created independently and linked to each other in the HLR (section 2.3.3). However the IMSI is the identifier in the GSM system for an MS and it belongs uniquely to a single SIM. [sic] while a new MSISDN can be linked to the IMSI." See also, European Telecommunication Standard Institute (ETSI), 2000. "Digital Cellular Telecommunications System (Phase 2): International Mobile Station Equipment Identities (IMEI)", November 2000, ETS 300 508/3GPP 02.16 v4.7.1, "an MS [mobile device] can only be operated if a valid "International Mobile Subscriber Identity" (IMSI) is present."

[263] ETSI, 2000. "Digital Cellular Telecommunications System (Phase 2): International Mobile Station Equipment Identities (IMEI)", November 2000, ETS 300 508/3GPP 02.16 v4.7.1: "As described in specification GSM 02.17, an MS can only be operated if a valid "International Mobile Subscriber Identity" (IMSI) is present. An IMSI is primarily intended for obtaining information on the use of the GSM network by subscribers for individual charging purposes."

[264] Fabian van den Broek, 2010. "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.3.3 "GSM services that the subscriber is allowed to access."

[265] ETSI, 2000. "Digital Cellular Telecommunications System (Phase 2): International Mobile Station Equipment Identities (IMEI)", November 2000, ETS 300 508/3GPP 02.16 v4.7.1: "Emergency calls can in some PLMNs be made without having to send the subscriber identity (IMSI) to the network. In this case the misuse of MS equipments after placing invalid emergency calls can be restrained by using the equipment identity."

[266] Christopher Beam, 2007. "How Do You Intercept a Text Message?", *Slate*, March 7, 2007, http://www.slate.com/articles/technology/technology/2007/03/how_do_you_intercept_a_text_message.html.

> services provided. This is a business function which is quite distinct from the technical matters relating to the transmission of data.[267]

The IMSI is distinct from some other types of subscriber identification information, as it is transmitted digitally between mobile devices and service providers and has technical and functional dimensions that govern its transmission.[268] However, like other customer data, the IMSI identifies subscribers, not devices, and is not "generated during the creation, transmission or reception of a communication" (paragraph b). It may therefore fall outside the definition of 'transmission data'.[269]

By contrast to the IMSI, the second key digital identifier sometimes obtainable by IMSI Catchers, the International Mobile station Equipment Identity (IMEI) number is inherently designed to uniquely identify a mobile *device* (the 'mobile station' i.e. mobile phone) as opposed to a subscriber, meeting the criteria in paragraph (b). However, it is arguable that the IMEI does *not* "relate to the telecommunication functions of dialing, routing, addressing or signaling" as required by paragraph (a). The IMEI is used to identify mobile devices to a network so that these can be checked against 'blacklists' of stolen or incompatible devices so that these can be blocked from access.[270] It is also used to identify devices that are incompatible with a given network.[271] While paragraph (a) employs a looser correlation ("relate to") than paragraph (b) ("is transmitted to…"), the identification of stolen devices is not closely related to the functional activity of routing.[272] The identification of device types that are blacklisted

---

[267] *Criminal Code (Can.)(Re)*, 2015 ABPC 178, para 30. See also: *Transmission Data Recorder Warrant (Re)*, 2015 ONSC 3072, para 7; *R v TELUS Communications Co*, 2015 ONSC 3226, paras 52-53: Finally, TELUS says that the assistance order should not be interpreted as permitting the police to obtain the subscriber information because Parliament did not include such information within the confines of the TDRW authorization. Specifically, Parliament did not include subscriber information in the definition of transmission data and, therefore, it can be taken that Parliament did not intend that subscriber information would be obtained through a TDRW. Once again, I do not agree with TELUS' position on this point. I fully understand why subscriber information would not have been included in the definition of transmission data. It has nothing to do with transmission data. Indeed, it would have been a strange result to draft a definition of transmission data that included the name and address of either the sender or receiver of that data. One only has to look at the existing definition of transmission data to see how subscriber information would not fit comfortably into such a definition."

[268] *Criminal Code (Can.)(Re)*, 2015 ABPC 178, paras 29-30: "It is apparent that Sub-paragraphs (a) and (b) of the definition deals only with scientific and technological concepts which relate to telecommunication 'functions'. Subscriber Information relates to non-technical issues. It relates to the information which the telecommunication company needs for the purpose of facilitating billing and collection of fees arising from use of the cell phone network or for other services provided. This is a business function which is quite distinct from the technical matters relating to the transmission of data."

[269] By contrast, the Temporary Mobile Subscriber Identity (TMSI) number, described in greater length in **Section One: B**, above, *is* "generated" as part of the communication process and,

[270] Fabian van den Broek, 2010. "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.3.6. See also: "Besides the IMSI, the implementation of IMEI is found necessary in order to obtain knowledge about the presence of specific mobile station equipment in the network, disregarding whatever subscribers are making use of these equipments. The main objective is to be able to take measures against the use of stolen equipment or against equipment of which the use in the GSM system can not or no longer be tolerated for technical reasons."

[271] *Ibid*.

[272] *Criminal Code (Can.)(Re)*, 2015 ABPC 178, paras 29-30.

for compatibility purposes is more closely related to the general purpose of 'routing', the function of the IMEI is to identify categories of devices in order to determine whether network access should be granted, not to identify specific devices for the purpose of functional routing. By contrast, 'transmission data' such as an IP address or telephone number is typically integral to the actual function of routing – it determines where a device is or actively changes its configuration. The IMEI might not fit the definition of 'transmission data' either, then, rendering s 492.2 unavailable as authorization for its interception.

A final identifier that can be obtained by means of an IMSI Catcher, the Mobile Station ISDN ('MSISDN' or 'phone number') *is* designed for technical 'routing' purposes as well as to identify the Mobile Station (commonly known as the mobile device or phone), meeting the criteria of paragraphs (a) and (b). However, while many IMSI Catchers are able to intercept the telephone number associated with a particular mobile device as a means of identifying that device, it is the IMSI and IMEI that are typically used to do so.[273] This is because, as described in **Section One** above, while an IMSI Catcher can induce transmission of the IMSI and IMEI with relative ease, identifiers such as the MSISDN require more intrusive interactions to obtain. While the MSISDN might therefore qualify as 'transmission data', it is rarely the immediate object of an IMSI Catcher deployment.

A final central mobile identifier that is used for routing purposes is the Temporary Mobile Subscriber Identity number (TMSI). The TMSI is transmitted frequently between the mobile device and the tower and is used to locate the mobile device to process incoming calls. This identifier, however, is ephemeral and hence of minimal utility as means of tracking a mobile device or identifying the individual subscriber associated with it (see **Section One: B**, above).

Moreover, even if some digital identifiers might meet the definition of 'transmission data', the availability of section 492.2 as a basis for IMSI Catcher authorization remains in question. For one thing, the *Criminal Code*'s wiretapping regime may apply to IMSI Catchers and, in particular, to such devices when they are deployed to intercept data for the purpose of identifying telecommunications subscribers. The argument, as elaborated upon in **sub-section iii**, below, implies that identifiers such as IMSIs or IMEIs may be viewed as 'private communications' or 'radio-communications' as they are transmitted to a network provider for the sole purpose of identifying the subscriber.

[273] 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).

At the same time, as noted above, it is by no means clear that section 492.2 was ever intended to identify individual *subscribers* as opposed to identifying devices and exposing the interactions between these devices.[274] IMSI Catchers, on the other hand, are often employed by state agencies for the purpose of identifying otherwise anonymous individuals, not solely for the purpose of obtaining a device's functional identification to facilitate routing. Courts have recognized that the definition of 'transmission data' is focused on the identification of devices and the interactions between them, not the subscribers associated with those devices.[275] Some courts have held that there is no value in merely identifying interactions between devices such as telephones without revealing the identity of individuals behind those devices.[276] This approach, however, ignores the nature of section 492.2 which is intended to be an intermediary, as opposed to final, investigative step.[277] It provides a means to identify suspicious interactions (i.e. specific phone calls) that warrant further investigative measures (i.e. that can form the grounds necessary for deployment of *other* investigative powers aimed at identification or wiretapping).[278] In this context, its

[274] As noted above, courts have recognized that the definition of 'Transmission Data' is aimed at identifying *devices* not *subscribers*:

[275] *Criminal Code (Can.)(Re)*, 2015 ABPC 178, para 30. See also: *Transmission Data Recorder Warrant (Re)*, 2015 ONSC 3072, para 7; *R v TELUS Communications Co*, 2015 ONSC 3226, paras 52-53: "Finally, TELUS says that the assistance order should not be interpreted as permitting the police to obtain the subscriber information because Parliament did not include such information within the confines of the TDRW authorization. Specifically, Parliament did not include subscriber information in the definition of transmission data and, therefore, it can be taken that Parliament did not intend that subscriber information would be obtained through a TDRW. Once again, I do not agree with TELUS' position on this point. I fully understand why subscriber information would not have been included in the definition of transmission data. It has nothing to do with transmission data. Indeed, it would have been a strange result to draft a definition of transmission data that included the name and address of either the sender or receiver of that data. One only has to look at the existing definition of transmission data to see how subscriber information would not fit comfortably into such a definition."

[276] *Transmission Data Recorder Warrant (Re)*, 2015 ONSC 3072, para 7; *R v TELUS Communications Co*, 2015 ONSC 3226: "Further, it is important to remember the purpose behind making an assistance order. An assistance order is granted where the court is satisfied that a person's assistance "may reasonably be considered to be required to give effect to the authorization or warrant". The reality is, of course, that the data obtained through the transmission data recorder warrant is of little or no use to the police unless they are provided with the identities of the persons who are connected to the cellular telephone numbers that represent the beginning and the end of the data transmitted." For a contrary view, particularly with respect to mobile phones, see: *R v Nguyen*, 2004 BCSC 76, paras 8-10: "The Crown had argued that subsection [492.1] (2) enabled the police to seize telephone records from telephone companies which would enable them to identify the names and addresses of the subscribers to all telephones that had received a call from the target telephone, or that had been used to make a call to the target telephone. Crown counsel submitted that the telephone numbers alone, would be useless to the police. I rejected that argument and ruled that only telephone records for the target telephones identified in the warrant, could be obtained under ss. 2. ... There is another distinction between land-land telephones and cellular telephones, concerning the publication of telephone numbers. All land-line telephone numbers, except those owned by subscribers who pay to have their telephone number 'unlisted', are published with the name and address of the subscriber, in the telephone directory that is circulated to members of the public. By contrast, no cellular telephone numbers are published in any such directory."

[277] Department of Justice, "Lawful Access – Consultation Document", August 25, 2002, http://www.canada.justice.gc.ca/eng/cons/la-al/la-al.pdf, p 11: "the Criminal Code also provides for production/collection orders under a lower standard in a very limited number of cases, such as income tax information for specific offences, tracking devices and dial number recorders (devices that record incoming and outgoing telephone numbers), at an earlier stage of the investigation. Except in these very limited cases, the current safeguard prevents important information from being gathered at an early investigation stage, even if there is a low expectation of privacy in relation to the information being sought." Note, the consultation launched by this document formed the basis for what ultimately became Bill C-13.

[278] For example, see: *R v Whitman-Langille*, [2004] QJ No 14164 (Que SC), para 7: "Mr. Fraser also testified, based upon his 32 years of experience, that this kind of evidence, namely the DNR records, also can lead eventually to other, more specific, methods of

bifurcation of 'subscriber identification' from 'device identification' is understandable, as the latter has value independent of the former.[279] It is also in keeping with the principle of 'minimal intrusion' on privacy to bifurcate access to routing information from identification of subscribers associated with this information.[280] This bifurcated approach is confirmed by the legislative history of section 492.2, which was recently updated in Bill C-13, but without any attempt to include a subscriber identification component to the power.[281] Indeed, an earlier version of Bill C-13 *did* include an independent and specific 'subscriber identification' power that would have been complimentary to section 492.2.[282] Notably, previous (and otherwise identical) versions of this Bill included IMSI and IMEI numbers as 'subscriber information' obtainable by means of the subscriber identification power contemplated.[283]

Another challenge to reliance on section 492.2 as IMSI Catcher authorization relates to the overlap between transmission data covered by section 492.2 and 'tracking data', under section 492.1. The definition of transmission data implicitly includes a concept of 'location' (i.e. the device that is the destination or termination of any digital communication or the 'origin or destination of a communication'). Historically, the location of fixed line communications devices was a known quantity. Identifying the origin and destination telephone numbers of two participants in a fixed line telephone call would therefore locate these two participants at their home, office or a public pay phone. Such is not the case for mobile devices, which of course are not associated with any specific physical location and are more closely associated with *individuals* not

---

investigation. For instance, wiretapping and searches can be carried out, with warrants, once the DNR information confirms or corroborates associations between suspected persons. The DNR information can also be sometimes used to displace associations, that is, to remove certain persons from suspicion." See also *R v Cody*, 2007 QCCA 1276 (affirming *R v Whitman-Langille*) at para 17: "... at the time DNR warrants are usually sought, the police do not in fact have "reasonable grounds to believe" that a crime may be committed by a particular target, since the police are still at an early stage of an investigation as it may relate to a particular individual. Rather, it is to enable the police to reach the stage of "reasonable grounds to believe" that DNR warrants are used, or to exclude someone from further investigation."; *R v Kutsak*, [1993] 108 Sask R 241 (Sask QB): "In this case, a security officer employed by SaskTel was assisting a police investigation into complaints from women who had received indecent telephone calls. There was reason to believe that the calls emanated from phones located at Kutsak's place of employment. The security officer connected a dial number recorder to the suspect phone lines and determined what numbers had been dialled. The police were given the information, the recipients of the calls were interviewed, and the charges against Kutsak resulted."

[279] *R v Rogers Communications Partnership*, 2016 ONSC 70, paras 58-59: "Consider the common scenario in which a tower dump order is sought to attempt to identify individuals proximate to multiple crime scenes. The underlying data may related to where tens of thousands of individuals were at a particular time and who they communicated with. The report, however, would only identify the very few individuals, if any, who happened to be proximate to more than one crime scene."

[280] *R v Rogers Communications Partnership*, 2016 ONSC 70, para 41.

[281] Bill C-13: Protecting Canadians from Online Crime Act. (2014). First reading November 20, 2013, royal assent December 9, 2014. Parliament of Canada. See: http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&Bill=C13&Parl=41&Ses=2.

[282] Bill C-30, 1st Sess 41st Parl, (First Reading), February 14, 2012, http://www.parl.gc.ca/content/hoc/Bills/411/Government/C-30/C-30_1/C-30_1.PDF, section 16. This provision was later dropped over controversy associated with its invasive potential.

[283] Bill C-52, *Investigating and Preventing Criminal Electronic Communications Act*, (2010) 3rd Sess, 40th Parl, (First Reading), November 1, 2010, http://www.parl.gc.ca/content/hoc/Bills/403/Government/C-52/C-52_1/C-52_1.PDF, clause 16.

residences. While it appears that some law enforcement agencies refrain from retaining tracking information obtained through transmission data powers, some courts have implied that this functionality is not precluded:

> … the Toronto Police Service filters out the location information, if it is included in the data received under the TDRW [transmission data recorder warrant], unless it has received a separate authorization for the location information, such as would be authorized by a tracking warrant… While that position is commendable, it does not change the fact that the TDRW does appear to allow for such information to be included in the data since the definition of transmission data includes 'origin' and 'destination'. While that may not have been the intention of a TDRW, that appears to be the result.[284]

This approach, however, is contrary to the holistic regime for transmission and tracking data interception recently put in place by Bill C-13, which appears to have amended section 492.2 with the explicit intent of preventing its use as a tracking power.

The term 'location' was removed from the definition of the data obtainable by section 492.2, which previously included any devices that could be "used to record or identify the telephone number *or location* of the telephone from which a telephone call originates, or at which it is received…"[285] Now it only includes data that "is transmitted to identify, activate or configure a device… or … the … origin, destination or termination of the communication."[286] The definition appears more focused on identifying devices that originate or terminate communications with all reference to location excised. In addition, Bill C-13 added sub-section 492.2(3), which holds that the transmission data recorder authorization provisions are no longer even available where tracking data is sought by the interception: "[n]o warrant shall be issued under this section for the purpose of obtaining tracking data."[287] The question therefore arises whether the data obtained by IMSI Catchers can be classified as 'tracking data'.

---

[284] *R v TELUS Communications Co*, 2015 ONSC 3964, para 39. See also *R v Cody*, 2007 QCCA 1276, para 14, quoting the court below, at *R v Whitman-Langille*, [2004] QJ No 14164 (Que SC), paras 5-6: "It was Mr. Fraser, in his testimony before the undersigned, who set out the purpose of the DNR warrants, in relation to an investigation as a whole, explaining that DNR records are used to confirm previous intelligence and to support physical surveillance being carried out simultaneously. For instance, if the subject of physical surveillance is lost, phone calls made by the subject on his cell phone can be used to indicate the area of the city or the county that the subject is in, enabling the surveillance team to recommence physical surveillance of the subject with little delay. In this case, for instance, investigators were able to effect the physical surveillance of a meeting between two subjects, as the result of such DNR records, which showed that one of the surveillance subjects, Pierre Bergeron, was coming from Montreal to Halifax."

[285] *Criminal Code*, RSC 1985, c C-46, version of section 492.2 from 2003-01-01 to 2015-03-08, http://laws-lois.justice.gc.ca/eng/acts/C-46/section-492.2-20030101.html, sub-section 492.2 (4), "Definition of 'Number Recorder'", emphasis added.

[286] *Criminal Code*, RSC 1985, c C-46, sub-section 492.2 (6), "Transmission Data".

[287] *Criminal Code*, RSC 1985, c C-46, sub-section 492.2(3).

Mobile Digital Identifiers as Tracking Data?

Tracking Data related interception powers are set out in section 492.1 of the *Criminal Code*. "Tracking Data" and a "Tracking Device" are defined as follows:

> *tracking data* means data that relates to the location of a transaction, individual or thing.
>
> *tracking device* means a device, including a computer program within the meaning of subsection 342.1(2), that may be used to obtain or record tracking data or to transmit it by a means of telecommunication.[288]

The difficulty that IMSI Catchers present is that their tendency is to expose "the location of a transaction, individual or thing" even where this is not the intention underlying their deployment.[289]

For example, where an IMSI Catcher is deployed for the purpose of identifying a device used by a known target in a known location, it will still capture the identifiers of all other devices in range, effectively geo-locating all of those devices and the individuals persistently associated with them.[290] State agencies operating an IMSI Catcher will be doing so in a given locale, and the digital identifiers captured by the device will therefore locate devices within the vicinity (whether targeted or not) as being within that locale. It would appear that most if not all IMSI Catcher deployments would collect "data that relates to the location of a transaction, individual or thing".[291] It is perhaps of little surprise that some US courts have similarly concluded that comparable metadata interception powers do not apply:

> ...the Hailstorm device, which is capable of obtaining active real-time location information—far different from a pen register (a device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument) or track and trace device (a device or process that captures the incoming electronic or other impulses that identify the originating number).[292]

The modern ubiquity of mobile devices has created a greatly enhanced tracking capability that can be readily exploited by metadata collection and interception

---

[288] *Criminal Code*, RSC 1985, c C-46, sub-section 492.1 (8), "Tracking Data" and "Tracking Device".

[289] *Criminal Code*, RSC 1985, c C-46, sub-section 492.1 (8), "Tracking Data".

[290] See, for example: *Maryland v Taylor*, Case No 11410031, Suppression Hearing, November 21, 2014, 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. 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."

[291] *Criminal Code*, RSC 1985, c C-46, sub-section 492.1 (8), "Tracking Data".

[292] *Maryland v Andrews*, (2016) *Md App LEXIS 33, File No 1496 (Md Ct of Special Appeals), p *35.

activities.[293] When the tracking powers in the *Criminal Code* were updated by Bill C-13, this ubiquity was recognized by the adoption of a more protective tracking data regime and of sub-section 492.2(3), to ensure this more protective regime is not undermined by the use of the overlapping transmission data interception powers.[294]

Should the digital identifiers obtained by an IMSI Catcher, in fact, qualify as 'tracking data', additional questions remain as to the proper application of section 492.1. This section creates two types of authorization powers that facilitate the use of a tracking device to obtain tracking data. Per sub-section 492.1(1), a judge may authorize state agencies to obtain, by means of a tracking device, tracking data associated with "the location of one or more transactions or the location of a movement of a thing, including a vehicle" ("Object Tracking Warrant"). A judge will issue such a warrant if there are reasonable grounds to suspect a crime has been or will be committed, and that the information sought will assist in the investigation of the offence – a low standard typically reserved for less sensitive and private data. In contrast, under sub-section 492.1(2), a judge may authorize state agencies to obtain tracking data associated with the "location of a thing that is usually carried or worn" by an individual by means of a tracking device ("Individual Tracking Warrant"). Sub-section 492.1(2) employs the higher "reasonable grounds to believe" standard, which is more protective of privacy interests. Under the transmission data powers, set out in section 492.2, a judge may authorize state agencies to intercept 'transmission data' by means of a transmission data recorder if the lower 'reasonable grounds to suspect' standard has been met ("Transmission Data Warrant").

The less protective 'Object Tracking Warrant' appears designed to capture less precise and comprehensive location information under the assumption that this kind of data is less privacy invasive. For example, if a tracking device were covertly placed inside a crate carrying goods in order to track it to its destination, such tracking is less likely to reveal intimate details relating to the owner of the crate.[295] Or, where police are more interested in locating a stolen device rather than any specific individual, they may seek geo-location data emitted by that device without direct interest in any person potentially associated with the device. Or, if GPS data emitted by an individual's Internet-connected car were recorded, this might tell law enforcement where the car is but not necessarily

[293] See *R v Foster*, 2013 ONCJ 723, para 36: "The overwhelming and ubiquitous use of cellphones, the advance cellphone technology and the extent of information that can be obtained about cellphones and the people who use them may permit such information to reveal personal information and biographical information about the users such as the identification of movement, who the person associates with and the frequency of such contact." See also: **Box 2** on p 88.

[294] Bill C-13: Protecting Canadians from Online Crime Act. (2014). First reading November 20, 2013, royal assent December 9, 2014. Parliament of Canada, http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&Bill=C13&Parl=41&Ses=2.

[295] See for example: *R v Cook*, 2010 ONSC 1188; *R v Al-Amiri*, 2013 NLTD(G) 69; *R v Scott*, 2009 BCPC 235.

the precise location of the car's owner. Devices closely associated with an individual require the more protective 'Individual Tracking Warrant' if they are to be tracked.[296] The reason for this distinction is that the less protective 'reasonable suspicion' standard used for Object Tracking Warrants is only available when police want to access non-sensitive data, whereas it is presumed that tracking devices closely associated with an individual will provide a clearer window into that individual's life and, as a result, is more intrusive when compared to tracking an object or thing.

The differentiation between Object Tracking and Individual Tracking Warrants may be unsustainable since both kinds of surveillance can engage roughly equivalent privacy interests. Tracking an individual's car, for example, can provide a comprehensive picture of that person's location and, over time, of their personal life as it would indicate the stores they visit, the medical clinics they visit, the religious institutions they visit, the people they visit, etc.[297] Likewise, an attempt to track a stolen device is also an attempt to track the individual who stole it, so the distinction between tracking a 'device' or an 'individual' is inherently unstable.[298] Regardless of this broader potential clash in definitions, IMSI Catcher use should typically and unambiguously engage the more protective 'Individual Tracking' powers. It is widely recognized that mobile phones now accompany individuals almost everywhere they go, leading a justice of the Supreme Court of the United States to go so far as to remark that:

> … modern cell phones … are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.[299]

In light of this ubiquity and the persistent nature of the digital identifiers obtained by IMSI Catchers, deployment is not only likely geolocate individuals within range on the basis of the mobile devices in their pockets, purses and backpacks, but will do so persistently. Once obtained, these identifiers can be used to locate individuals appearing in *future* IMSI Catcher deployments as well – a factor that rapidly becomes meaningful if IMSI Catchers are used as widely in Canada as abroad.[300]

---

[296] See for example, *R v Edwards*, 2014 ONSC 6233 and *R v Riley*, [2008] 234 CCC (3d) 181 (ON SC), for examples where a phone is specifically tracked for the purpose of locating and identifying an individual associated with it.

[297] See, for example, *R v Scott*, 2009 BCPC 235, where tracking of the vehicle was synonymous with tracking of the individual. See also: *US v Jones*, (2012) 565 US __, (Supreme Court of the United States).

[298] *Redmond v State*, 73 A.3d 385, (2013), (United States Maryland Court of Special Appeals).

[299] *Riley v California*, (2014) 573 US __ (Supreme Court of the United States), Chief Justice Roberts, writing on behalf of the court.

[300] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div); ; 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 ("in one case last summer, a detective testified that the Baltimore police have used a Hailstorm some 4,300 times"); Colin Freeze, Matt

Bill C-13 represents a clear legislative intent to protect 'individual' location data more rigorously than 'object or transactional' location data. Given the capacity of IMSI Catcher-obtained data to reveal the movements of individuals, now and in the future, the authorization of such devices should not fall to the less protective "Object Tracking" or "Transmission Data" authorization regimes. Further, as argued below, the use of the reasonable suspicion standard associated with these two powers is likely fails to meet the minimal constitutional standard for privacy protection implicated by most IMSI Catcher deployments.

Inducing Transmission of Mobile Identifiers

A final hurdle remains to state agencies seeking to rely on either section 492.1 or 492.2 as authorization for deploying an IMSI Catcher. This additional challenge relates to the manner in which IMSI Catchers operate by interfering with the normal functioning of mobile devices to induce transmission of mobile identifiers. Such functionality is more intrusive than that carried out by transmission data recorders and tracking devices and might therefore fall outside their statutory definition.

As noted above, the *Criminal Code* defines tracking devices and transmission data recorders, respectively, as such:

> 492.1 (8) *tracking device* means a device, including a computer program within the meaning of subsection 342.1(2), that may be used to obtain or record tracking data or to transmit it by a means of telecommunication.
>
> 492.2 (6) *transmission data recorder* means a device, including a computer program within the meaning of subsection 342.1(2), that may be used to obtain or record transmission data or to transmit it by a means of telecommunication.[301]

Further, state agencies are authorized to "install, activate, use, maintain, monitor and remove" such devices.[302]

These provisions envision devices that intercept or acquire data, and can transmit it. This could include the installation of a traditional interception device within a service provider's network that, once installed, passively obtains or records information as it

---

Braga & Les Perreaux, "RCMP Fight to Keep Lid on High-Tech Investigation Tool", *The 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/ ("the New York Police Department, for example, was recently forced to release documents showing it had secretly used similar tracking technology more than 1,000 times since 2008."); *R v Rogers Communications*, 2016 ONSC 70 (much as with a 'tower dump', a single deployment can implicate the privacy of thousands or even tens of thousands of individuals, and there is no clear obligation to delete non-targeted data once it is legitimately obtained), see paras 25, 58 and 65 (e)..

[301] *Criminal Code*, RSC 1985, c C-46.

[302] *Criminal Code*, RSC 1985, c C-46, sub-sections 492.1(3) and 492.2(2).

travels through the network or the covert installation of a GPS device on a person or vehicle that will emit longitude and latitude at regular intervals via telecommunications. Some have argued these provisions may extend to include the remote activation of a tracking device already embedded in a mobile device, most of which already include GPS capabilities.[303] Others have stated concerns that the provision might be used to install malware on devices for the purpose of transmitting data to law enforcement by means of telecommunications.[304] These latter two usage scenarios, if indeed within the authorization framework established by sections 492.1 and 492.2, certainly entail more active interference with the operation of a mobile device than their historical antecedents. However, the 'active interference' envisioned by these use cases relate to the installation or activation of the device in question, not its operation, which are independently authorized.[305]

By contrast, an IMSI Catcher, once activated, subverts the operation of the GSM network to induce mobile devices to interact with it and to transmit data that would not otherwise be transmitted.[306] First, it convinces devices in range to interact with it by impersonating the customer's mobile network provider and tricking the customer's devices into believing that the IMSI Catcher has become the 'closest' cell tower. Next, the IMSI Catcher induces these devices to transmit their IMSI and IMEI numbers to the IMSI Catcher – transmission that typically will only occur when a device is activated or first joins a service provider's network.[307] If additional digital identifiers such as the MSISDN (phone number) are sought, the IMSI Catcher must induce mobile devices within range to engage in fake phone calls by initiating a fake or 'silent' call. Repeated 'silent calls' may be initiated by the IMSI Catcher if more precise location information is sought, as such calls force recipient mobile devices within range to 'check in' with the IMSI Catcher more frequently, creating a richer dataset from which to map the devices' movements more comprehensively.

---

[303] See: Julia Nicol & Dominique Valiquet, "Bill C-13: An Act to Amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", December 11, 2013, Revised August 28, 2014, Legislative Summary, 41.2.C13.E, http://www.lop.parl.gc.ca/Content/LOP/LegislativeSummaries/41/2/c13-e.pdf, p 13.

[304] Christopher Parsons, 2014. "Canadian Cyberbullying Legislation Threatens to Further Legitimize Malware Sales", June 4, 2014, *Technology, Thoughts & Trinkets*, https://www.christopher-parsons.com/canadian-cyberbullying-legislation-threatens-to-further-legitimize-malware-sales/.

[305] *Criminal Code*, RSC 1985, c C-46, sub-sections 492.1(3) and 492.2(2).

[306] The inducement process is described in greater detail in **Section One: B**, above. Only a cursory summary is provided here.

[307] Fabian van den Broek, 2010. "Catching and Understanding GSM-Signals", March 2010, Thesis Number 628, http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf, section 2.5.2 and p 90: "A much easier way would be an active fake base station attack. If an attacker starts a fake base station, seemingly from the correct provider, in the neighborhood of his victim MS, then this MS will try to register to the fake base station. Probably the MS will start sending its TMSI, which the fake base station will reject, resulting in the MS transmitting its IMSI. Naturally the attacker would have to make sure that the reception from his fake base station is better than the reception of the current serving BTS. This attack, being an active attack, can be detected. This is typically how industrial IMSI catchers work."

This active interference and inducement may well fall outside the functional definition of a transmission data recorder and tracking device. These devices can 'obtain, record or transmit' data, terms that have not been judicially interpreted in Canadian law. Some US courts have held, with respect to comparable interception powers, that the active manner in which IMSI Catchers induce mobile devices to transmit the identifiers sought impacts on the availability of the underlying powers in question:

> The function of the [IMSI Catcher] Hailstorm device—to shower an electronic barrage of signals into a target area to actively engage the target cell phone—goes well beyond the bounds of the pen register statute which by its terms is limited to authorizing devices that record or identify the source of a communication or capture an originating number.[308]

The legislative language in the Canadian *Criminal Code* is broader than that in the US statutes relating to the interception of transmission data, which limit authorization to recording or interception of "incoming" data that "is transmitted" from an electronic communications device.[309] By contrast, sections 492.1 and 492.2 authorize the use of devices that can "obtain or record" transmission or tracking data, or "to transmit it by a means of telecommunication".

However, both the US and Canadian provisions have historically aimed at authorizing devices that passively intercept data that is already being transmitted between one device and another.[310] Indeed, the terms 'obtain or record' are synonymous with the terms 'record or acquire' found in the definition of "intercept" in Part VI of the *Criminal Code*,[311] and emulate the historic functionality of interception devices used to passively record telephone numbers (or other data) emitted by mobile devices.[312] The term 'transmit by telecommunications' reflects the historical functionality of a tracking device that, once installed on a person or object, transmits its location by means of telecommunications. IMSI Catchers are of a different class of instrument. An IMSI Catcher does not 'transmit data by means of telecommunications'. Rather, it induces transmission of such data from the mobile device. This active inducement of data

---

[308] *Maryland v Andrews*, (2016) *Md App LEXIS 33, File No 1496 (Md Ct of Special Appeals), pp *77-79.

[309] *Maryland v Andrews*, (2016) *Md App LEXIS 33, File No 1496 (Md Ct of Special Appeals).

[310] *Criminal Code*, RSC 1985, c C-46, sub-sections 492.1(3) and 492.2(2) employ the terms 'obtain' and 'record' in lieu of the terms 'acquire' and 'intercept' found in Part VI of the *Criminal Code*, but are effectively synonymous. The term 'transmit by means of telecommunications' is intended to replicate the historical functionality of a standard tracking device, a homing device that, once attached to an object or thing, emits an electronic signal that can be used to track the thing to which it is attached, see for example: See for example: *R v Cook*, 2010 ONSC 1188; *R v Al-Amiri*, 2013 NLTD(G) 69; *R v Scott*, 2009 BCPC 235.

[311] *Criminal Code*, RSC 1985, c C-46, section 184.2, "Intercept".

[312] Described in *R v Fegan*, [1993] 13 OR (3d) 88, (CA)(digital number recorders) and *R v Edwards*, 2014 ONSC 6323, (tracking device used to intercept). See also: *R v Riley*, [2008] 234 CCC (3d) 181 (ONSC)(Tracking devices), para 125: "Apparently, the technology used for tracking cell phones can be used to intercept private communications, and so this warning was thought to be advisable.".

transmission extends beyond the passive interception that is the functionality of interception devices as well. Moreover, the active inducement entails significant interference with the functionality of the mobile device itself, disrupting its ability to function for the extent of the interference. By contrast, passive interception devices (data recorders, wiretaps, etc) do not cause such interference when obtaining or recording communications – indeed, such interference would risk revealing the presence of the interception. Overall, the invasive and active manner in which IMSI Catchers induce the transmission of data may take these devices outside the passive interception envisioned by sections 492.1 and 492.2.

ii. General Warrants: Residual Authorization Power

Under section 487.01 of the *Criminal Code*, law enforcement agencies may seek authorization to "use any device or investigative technique or procedure or do any thing" that would constitute an unreasonable search and seizure if carried out without prior judicial authorization.[313] This section was introduced into the *Criminal Code* following a series of decisions of the Supreme Court holding that unauthorized use of some invasive electronic surveillance techniques violated section 8 of the *Charter* and was impermissible.[314] In anticipation of unforeseen future techniques that lacked an explicit *Criminal Code* authorization mechanism but that would still require judicial authorization, this general warrant provision was added. It was intended to be used sparingly, as a supplementary power of limited resort.[315]

General warrants can only be issued if there are reasonable grounds to believe that information concerning an offence will be obtained and if such issuance is in the best interests of the administration of justice.[316] Given their open-ended nature and potential for intrusiveness, general warrant authorizations must also include any terms or conditions the authorizing judge considers necessary to ensure that the contemplated search or seizure is reasonable.[317] General warrants are intended as a supplementary power, not a substitute to existing search and seizure powers and, as such, are only available where no other provision exists that would provide

[313] *Criminal Code*, RSC 1985, c C-46, section 487.01.

[314] *R v Duarte*, [1990] 1 SCR 30; *R v Wong*, [1990] 3 SCR 36; *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Moldaver, J, concurring, paras 54-56.

[315] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Moldaver, paras 80, 93: "...it is important for the police to appreciate that general warrants are not warrants of general application. On the contrary, they are to be used sparingly, when the investigative technique they wish to employ is truly different in substance from an investigative technique accounted for by another legislative provision."

[316] *Criminal Code*, RSC 1985, c C-46, paragraphs 487.01(1) (a) - (b).

[317] *Criminal Code*, RSC 1985, c C-46, sub-section 487.01(3).

authorization for the investigative technique in question.[318] This extends to situations where a general warrant is sought to achieve a technique that is substantially similar to that which can be achieved by an existing search or seizure power.[319] The ability to achieve a substantially similar law enforcement objective,[320] or to obtain the same data[321] by other legal powers can be indicative of 'substantial equivalence', but the focus of the analysis is on whether what police seek to authorize under a general warrant is substantially different from what they can do under a different power.[322] Where the technique law enforcement seek to carry out bears similarity to a search or seizure that typically includes more expansive safeguards, scrutiny of substantive equivalency is more rigorous.[323]

Whether a general warrant is available as authorization for IMSI Catcher use will, then, depend on whether such devices can be authorized by other powers and, in particular, by other powers with more extensive safeguards. As highlighted in the previous section, IMSI Catcher use is an imperfect fit within the overlapping *Criminal Code* provisions for intercepting metadata such as transmission data and tracking data. It remains unclear whether such use amounts to interception of transmission data, tracking data or neither. While we argue that the Individual Tracking power is the most appropriate source of IMSI Catcher authorization from within that framework, its overall ambiguity suggests that a general warrant might be better suited.

Further, in the following sub-section, we argue that at least in some instances, a Part VI wiretapping authorization might be required before an IMSI Catcher can be deployed. In such instances, general warrants should not be available as an option for IMSI Catcher authorization, as use of a general warrant would undermine the more rigorous protections found in Part VI.[324] Finally, as noted above, the active

---

[318] *Criminal Code*, RSC 1985, c C-46, paragraph 487.01 (1)(c); *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Abella, J, paras 16-18, per Moldaver, J, concurring, para 91.

[319] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Abella, paras 20; Moldaver, J, concurring, para

[320] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Moldaver, concurring, J, para 68, 74: "I accept the Crown's contention that, as a technical matter, what occurred here was different from what would occur pursuant to a Part VI authorization. I do not accept, however, that that fact [page38] is determinative in light of the identical privacy interests at stake. But for the 24-hour time delay, the investigative techniques were the same. … Consequently, in this case, a narrow focus on the mechanics of the search is to miss the forest for the trees. The general warrant must be analogized to a Part VI authorization if one is to appreciate the actual incentives before the police. A mechanistic interpretation of the "no other provision" requirement cannot hold because, put bluntly, a general warrant can prove easier to obtain than a Part VI authorization. For that reason, one can hardly fault the police for seeking a general warrant instead of a Part VI authorization. There was little to be lost (a delay in the receipt of the data sought, which may well have had little consequence) and much to be gained…"

[321] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Moldaver, J, concurring, para 67.

[322] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Moldaver, J, concurring, paras 80, 101-102.

[323] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Abella, J, para 44 and Moldaver, J, concurring, para 81.

[324] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16.

interference inherent in IMSI Catcher operation might mean that the use of such devices falls wholly outside of Part VI and the metadata interception framework, making a general warrant the only available vehicle for authorization.

However, even if this were the case, it would still fall to courts to consider if state agencies could rely on 'substantially similar' powers that are less invasive because they do not rely on IMSI Catchers at all. We explore the potential impact of these substantially similar powers in the following paragraphs. Regardless, as we note in **Section Four**, below, the intrusive nature of IMSI Catchers requires the imposition of additional safeguards that should be inserted into whatever authorization mechanism is used to ensure that these devices do not unduly impact on privacy interests. Moreover, general warrants are designed to fill authorization gaps and to be of limited resort.[325] If IMSI Catcher use becomes as prevalent in Canada as in other jurisdictions,[326] and general warrants become the primary mechanism of their authorization, such use will by no means be 'limited'. It would therefore be appropriate for the legislature to establish an appropriate authorization framework for such devices.

Substantial Equivalence: Achieving IMSI Catcher objectives by less intrusive means

The *Criminal Code* includes a number of production powers that might be used to carry out substantively equivalent techniques by far less invasive means than the use of an IMSI Catcher. Regardless of their availability as authorization for IMSI Catchers, the metadata interception powers described in the next section can be used to install tracking and transmission data emitted by mobile devices without raising the same invasive challenges.[327] In particular, the *Criminal Code* includes additional powers that could be used to effectively turn cellular networks into functional IMSI Catchers. Instead of impersonating mobile phone towers, law enforcement could use these powers to compel service providers to provide the same IMSI/IMEI information, as collected by the provider's own towers in the normal course of business.

---

[325] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Moldaver, paras 80, 93: "…it is important for the police to appreciate that general warrants are not warrants of general application. On the contrary, they are to be used sparingly, when the investigative technique they wish to employ is truly different in substance from an investigative technique accounted for by another legislative provision."

[326] 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/.

[327] See for example: *In re Application for Cell Tower Records Under 18 USC §2703(D)*, (2015) 90 F.Supp.3d 673 (Southern District of Texas, Houston Division): "A further word is necessary to avoid possible misunderstanding. This holding has no application to a related though very different investigative technique using a device known as a cell site simulator, sometimes referred to as a 'StingRay.' Like a cell tower dump, the StingRay device may be used to discover telephone and other identification numbers of wireless devices in a given location. However, there are several critical differences: (1) the device is deployed by law enforcement, not the provider; (2) the information obtained is transmitted in real time directly to law enforcement, not retrospectively via the provider's records; and (3) the device allows continuous real time tracking of the wireless devices in contact with it."

Specifically, the government could apply for a production order forcing a network operator to disclose historical tracking data under section 487.017. Such an order may be granted when a justice or judge is satisfied there are "reasonable grounds to suspect that an offence has been or will be committed … and the tracking data is in the person's possession or control and will assist in the investigation of the offence."[328] Data derived from this kind of production order could be used to track the movements of persons within a stated geographic area at a given time, or specific persons as they move about during their daily lives.

In addition, state agencies have the option of obtaining a production order for historical transmission data under 487.016. Such an order would compel a service provider to produce transmission data under comparable conditions to those attached to the tracking data power encoded in section 487.017.

Finally, a 'communications trace' order under section 487.015 could be used to compel a service provider to produce any historical transmission data "for the purpose of identifying a device or person involved in the transmission of a communication." A communications trace order is granted under comparable conditions to 487.017 orders, including use of the lower reasonable suspicion standard. **Table 2** summarizes these various production powers, the grounds under which they are authorized, and the purposes of each kind of order:

Order Type	***Grounds to Issue***	***Purpose of Order***
Historical Tracking Data (487.017)	Suspicion privacy invasion will assist in investigation of an offence	Compel service provider to produce data that can indicate the location of a transaction, individual or thing
Historical Transmission Data (487.016)	Suspicion privacy invasion will assist in investigation of an offence	Compel service provider to produce data that is transmitted to identify a device in order to facilitate telecommunications
Communications Trace (487.015)	Suspicion privacy invasion will assist in investigation of an offence	Produce historical transmission data that might assist in identifying a device or person involved in the transmission

Table 2: Relevant Production Orders

In **Section Three: B-i**, above, we question whether the types of identifiers sought by IMSI Catchers fall within the definitions of 'transmission' and 'tracking' data,

[328] *Criminal Code*, RSC 1985, c C-46, *s*ection 487.017.

respectively. If they *do* fall within these definitions, then any of these production powers could technically be available if a law enforcement agency wished to compel a service provider to disclose stored historical IMSI/IMEI information that is captured by the provider in the course of a mobile device's transmission activities.

The use of these production powers will, in many (but not all) instances, produce a comparable outcome to deploying an IMSI Catcher. In addition, the metadata interception powers highlighted in the previous section can also be used in many, but not all, instances to achieve comparable outcome. A court asked to authorize IMSI Catcher use by means of a general warrant would therefore need to consider whether these alternative options are 'substantially similar'. This standard does not amount to an investigative necessity requirement – state agencies need not demonstrate that they have tried all other reasonable available techniques to demonstrate that what they seek to do is 'substantially different'.[329] However, where less intrusive techniques are available to obtain the same data and achieve the same investigative objective by comparable but less intrusive means, a general warrant may not be available.

In *R v TELUS*, for example, the use of a general warrant to authorize production of all prospective text messages at the end of every day was seen as substantially similar to a wiretap, which forwards all text messages to law enforcement 'in real time'.[330] Both techniques provided state agencies access to future text messages that had not yet been sent. However, in *TELUS*, obtaining this data and objective by means of a general warrant would allow law enforcement to bypass important safeguards built into the wiretapping regime based on narrow functional differences in the method of acquisition (obligating the service provider to produce the text messages at the end of each day instead of installing a real-time wiretap). Here, the question would be whether state agencies can obtain a general warrant to authorize a more intrusive investigative method (IMSI Catchers) in instances where less intrusive production orders are available to achieve substantially the same investigative outcome.

iii. *Criminal Code* Wiretapping Protections & Interception of Metadata

In light of the invasive nature of IMSI Catchers, part VI of the *Criminal Code* provides the most appropriate framework for the authorization of IMSI Catchers. It has historically been reserved for more intrusive electronic surveillance techniques and as such includes critical safeguards and transparency measures necessary to ensure IMSI Catcher use is properly confined. Below, we argue that as a matter of law, Part VI may

[329] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, paras 101-102.

[330] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16.

apply to at least some IMSI Catcher deployment scenarios. Regardless, as articulated in **Section Four** below, it provides the most appropriate vehicle for authorizing what is an inherently invasive tool, and the application of Part VI (with some specific modifications) to this tool in full should be confirmed by legislative amendment.

Part VI of the *Criminal Code* prohibits the interception of private communications without prior judicial authorization and offers a number of additional protections and safeguards not required by other authorization mechanisms.[331] Some have advanced a narrow view of what constitutes a private communication that would preclude the application of Part VI: this view excludes machine-to-machine communications as well as communications that 'enable' communications, but are not themselves the 'content' of communications. Such an approach would exclude interception of IMSI/IMEI from Part VI protection. However, courts have suggested that Part VI should receive a purposive interpretation that adapts to changes in communications mediums. The role of machine-to-machine communications and metadata that undergird daily life today, and which are responsible for enabling person-to-person communications, would suggest that Part VI protections should indeed extend to the use of IMSI Catchers. These competing arguments are examined in this section.

The narrow view of what constitutes a private communication was summarized by the Ontario Court of Appeal in *R v Fegan*: it only includes information communicated between human beings, excluding data that is either communicated at the initiation of a machine or is received by one:

> I would not expect the above definition to include electronic or other signals between machines even without the modifying words that the originator would not expect an interception. Even without the benefit of authority, I think that "communication" in the sense of private communication contemplates an exchange of information between persons, whether it be oral or otherwise.[332]

Alternatively, others have argued that Part VI excludes data disclosed to a service provider for the purpose of processing a communication as it constitutes information 'about' a communication, not the content thereof.[333] However, it may well be that use of IMSI Catchers may fall under the more expansive protections found in Part VI of

---

[331] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16.

[332] *R v Fegan*, [1993] 13 OR (3d) 88, (CA), para 30.

[333] Historical jurisprudence on this question is reviewed comprehensively by Sulyma, J., in *R v Lee*, 2007 ABQB 767, as well as in Craig Forcese, "Law, Logarithms and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives", in Michael Geist, *Ed*, *Privacy & Surveillance in Canada in the Post Snowden Era*, (Ottawa: University of Ottawa Press, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436615.

the *Criminal Code* in spite of these two historical considerations.

To begin with, defining 'private communications' as exclusively encompassing interactions initiated and received by human beings is out of step with the realities of today's communications systems. Today's computing and mobile devices generate a steady stream of information regarding their owners. The multiple applications on the average computing device harvest data such as our GPS-tracked location history, our contact books, our never-sent commentary, audio and video recordings of our living rooms and general surroundings, exhaustive telemetrics, critical network security passwords, the objects we touch, our emotions and sentiments, and web browsing activities.[334] While individuals typically install all of these applications, the information they generate and send is often dissociated from their core functionality.[335]

This trend will only intensify in the future and is already taking hold. The so-called Internet of Things is premised on the concept of machine-to-machine communications, with network-enabled components sending a constant stream of information on their individual owner's behalf. This data encompasses such sensitive data as health monitoring and detailed financial information. The Internet of Things transmits more innocuous data at such a level of comprehensiveness that it will paint detailed pictures of the lives of those behind the machines.[336] This trend is already taking hold – CISCO's Visual Networking Index (VNI) reports that machine-to-machine (M2M) connections reached half a billion in 2014, generating roughly 36 petabytes of data per month.[337] Mobile devices play a central role in the Internet of Things as

---

[334] Jennifer Golbeck, "On Second Thought…: Facebook Wants to Know Why you Didn't Publish That Status Update You Started Writing", *Slate*, 13 December, 2013, https://www.abine.com/blog/2014/facebook-tracking-browsing/; Samuel Gibbs, "Samsung's Voice-Recording Smart TVs Breach Privacy Law, Campaigners Claim", *The Guardian*, 27 February, 2015, http://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim; Daniel Hoffman, "Exposing Your Personal Information – There's An App for That", *Juniper Networks*, 30 October, 2012, https://forums.juniper.net/t5/Security-Now/Exposing-Your-Personal-Information-There-s-An-App-for-That/ba-p/166058; Gordon Kelly, "Windows 10 Worst Feature to Install on Windows 7 and Windows 8", *Forbes*, 30 August, 2012, http://www.forbes.com/sites/gordonkelly/2015/08/30/windows-10-spying-on-windows-7-and-windows-8/; David Kravets, "Researcher's Video Shows Secret Software on Millions of Phones Logging Everything", *Wired*, 29 November, 2011, http://www.wired.com/2011/11/secret-software-logging-video/; Simon Rockman, "Uh Oh: Windows 10 Will Share your Wi-Fi Key With Your Friends' Friends", *The Register*, 30 June, 2015; Sean Gallaghar, "Does NSA Know Your Wi-Fi Password? Android Backups May Give it to Them", 17 July, 2013, http://arstechnica.com/security/2013/07/does-nsa-know-your-wifi-password-android-backups-may-give-it-to-them/; Ron Amadeo, "Disney's Smartwatch Prototype Can Identify and Track Everything You Touch", 10 November, 2015, http://arstechnica.com/gadgets/2015/11/disneys-smartwatch-prototype-can-identify-and-track-everything-you-touch/; Microsoft, "Project Oxford: Emotion APIs", accessed December 22, 2015, https://www.projectoxford.ai/emotion.

[335] See, for example: *Goldenshores Technologies v Geidl*, Docket No 132 3087, (2013)(United States Federal Trade Commission), https://www.ftc.gov/sites/default/files/documents/cases/131205goldenshorescmpt.pdf; Daniel Hoffman, "Exposing Your Personal Information – There's An App for That", *Juniper Networks*, 30 October, 2012, https://forums.juniper.net/t5/Security-Now/Exposing-Your-Personal-Information-There-s-An-App-for-That/ba-p/166058.

[336] Julia Powles, "Internet of Things: The Greatest Mass Surveillance Infrastructure Ever?", *The Guardian*, 15 July, 2015, http://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance.

[337] CISCO, "Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014-2019", 3 February, 2015,

hubs by which 'things' are controlled and through which resulting data flows.[338] It is difficult to characterize any of these interactions as communications 'initiated by a person' or anything other than machine to machine interactions.[339]

Nonetheless, the devices and applications that generate this data belong to the person who installed them, and the information transmitted relates to them. The Part VI analysis is a normative one. As noted by the British Columbia Court of Appeal in 2015: "[t]he question is whether, in keeping with societal and legal norms in Canada, the sender of [a message] should reasonably expect that [it] will remain private…".[340] Therefore, even if individuals are not aware that their devices are generating and transmitting all of this information, the question is normative – *should* individuals be able to expect that the data will not be intercepted? The information transmitted by devices on behalf of individuals (information identifying the individual, revealing her location, monitoring her health, etc.) is, often, today's equivalent of a phone call. The health monitoring tools that automatically transmit your state to your doctor replace the phone call you would have made a decade ago. A categorical exclusion of communications from Part VI protection on the sole basis that they are 'machine generated' would be starkly at odds with an individual's normative expectations as well as with the underlying purposes of Part VI. Moreover, to exclude IMSI numbers and other types of metadata from the purview of Part VI would allow a narrow "technical approach" to "render Part VI irrelevant to the protection of…privacy in new…communications technologies."[341]

A second independent argument against including IMSI Catchers from Part VI protection might arise from the view that Part VI only applies to 'content rich' data, excluding

---

http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf, pp 14-17 and Appendix A.

[338] Sang-Joong Jung, Risto Mylllyla and Wan-Young Chung, "Wireless Machine-to-Machine Healthcare Solution Using Android Mobile Devices in Global Networks", (2013) 13(5) *IEEE Sensors Journal* 1419, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6392192.

[339] *R v Fegan*, [1993] 13 OR (3d) 88, (CA), para 30: "I would not expect the above definition to include electronic or other signals between machines".

[340] *R v Pelucco*, 2015 BCCA 370, per Groberman, J.A. Contrast with: *R v Fegan*, [1993] 13 OR (3d) 88, (CA), para 30: ("I am not now discussing the concept of a reasonable expectation of privacy in a communication but of what amounts to a communication within the language of s. 183 of the Code.") and *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Abella, J, paras 25-26, 36: ("Consistent with the broad scope of Part VI, this definition is not exhaustive and focuses on the state acquisition of informational content — the substance, meaning, or purport — of the private communication. It is not just the communication itself that is protected, but any derivative of that communication that would convey its substance or meaning. … This definition focuses on the individual's reasonable expectation of privacy in the communication. … The interpretation of "intercept a private communication" must, therefore, focus on the acquisition of informational content and the individual's expectation of privacy at the time the communication was made."). See also: Craig Forcese, "Law, Logarithms and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives", in Michael Geist, *Ed*, *Privacy & Surveillance in Canada in the Post Snowden Era*, (Ottawa: University of Ottawa Press, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436615, p 142: "The reasonable expectation of privacy is a normative concept that does not vary with naiveté and risk that people's privacy expectations may be dashed."

[341] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Abella, J, para 33.

'metadata' or data 'about' a communication such as that identifying its origin, location, length, or destination. This argument is equally difficult to defend in the era of modern communications. Metadata such as IMSI/IMEI numbers, IP addresses, and other identifiers "constitute revealing, personal information from which potentially intimate content data can be inferred."[342] Such identifiers may not be deeply sensitive if analyzed in and of themselves but, in *R v Spencer*, the Supreme Court of Canada unanimously rejected a reductionist approach to assessing the reasonableness of privacy expectations by holding that one must look past the individual piece of information in question (the identifier or IMSI) and rather look to the activity its acquisition reveals.[343] As noted in the previous sub-section, IMSI numbers are a dynamic source of data that can be used to infer a great deal of information, including places of residence, workplace, political activity, and so forth. Such identifiers are "the means by which a biographical core of personal information is assembled."[344]

The argument that private communications only include 'content-rich' interactions also at times rests on the fact that some identifiers and metadata are disclosed to third parties (service providers) and are thus not considered 'private' communications.[345] This argument fails as Canadian courts have rejected the so-called 'third party' doctrine, which holds that information disclosed to a third party somehow loses its privacy expectations.[346] Moreover, whereas number recorders are typically deployed within a service provider's actual network,[347] IMSI Catchers are operated directly by law enforcement agencies. By impersonating the service provider, IMSI Catchers intercept transmitted IMSI/IMEIs before they reach the network operator at all and, hence, are not "already in the hands of third parties". [348]

Finally, it is notable that the content component of private communications protected by

---

[342] Craig Forcese, "Law, Logarithms and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives", in Michael Geist, *Ed*, *Privacy & Surveillance in Canada in the Post Snowden Era*, (Ottawa: University of Ottawa Press, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436615**Error! Hyperlink reference not valid.**, p 138.

[343] *R v Spencer*, [2014] 2 SCR 212, 2014 SCC 43.

[344] Daphne Gilbert, Ian R Kerr & Jena McGill, 2007. "The Medium and the Message: Personal Privacy and the Force Marriage of Police and Telecommunications Providers", (2007) 51(4) *Crim L Q* 469, http://iankerr.ca/wp-content/uploads/2011/08/the_medium_and_the_message.pdf, p 503.

[345] See for example, *R v Lee*, 2007 ABQB 767, para 282: "…the originator of such data knows some or all of it will or might be collected by the phone company in the normal course of business."

[346] *R v Duarte*, [1990] 1 SCR 30; *R v Spencer*, [2014] 2 SCR 212, 2014 SCC 43. Although the Supreme Court of Canada has acknowledged that where information is disclosed to a third party, it *can* lower the privacy expectations accorded to that information. See: *R v Edwards*, [1996] 1 SCR 128; *R v Gomboc*, [2010] 3 SCR 211, 2010 SCC 55.

[347] See for example: *R v Fegan*, [1993] 13 OR (3d) 88, (CA), paras 25-28.

[348] Craig Forcese, "Law, Logarithms and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives", in Michael Geist, *Ed*, *Privacy & Surveillance in Canada in the Post Snowden Era*, (Ottawa: University of Ottawa Press, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436615, pp 145-46.

Part VI includes the communication itself as well as "any derivative of that communication that would convey its substance or meaning."[349] This is reflected in the *Criminal Code* definition of "transmission data" adopted by Bill C-13, which applies to routing information but excludes data that would "reveal the substance, meaning or purpose of the communication."[350] IMSI Catchers allow state agencies to insert themselves into the middle of an interaction between a customer and their service provider, impersonating the service provider in order to intercept communications between the two. The communication intercepted by IMSI Catchers as a result has an underlying purpose – to identify the customer to the network. Moreover, state agencies often deploy IMSI Catchers for the same purpose, to identify an individual associated with a device. The resulting interception can therefore implicate the 'purpose' of the communication between a customer and her service provider (namely, to identify the former to the latter).[351] By extension, intercepting these identifiers can amount to obtaining the substance of the communication in question, whose primary purpose is to identify the customer to the provider.

Similarly, IMSI/IMEI interception might fall outside the *Criminal Code* definitions of transmission data as well, as that definition does not extend to subscriber identifying information, but is limited to information needed to identify the functional route of communications transmissions.[352] In most instances, IMSI Catchers are not capturing this information in order to facilitate the tracking of a given transmission. The information is being captured to identify an individual. Even where identification is not the primary state agency objective animating an IMSI Catcher deployment, it remains the case that the resulting interception obtains the substance of the communication between the customer and the service provider.

However, where the state agency objective is to track the individual, the resulting interception may fall outside of Part VI.[353] Additionally, the manner in which a mobile device is induced to interact with an IMSI Catcher and then further induced to transmit mobile identifiers that it would not otherwise transmit may, as argued above, take such devices outside the functional definition of 'interception'. If this were the case, than Part

---

[349] *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16, per Abella, J; Craig Forcese, "Law, Logarithms and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives", in Michael Geist, *Ed*, *Privacy & Surveillance in Canada in the Post Snowden Era*, (Ottawa: University of Ottawa Press, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436615.

[350] *Criminal Code*, RSC 1985, c C-46, *s*ection 487.011, "Transmission Data".

[351] *R v Spencer*, [2014] 2 SCR 212, 2014 SCC 43 (must adopt purposive analysis when assessing privacy interest implicated); *R v Fegan*, [1993] 13 OR (3d) 88, (CA), para 39 (the communication of routing information and other metadata is between the customer and the communications service provider).

[352] *Criminal Code (Can) (Re)*, 2015 ABPC 178.

[353] However, this argument may not hold where the IMSI/IMEI is being obtained for the purpose of tracking a device associated with an individual or for the purpose of identifying a device as a source of a communication: *Criminal Code (Can) (Re)*, 2015 ABPC 178, para 30-31.

VI would likely not apply at all, for the same reasons, described in **Section Three: B-i** above, that might render the metadata interception mechanisms in the *Criminal Code* unavailable.

C. IMSI Catcher Use in Canada: Minimal Constitutional Standards?

Sub-section B, above, examined Canada's statutory framework for electronic surveillance in its potential application to the authorization of IMSI Catcher use. However, the *Charter* is likely to play a role in establishing minimum thresholds for IMSI Catcher authorization as well.

There are legitimate concerns that Canadian law enforcement agencies may fail to constrain their use of IMSI Catchers to legitimate parameters. Generally speaking, these concerns relate to whether state agencies' use of IMSI Catchers will conform to the law. As explored in more depth in following sub-sections, the *Criminal Code* includes a number of search powers that state agencies might rely upon to authorize their use of IMSI Catchers. However, unlike its counterparts in other jurisdictions such as the United States (such as the *Pen Register Statute*), which establish mandatory conditions to the privacy invasive activities they enable, most Canadian *Criminal Code* search powers are permissive. This means that state agencies can rely on the provisions to authorize privacy invasive activity, but are free to ignore their requirements unless the activity is otherwise prohibited by Part VI of the *Criminal Code* or by the *Charter*. It is therefore possible that state agencies might presume that they can deploy these devices without any judicial authorization at all.

This sub-section begins by examining how Canadian agencies have treated the acquisition of digital identifiers such as IMSI/IMEI numbers in the past. This examination implies that Canadian investigative agencies may be operating under the assumption that IMSI Catchers can be deployed without prior judicial or explicit lawful authorization. The remainder of this sub-section proceeds by presenting arguments for why the Canadian *Charter* likely requires prior juridical authorization as a pre-condition to deploying IMSI Catchers in non-exigent circumstances. It subsequently examines what additional minimal requirements the *Charter* might impose onto the authorization of IMSI Catcher use by state agencies.

i. Historical treatment of digital identifiers by Canadian agencies

When operating in Identification Mode, IMSI Catchers primarily capture digital identifiers (e.g. IMSI/IMEI numbers) which can then be correlated with particular

telecommunications subscribers.[354] Past attempts to legislate access to IMSI/IMEI identifiers have classified them as "subscriber information", more explicitly defined as "identifying information in [a] service provider's possession or control … that are associated with [a] subscriber's service and equipment".[355] When assessed in isolation, such identifiers are revealing of some, but not an immense amount of information about an individual. This has caused Canadian law enforcement and other agencies to previously argue for access to such information without prior authorization from a judge.

Indeed, Canadian law enforcement agencies have a history of treating such subscriber information as less sensitive and hence accessible to them with fewer barriers.[356] Bill C-30, which was withdrawn by the government on February 11, 2013 due to public resistance, sought to encode a new power that would allow law enforcement to compel disclosure of a long list of subscriber identifiers.[357] This power could have been invoked even without the need for suspicion that the information might assist in an investigation and without prior judicial authorization. After Bill C-30 was withdrawn, elements of it were reintroduced as Bill C-13.[358] These elements excluded the subscriber identification power, which was deemed to be too invasive.

Box 1: More Intrusive Than Your Typical Surveillance Technique

While all electronic surveillance can be characterized as inherently intrusive,[359] IMSI Catchers represent a particularly invasive tool.[360] Their invasiveness follows from their capacity for self-

[354] See discussion at *infra*, pp 2- 17.

[355] For example, Bill C-52, *Investigating and Preventing Criminal Electronic Communications Act*, (2010) 3rd Sess, 40th Parl, (First Reading), November 1, 2010, http://www.parl.gc.ca/content/hoc/Bills/403/Government/C-52/C-52_1/C-52_1.PDF, clause 16. First introduced as Bill C-47, *Technical Assistance for Law Enforcement in the 21st Century Act*, 2nd Sess, 40th Parl, (First Reading), June 18, 2009, http://www.parl.gc.ca/content/hoc/Bills/402/Government/C-47/C-47_1/C-47_1.PDF, clause 16; later incorporated in modified form into Part 1 of Bill C-30, 1st Sess 41st Parl, (First Reading), February 14, 2012, http://www.parl.gc.ca/content/hoc/Bills/411/Government/C-30/C-30_1/C-30_1.PDF, clause 2, enacting section 16 of the *Investigating and Preventing Criminal Electronic Communications Act*.

[356] For example, a program carried out in cooperation with major Canadian ISPs created an informal process by which law enforcement would request identifiers associated with anonymous online activity through an informal process that did not require any judicial or statutory authorization. The informal protocol is described in: *R v Ward*, 2012 ONCA 660, paras 36-38 and in Andrea Slane and Lisa M Austin. (2011). "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations," *Criminal Law Quarterly* 57, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2062404, pp 489 *et seq*.

[357] For more, see: Christopher Parsons. (2012). "The Issues Surrounding Subscriber Information in Bill C-30," *Technology, Thoughts, and Trinkets,* February 28, 2012, retrieved December 3, 2015, https://www.christopher-parsons.com/the-issues-surrounding-subscriber-information-in-bill-c-30/.

[358] Michael Geist. (2013). "Lawful Access is Back: Controversial Bill Returns Under the Guise of Cyber-Bullying Legislation," *Michael Geist*, November 20, 2013, retrieved December 3, 2015, http://www.michaelgeist.ca/2013/11/lawful-access-back-c-13/.

[359] *R v Duarte*, [1990] 1 SCR 30; See also: Necessary & Proportionate Coalition, *Necessary & Proportionate Principles*, (May 2014), https://necessaryandproportionate.org/principles.

[360] 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.

deployment (see **Box 4**), the inherent coarseness of their targeting mechanisms (see **Box 3**) and the quality of the data they acquire which, on its own may be innocuous but in practice provides the capacity to identify otherwise anonymous activity and to pervasively track individuals (see **Box 2**).

The ability for government agencies to self-deploy IMSI Catchers bypasses key safeguards that could temper any tendency to cast too wide a net when setting the intended scope of its deployment. Moreover, the manner in which IMSI Catchers capture information leads to significant collateral privacy impact as many non-targets are swept up alongside every legitimate target simply for being in the vicinity. Finally, the digital identifiers obtained by IMSI Catchers are persistent and can be used to uncover highly sensitive information about the private lives of individuals. These factors resonate to varying degrees depending on the different legal facets through which they are viewed but, collectively, they constitute a highly intrusive capacity.

While historically, the high cost of IMSI Catcher devices has served as a practical limitation on their quotidian usage, this cost has been rapidly dropping, leading to sharp increases in the volume of such use as well as in the nature of such use. These devices, which were once reserved to achieve national security objectives, are increasingly used as routine policing tools, in one instance even to investigate the alleged theft of a few chicken wings by a restaurant employee.[361]

However, law enforcement continued to rely on a program through which Canadian ISPs voluntarily provided access to some subscriber identifiers upon request. This program generated significant data requests.[362] In 2013, for example, transparency reports issued by mobile and home Internet and telephone companies reported that significant proportions of data requests related to subscriber identifiers and were issued without any prior judicial authorization.[363] In 2014, however, the Supreme Court of Canada ruled in *R v Spencer*, 2014 SCC 43[364] that Canada's privacy law, PIPEDA, prevents law enforcement from asking ISPs to voluntarily identify anonymous customers of their internet services. Following this decision, Canadian ISPs changed their policies such that Internet subscriber information is no longer generally available to law enforcement without a court order. Even lacking subscriber information, however, state agencies may (and presumably do) continue to collect some identifiers associated with subscribers, such as IP addresses in contexts where these are publicly

[361] Courtney Mabeus, 2016, "Battlefield Technology Gets Spotlight in Maryland Courts: Secrecy and Defence Concerns Surround Cell Phone Trackers", May 3, 2016, *Capital News Service*, http://cnsmaryland.org/interactives/spring-2016/maryland-police-cell-phone-trackers/index.html. 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/.

[362] See footnote 356, above. See also: Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians", *Telecom Transparency Project*, CC-BY-SA CA 2.5, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[363] For two of Canada's three largest providers of mobile and fixed Internet and voice, Rogers and TELUS, such requests constituted 38% and 39.5% of all requests, respectively: Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians", *Telecom Transparency Project*, CC-BY-SA CA 2.5, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf, Table 2 on pp 45-46.

[364] *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212.

transmitted to other peers.[365] To date, courts have not ruled directly on the *Charter* implications of collecting publicly transmitted identifiers. In some contexts, unauthorized collection of such identifiers could raise privacy concerns in the future, as it represents a substantial and salient step towards uncovering presumptively anonymous activity.[366] This would particularly be the case where state agencies have the ability to readily connect these identifiers to subscribers so as to reveal otherwise anonymous activity directly.[367]

Despite the *Spencer* decision, Canadian law enforcement agencies continue to seek access to subscriber information without a warrant. For example, in 2015, the Canadian Association of Chiefs of Police (CACP) adopted a resolution to "develop new legislation that supports the creation of a reasonable law designed to specifically provide law enforcement with the ability to obtain, in real-time or near real-time, [Basic Subscriber Information] from telecommunications providers."[368] Earlier the same year, the Canadian Department of Justice likewise issued a discussion paper that included as one of its suggestions the creation of a warrantless access power for subscriber information.[369] Canadian law enforcement agencies, then, continue to regard subscriber identifiers as less sensitive and, thus, requiring a lower level of privacy protection than other types of metadata or the 'content' of communications. It would not be surprising, then, if Canadian state agencies might consider it appropriate to use IMSI Catchers to obtain identifiers without prior judicial approval in some contexts. Indeed, one police officer has indicated in court documents his view that there is no reasonable expectation of privacy in digital identifiers broadcast by mobile phones to their mobile service providers, implying that no judicial authorization would be required to use an IMSI Catcher.[370]

Such an approach would, however, be mistaken. It is highly likely that the *Charter* requires prior judicial authorization as a pre-condition to deploying IMSI Catchers in non-exigent contexts. Further, to the extent that IMSI Catcher use constitutes an

---

[365] For example, from individuals connecting to peer-to-peer sites.

[366] See Office of the Privacy Commissioner of Canada, Technology Analysis Branch, "What an IP Address Can Reveal About You", May 2013, https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.pdf. For an example from the civil discovery context, see: *Warman v Wilkins-Fournier*, 2010 ONSC 2126 (Div Ct), particularly at paras 36-37.

[367] *R v Spencer*, [2014] 2 SCR 212, 2014 SCC 43.

[368] Canadian Association of Chiefs of Police (CACP). (2015). "Resolutions adopted at the 110th Annual Conference," CACP, August 2015, retrieved November 16, 2015, https://www.cacp.ca/index.html?asst_id=927.

[369] As mentioned in: Canadian Association of Chiefs of Police (CACP). (2015). "Resolutions adopted at the 110th Annual Conference," CACP, August 2015, retrieved November 16, 2015, https://www.cacp.ca/index.html?asst_id=927.

[370] Colin Freeze, 2016. "Case Sheds Light on How Police in Toronto Use 'Stingray' Surveillance", May 17, 2016, *Globe and Mail*, http://www.theglobeandmail.com/news/national/case-involving-first-documented-use-of-stingray-technology-in-toronto-goes-to-trial/article30057813/.

interception of private communications (as analyzed in the preceding section), its general use without judicial authorization is prohibited by Part VI of the *Criminal Code*.

ii. The Charter & Warrantless Access to Digital Identifiers

Under Canadian law, an investigative agency seeking to invade a reasonable expectation of privacy must rely on a lawful authority to do so.[371] The general rule is that in the absence of a statute justifying warrantless access, authorization will take the form of prior judicial authorization.[372] Exceptions to this general rule are limited to emergency or exigent circumstances,[373] the power to search an individual on arrest,[374] and the ancillary powers doctrine. The ancillary powers doctrine – a common law power that can provide police with lawful authority to interfere with privacy under some conditions – is most relevant to our discussion of IMSI Catchers as there is no general statute authorizing warrantless use of these devices. While emergency uses and 'on arrest' uses can be problematic,[375] these presumably represent more isolated uses and are outside the scope of this part of the report. It is noteworthy that, historically, some identifiers associated with communications have been considered 'less private' and, hence, obtainable without prior authorization. However, this historic approach does not fit the more sensitive and dynamic nature of modern digital communications.

IMSI Catchers collect vastly more data and under more ambiguous conditions than can be lawfully authorized under the common law ancillary powers doctrine. However, the broad surveillance capacities of IMSI Catchers are such that these fall outside of the proper parameters of the ancillary powers doctrine; as such, government agencies should be required to obtain judicial authorization as a precondition to using them in non-exigent contexts. This is because IMSI Catchers are deployed to identify individuals or to locate them and, in both instances, the Supreme Court of Canada has held that prior judicial authorization is required.[376]

---

[371] *R v Collins*, [1987] 1 SCR 265.

[372] *Hunter v Southam Inc*, [1984] 2 SCR 145; *R v Collins*, [1987] 1 SCR 265; *R v Cole*, [2012] 3 SCR 34, 2012 SCC 53, para 10.

[373] *R v Grant*, [1993] 3 SCR 223, paras 22-24 and 28-29; *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16.

[374] *Cloutier v Langlois*, [1990] 1 SCR 158; *R v Fearon*, [2014] 3 SCR 621, 2014 SCC 77.

[375] See for example: Chuck Grassley. (2014). "Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program," United States Senate, December 31, 2014, retrieved November 16, 2015, http://www.grassley.senate.gov/news/news-releases/leahy-grassley-press-administration-use-cell-phone-tracking-program, (stating concerns regarding the adoption of adequate privacy safeguards, particularly with respect to non-targets, when cell-site simulators are deployed *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16 (emergency interception powers justified, but must have some accountability measures built in).

[376] *R v Spencer*, [2014] 2 SCR 212, 2014 SCC 43; *R v Wise*, [1992] 1 SCR 526; 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.

As a starting point, some may argue that mobile device identifiers such as IMSI/IMEI and perhaps even device phone numbers do not attract reasonable expectations of privacy, regardless of the context or nature of their collection. Indeed, some have advanced the argument that such identifiers are not, in and of themselves, 'private' because the discrete items of information in question reveal little about any given individual.[377] Analyzed in isolation, a telephone number, for example, reveals little about its owner.[378] The argument which follows is that since these identifiers reveal little about an individual, their interception by state agencies is not constitutionally protected. Appellate courts have ultimately rejected the fragmented approach to assessing privacy interests which underpins the logic behind these decisions – that the privacy expectations attached to an item of data can be assessed in isolation of the otherwise anonymous activity it reveals.[379]

Box 2: Assessing the True Privacy Interest at Stake

The data obtained by IMSI Catchers constitutes device identifiers used by service providers to identify subscribers or, at times, to route calls and data to and from specific devices. In and of itself, the information is innocuous – a string of numbers.[380] However, courts assessing the privacy interest inherent in digital identifiers have increasingly adopted a purposive analysis that looks past the nature of the underlying number strings themselves and towards the information revealed by their collection.[381] As a result of the ubiquitous nature of mobile devices and the

[377] See: *R v Khan*, 2014 ONSC 5664; *R v Schertzer*, 2011 ONSC 220, para 25 and footnote 1; *R v Wilson*, [2009] OJ No 1067 (ONSC), para 26, 42 ("In my view, the Applicant had no reasonable expectation of privacy in the information provided by Bell considering the nature of that information. One's name and address or the name and address of your spouse are not "biographical information" one expects would be kept private from the state. It is information available to anyone in a public directory and it does not reveal, to use the words of Sopinka J. in Plant "intimate details of the lifestyle and personal choices or decisions of the applicant".."); *R v Friers*, 2008 ONCJ 740, paras 23 – 24 ("...account information, per se, reveals very little information about the personal lifestyle or private decisions of the occupants of the defendant's residence other than they have chosen to have some form of Internet connection installed in that residence. Moreover, the prevalence of wireless and hand-held technology makes a particular address an even less significant fact so far as internet use is concerned, since that use is no longer tied to a land line tied to a particular address. Like Lalande J. in R. v. Ward, I conclude that subscriber information is not core personal information.)"; *R v Spencer*, 2009 SKQB 341 (reversed on appeal to the Supreme Court of Canada), paras 14 and 17-18 ("The information...was 'tombstone' information of a general nature...I conclude that there is [no] expectations of privacy in a subscriber's name and address relating to the IP address issued by the internet service."); *R v McNeice*, 2010 BCSC 1544, para 49 (relying on *R v Wilson*); *R v Hutchings*, [1996] 83 BCAC 25 (BCCA).

[378] However, it must be noted that identifiers such as IMSI and IMEI do reveal some information even in isolation of their role as tools of identification: Christopher Parsons. (2011). "The Anatomy of Lawful Access Phone Records", *Technology, Thoughts & Trinkets*, November 21, 2011, https://www.christopher-parsons.com/the-anatomy-of-lawful-access-phone-records/.

[379] *R v Ward*, 2012 ONCA 660; *R v Trapp*, 2011 SKCA 143; *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212. Andrea Slane and Lisa M Austin. (2011). "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations," *Criminal Law Quarterly* 57, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2062404; Daphne Gilbert, Ian R Kerr & Jena McGill. (2007). "The Medium and the Message: Personal Privacy and the Force Marriage of Police and Telecommunications Providers", (2007) 51(4) *Crim L Q* 469, http://iankerr.ca/wp-content/uploads/2011/08/the_medium_and_the_message.pdf.

[380] Christopher Parsons, "The Anatomy of Lawful Access Phone Records", *Technology, Thoughts & Trinkets*, November 21, 2011, https://www.christopher-parsons.com/the-anatomy-of-lawful-access-phone-records/.

[381] *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212, paras 42, 47: "The privacy interest at stake in these examples is not simply the individual's name, but the link between the identified individual and the personal information provided anonymously. ... the identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in a person's name, address and telephone number found in the subscriber information."

persistent nature of mobile identifiers, these numerical strings therefore provide much more than a permanent digital address for a device – they implicate the capacity of device owners to act and move around anonymously.

Anonymity is rapidly becoming central to the maintenance of any meaningful level of privacy in our highly inter-connected world. It "permits individuals to act in public places but to preserve freedom from identification and surveillance."[382] In digital spaces, the "[a]nonymity of communications is one of the most important advances enabled by the Internet, and allows individuals to express themselves freely without fear of retribution or condemnation."[383] As our brick and mortar world becomes inundated with devices that leave a constant trail of digital footprints in the wake of our physical activities, preserving anonymity becomes as important as in the digital world.[384]

IMSI Catchers pose a particularly insidious threat to real-world anonymity. They may be deployed strategically to identify otherwise anonymous individuals at a political protest, or a public event on a controversial matter, chilling individuals' ability to form and express opinions by threatening their ability to do so anonymously.[385] They can be deployed to geolocate and identify individuals in private homes, to see who visits a medical clinic or a religious meeting, or to identify travelling companions. They can be deployed permanently at border crossings, airports or bus depots, or distributed at various points of a city so that movement becomes effectively impossible without a record of it being created.[386] They can also form the basis for merging real-world and digital activity – once obtained, they can be used to link anonymous online activity to the mobile device that generated it.[387] While some of this information may ultimately be innocuous, "[i]t remains that in a number of cases it will be quite sensitive."[388] Given the revealing potential of these devices, their strict regulation is integral.

While appellate courts have not applied the more robust privacy approach to assessments of mobile device identifiers at the time of writing, courts have recognized that, in spite of analogously low levels of privacy protection in telephone identifiers, this

[382] *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212, para 43.

[383] 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, paras 23 *et seq*.

[384] Article 29 Data Protection Working Party. (2011). "Opinion 13/2011 on Geolocation services on smart mobile devices," European Commission, Adopted on May 16, 2011, retrieved December 1, 2015, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, p 7.

[385] David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/29/32, May 22, 2015, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement, para 21.

[386] 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; UK DPA on ALPRs. *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212, para 44; UK Information Commissioner, Enforcement Notice, July 15, 2013, http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/hertfordshire-constabulary-enforcement-notice.pdf; 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.

[387] Citizen Lab. (2015). "The Many Identifiers in Our Pockets: A primer on mobile privacy and security," *Citizen Lab*, May 13, 2015, retrieved November 16, 2015, https://citizenlab.org/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/.

[388] *R v Rogers Communications*, 2016 ONSC 70, para 20. See also: *R v Vu*, [2013] 3 SCR 657, 2013 SCC 60; *Riley v California*, (2014) 573 US __ (Supreme Court of the United States).

area of law is currently 'evolving'.[389] With respect to identification of telephone account holders, for example, some courts have held that telephone activity does not attract the expectations of anonymity associated with online activity,[390] pointing specifically to the fact that most landline numbers are listed in publicly available telephone books or caller ID display.[391] However, this does not apply to mobile devices, where phone numbers are not listed in telephone books and where individuals are commonly advised to protect their phone numbers from the general public to avoid telemarketers and other unsolicited calls.[392] Mobile phone numbers and the names attached to them are often revealed when a phone call is made by means of Call Display, but this is selective and only to the specific individual called.[393]

More importantly, the privacy interest cannot be assessed in a fragmented manner that is divorced from its context. Where any identifier such as a telephone number or IMSI/IMEI number is being intercepted by a device such as an IMSI Catcher for the purpose of identifying an individual, the privacy interest at issue must encompass the otherwise anonymous activity thereby revealed.[394] IMSI Catchers are not used to capture subscriber identifiers for the purpose of contacting an individual associated with a telephone number. They are deployed to identify one or more otherwise anonymous individuals who are at a particular place at a particular time or to locate a known individual or set of individuals whose location is otherwise unknown. This privacy interest is one that *does* attract a reasonable expectation of privacy and, hence, is protected by section 8 of the *Charter*.[395]

The ancillary powers doctrine is a controversial element of Canadian common law.[396]

---

[389] *R v Khan*, 2014 ONSC 5664, para 27.

[390] *R v Khan*, 2014 ONSC 5664, paras 25, 27,

[391] *R v Khan*, 2014 ONSC 5664, parsa 23, 27; *R v Wilson*, [2009] OJ No 1067 (ONSC); *R v Friers*, 2008 ONCJ 740, para 23; *R v TELUS Communications Co*, 2015 ONSC 3964, paras 34-35.

[392] *R v Nguyen*, 2004 BCSC 76, para 15. Protecting one's mobile number from availability is a widely recommended means of avoiding spam: Joe Ducey, 2013. "How to Stop Scam Text Messages from Getting to your Cell Phone", January 28, 2013, *ABC15 News*, http://www.abc15.com/news/let-joe-know/how-to-stop-scam-text-messages-from-getting-to-your-cell-phone: "Scammers use special software that crawls websites like Facebook and Craiglist looking for phone numbers you post. Don't post phone numbers." Kim Boatman, "Stop Cell Phone Spam in Seven Easy Steps", *Norton by Symantec*, Retrieved April 22, 2016, https://us.norton.com/yoursecurityresource/detail.jsp?aid=CellPhone: "*Guard your number*. "Be really careful who you share it with," says Neill. Too often, says Neill, we share our number without thinking about who might have access to that information. For instance, be cautious about listing it in public forums, such as social networking sites or on other information you post online. A simple listing in a membership directory could have unwanted consequences."; CRTC, 2014. "What You Should Know About Telemarketing in Canada", Last Modified November 26, 2014, http://crtc.gc.ca/eng/info_sht/t1048.htm: "To lessen the chances of a telemarketer getting your number: Be careful about providing your number to anyone".

[393] *R v TELUS Communications Co*, 2015 ONSC 3964, paras 34-35.

[394] *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212.

[395] *R v Wise*, [1992] 1 SCR 527 (coarse electronic surveillance of public movement attracts reasonable expectation of privacy).

[396] While adopted from other common law jurisdictions, the common law ancillary powers doctrine has arguably received expansive treatment in Canada, and has been criticized on this basis. See, for example: Steve Coughlan, 2007, "Common Law Police Powers and

Under this doctrine, state agencies are lawfully authorized to carry out some invasions of individual privacy in situations where seeking prior judicial authorization would be an unreasonable precondition to carrying out a police duty (i.e. where an immediate search is necessary to carry out a legitimate police duty) and where the resulting privacy invasion is not overly intrusive.[397] For example, the doctrine has been used to justify the use of drug-detection dogs. Even though tele-warrants are available expeditiously, requiring these as a precondition was seen as antithetical to the quick action and 'on-the-spot' nature of drug detection dog use, rendering their deployment ineffective.[398] However, IMSI Catchers are highly distinct from drug-detection dogs. Unlike drug-detection dogs,[399] their use is highly surreptitious and as such not subject to direct challenge or scrutiny by those who are being surveiled.[400] Moreover, while most electronic surveillance tools raise issues best addressed by a nuanced process capable of restraining their more invasive capabilities, IMSI Catchers present particular challenges. As an examination of the capacities of such devices (referred to as cell-site simulators) by a US District Court concluded:

> … cell-site simulator is simply too powerful of a device to be used and the information captured by it too vast to allow its use without specific authorization from a fully informed court.[401]

This invasive capacity suggests that law enforcement cannot be entrusted to deploy IMSI Catchers without excessively intruding on individual privacy or to properly calculate and mitigate the collateral capture of innocent mobile devices that are inevitably intercepted alongside the few legitimately targeted devices.

Box 3: Collateral Privacy Impact

Much like the cell towers they are designed to mimic, IMSI Catchers are not designed for targeted acquisition of signals emerging from specific devices. Rather, they are designed to receive all relevant signals within reach. This inherently coarse interception technique means that even if a given deployment is *intended* to be narrowly tailored (if police seek to identify one specific

---

the Rule of Law", (2007) 47 CR (6th) 266; Steve Coughlan, 2012, "Charter Protection against Unlawful Police Action: Less Black and White than it Seems" (2012) 57 *SCRL* (2d) 205; James Stribopoulos, 2005, "In Search of Dialogue: The Supreme Court, Police Powers and the Charter", (2005) 31 *Queen's L J* 1; Tim Quigley, 2008, "The Impact of the Charter on the Law of Search and Seizure", (2008) 40 *SCLR* 117; *R v Kang-Brown*, [2008] 1 SCR 456, 2008 SCC 18, per LeBel, J.

[397] *R v Kelsy*, 2011 ONCA 605; see also *R v MacDonald*, [2014] 1 SCR 37, 2014 SCC 3, paras 31, 37-43 ("…the police power to search is not unlimited. This power is constrained by a requirement of objectively verifiable necessity." See, regarding general limits of common law doctrines to authorize deviations from the general requirement for prior judicial authorization: CIPPIC, Factum of the Intervener, *R v Fearon*, SCC File No 35298, April 17th, 2014, https://cippic.ca/uploads/Fearon-Factum.pdf, para 7.

[398] *R v AM*, [2008] 1 SCR 569, 2008 SCC 19, para 90.

[399] See: *R v Kang-Brown*, 2008 SCC 18, para 54.

[400] *R v Tse*, [2012] 1 SCR 351, 2012 SCC 16.

[401] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

individual, for example) the intrusion will be significantly greater because the device will capture signals from all mobile devices in range. Some of these device identifiers will be emanating from private spaces such as people's homes.[402] It is legally ambiguous whether law enforcement agencies are under any obligation to delete the numerous untargeted identifiers it captures alongside each legitimate IMSI Cather target[403] and the government has recently taken steps to greatly expand the conditions under which any information, once obtained, can be shared within government for a range of unrelated purposes.[404]

As such it is unclear whether state agencies which deploy these devices will retain and make use of all collaterally captured digital identifiers,[405] at least in the absence of clear legislative, regulatory or judicial obligations to not use data in this way.[406] (The RCMP has implied in court documents that it intends to keep non-targeted digital identifiers obtained with IMSI Catchers indefinitely).[407] It should come as no surprise, then, that other jurisdictions have imposed strict restrictions mandating the expeditious deletion of untargeted data collaterally obtained by IMSI Catchers.[408]

The quality of information obtained by IMSI Catchers is also more sensitive and dynamic than that obtained from drug detection dogs. Unlike the latter, information obtained by IMSI Catchers – including collaterally captured information of non-targeted individuals – is not limited in scope to a binary 'yes / no' response to a single information query (e.g. might there be drugs present?).[409] The identifiers intercepted by IMSI Catchers are permanently linked to a device, meaning the identifiers can be used on an ongoing basis to obtain a dynamic and difficult to predict range of information. This includes the ability to cross-reference different locations wherein the identified device appears, and the

[402] See for example: *State v Tate*, 357 Wis 2d 271 (2014) (Supreme Court of Wisconsin), pp 23-24: "… when law enforcement contemplates tracking a cell phone, they may not know whether the phone is located in a private residence, which stands at the 'very core' of the Fourth Amendment, or is traveling down a public highway…" See also: *Maryland v Andrews*, (2016) *Md App LEXIS 33, File No 1496 (Md Ct of Special Appeals): "It would be impractical to fashion a rule prohibiting a warrantless search only retrospectively based on the fact that the search resulted in locating the cell phone inside a home or some other constitutionally protected area."

[403] *R v Rogers Communications*, 2016 ONSC 70, paras 59-60.

[404] Kent Roach & Craig Forcese, "Bill C-51 Backgrounder #3: Sharing Information and Lost Lessons from the Maher Arar Experience", *SSRN*, 18 February, 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2565886; Canadian Internet Policy & Public Interest Clinic, OpenMedia.ca & Canadian Journalists for Free Expression, "A Primer", April 2015, https://cippic.ca/uploads/BillC51-APrimer.pdf.

[405] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div), "States or any government body. 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."

[406] For an example of regulatory guidance of this type see: Office of the Information and Privacy Commissioner for British Columbia, Investigative Report F12-04, *Use of Automated License Plate Recognition Technology by the Victoria Police Department*, November 15, 2012, pp 10, 23-24.

[407] Jordan Pearson, 2016. "The RCMP Surveilled Thousands of Innocent Canadians for a Decade", June 10, 2016, *Motherboard (VICE)*, https://motherboard.vice.com/read/the-rcmp-surveilled-thousands-of-innocent-canadians-for-a-decade.

[408] See **Table 5: Minimization & Targeting Obligations for IMSI Catcher Use** on p 121 below, for a summary of the sources of these retention limitation obligations.

[409] *R v Kang-Brown*, [2008] 1 SCR 456, 2008 SCC 18, per Binnie, J, para 58 ("… because of the minimal intrusion, contraband-specific nature and pinpoint accuracy of a sniff executed by a trained and well-handled dog … a proper balance between an individual's s. 8 rights and the reasonable demands of law enforcement would be struck by permitting such "sniff" searches … without requiring prior judicial authorization.")

ability to identify anonymous online activity associated with a particular device.[410] Strategically located IMSI Catchers can pervasively track any specific individual or even all individuals in a given region. The devices could also be used to track all attendees at events that suggest sensitive political, religious, or other preferences by strategically setting IMSI Catchers outside specific events or other notable places of congregation. Finally, information obtained by IMSI Catchers can be used to identify individuals associated with a particular device.[411] The information obtained by drug detection dogs, by contrast, is a known commodity that can be assessed in advance, and is limited to revealing the presence or absence of drug residue. As such, granting law enforcement the ability to deploy IMSI Catchers without prior authorization is akin to signing a blank check; it is simply impossible to predict what data will be obtained as a result, or the inferences that will be derived from this data.

The identifiers captured by these devices share many features with IP addresses as well as with geo-locational information such as that generated by a tracking device. In other jurisdictions, some have argued that tracking of public location does not implicate a reasonable expectation of privacy and therefore attract constitutional protection, even coarse location information obtained by historical tracking devices has long been recognized as constitutionally protected in Canada.[412] Indeed, as explained in **Section One**, the information obtained by IMSI Catchers is far more detailed and sensitive than what could be obtained from a historical tracking device, justifying higher, not lower, levels of protection.

At minimum, however, where an IMSI Catcher is deployed to geo-locate individuals at a particular location at a particular time, prior judicial authorization is required under Canadian law, even if the place in question is public.[413] Moreover, IMSI Catchers operate through walls and, hence, can locate individuals in private places as well.[414] Additionally, IMSI Catcher use will often implicated the 'anonymity' privacy interest, as

---

[410] Adam Senft, Andrew Hilts, Christopher Parsons, Jakub Dalek, Jason Q. Ng, John Scott-Railton, Katie Kleemola, Masashi Crete-Nishihata, Ron Deibert, Sarah McKune. (2015). "A Chatty Squirrel: Privacy and Security Issues with UC Browser," *Citizen Lab*, May 21, 2015, retrieved November 30, 2015, https://citizenlab.org/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/.

[411] Infra, **Section One**.

[412] *R v Wise*, [1992] 1 SCR 527; See comprehensive review of case law in: 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.

[413] *R v Wise*, [1992] 1 SCR 527, *R v Mahmood*, 2011 ONCA 693.

[414] *State v Tate*, 357 Wis 2d 271 (2014) (Supreme Court of Wisconsin), pp 23-24: "Further complicating the matter is the location of the cell phone. For example, when law enforcement contemplates tracking a cell phone, they may not know whether the phone is located in a private residence, which stands at the "very core" of the Fourth Amendment, or is traveling down a public highway, in which case a defendant may have no expectation of privacy in his movements. Finally, even movements in public areas can reveal highly personal information such as "familial, political, professional, religious, and sexual associations," which if monitored too closely, may "chill[] associational and expressive freedoms.""

they will identify otherwise anonymous activity based on digital identifiers. Canadian courts have held in the context of online identifiers such as IP addresses that the common law ancillary power does *not* extend to such data access when it might reveal sensitive anonymous activity.[415] All in all, the identifiers obtained by IMSI Catchers can be correlated to a range of activities and, thus, are capable of providing a comprehensive picture of an individual's life.

Finally, as explained above, IMSI Catchers present immense potential for overbroad privacy invasion because they impact on the privacy of everyone in the vicinity of a legitimate 'target' or, alternatively, if law enforcement purposefully deploy these devices in an overly aggressive manner. Collateral impact is inherent in the functioning of IMSI Catchers, which, by design, capture all IMSI/IMEI numbers in a given vicinity. Unless affirmative action is taken to delete non-targeted identifiers they will be retained and remain available to state agencies for later use. Indeed, some Canadian agencies have asserted their intention to retain such collaterally captured identifiers indefinitely.[416] By contrast, much more targeted searches are possible where law enforcement rely on obtaining comparable data directly from a service provider.[417] As a result, the collateral privacy impact of IMSI Catcher deployment is high and should be objectively determined by a court.

The lack of objective prior authorization is also likely to lead to intended (as opposed to collateral) disproportionate over-deployment. For example, a police force in Ontario sought an order to compel two Canadian providers to produce mobile device identifiers associated with 21 mobile service towers in the vicinity of a single crime, affecting over 40,000 individuals (other service providers may have received similar orders, but did not challenge the order so it is unknown how many additional individuals were implicated).[418] When the two service providers in question (TELUS Communications Co and Rogers Communications Partnership) challenged the order as excessively broad the law enforcement agency sought to withdraw the expansive request on its own initiative and replace it with a significantly more tailored (yet still seemingly sufficient) one that only implicated 6 cell towers.[419] If law enforcement

[415] *R v Spencer*, [2014] 2 SCR 212, 2014 SCC 43, at paras 71-73; *R v Collins*, [1987] 1 SCR 265.

[416] Jordan Pearson, 2016. "The RCMP Surveilled Thousands of Innocent Canadians for a Decade", June 10, 2016, *Motherboard (VICE)*, https://motherboard.vice.com/read/the-rcmp-surveilled-thousands-of-innocent-canadians-for-a-decade.

[417] *R v Rogers Communications*, 2016 ONSC 70, paras 58 and 65 (e)

[418] *R v Rogers Communications Partnership*, 2014 ONSC 3853, para 11.

[419] *R v Rogers Communications Partnership*, 2014 ONSC 3853, paras 1-3, but contrast para 23. It could be that the replacement order was facilitated by progression in the investigation revealing additional information that permitted a more targeted approach. However, given the significant change in impact on innocent third party privacy, production orders *should* be calibrated to require these steps be taken (or at least attempted) prior to the issuance of excessively broad production orders.

sought to obtain the same information – to discover who will be in the same vicinity over the same period of time – they could have done so by deploying IMSI Catchers at the 21 cell tower locations on their own authority and the opportunity for an objective decision-maker to impose a more tailored approach would be lost. Other examples are likely to arise in the future. Whether disproportionately broad deployment results from collateral or intentional impacts, it is notable that there is no obligation to notify individuals whose privacy is ultimately affected and that, given the surreptitious nature of IMSI Catcher operation, there is no guarantee that excessive deployments will be challenged.[420]

Box 4: Direct & Unmediated Access to Data

As IMSI Catchers simulate cellular towers, the information they obtain in identification mode is comparable to what state agencies could obtain from companies operating actual towers in the locale in question.[421] However, direct deployment by law enforcement agencies renders the search more intrusive. To begin, the mere presence of an intermediary such as a service provider allows for more tailored searches because service providers can sift data from mobile towers so that only what is relevant is disclosed, thus reducing collateral privacy impact.[422]

Second, while electronic surveillance of this type is equally surreptitious and invisible to those whose privacy is affected regardless of whether the information is obtained from a service provider or directly by means of an IMSI Catcher, a service provider at least has the option of challenging excessively broad surveillance attempts.[423] This can lead to a more narrowly tailored (but equally effective) search,[424] to the imposition of important safeguards,[425] and to more accurate assessments of what might properly constitute exigent circumstances triggering emergency interception powers.[426] Relying on an intermediary can also provide an added measure of transparency, as they provide an independent record of the scope and nature of electronic surveillance as well as an avenue for potentially obtaining more individualized information regarding potential privacy invasions.[427]

---

[420] *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16; *R v Rogers Communications Partnership*, 2014 ONSC 3853, paras 39, 41.

[421] See **Table 2: Relevant Production Orders** on p 76, below, for examples of the production powers that might be used to access comparable data. See also: *In re Application for Cell Tower Records Under 18 USC §2703(D)*, (2015) 90 F.Supp.3d 673 (Southern District of Texas, Houston Division): "A further word is necessary to avoid possible misunderstanding. This holding has no application to a related though very different investigative technique using a device known as a cell site simulator, sometimes referred to as a 'StingRay.' Like a cell tower dump, the StingRay device may be used to discover telephone and other identification numbers of wireless devices in a given location. However, there are several critical differences: (1) the device is deployed by law enforcement, not the provider; (2) the information obtained is transmitted in real time directly to law enforcement, not retrospectively via the provider's records; and (3) the device allows continuous real time tracking of the wireless devices in contact with it."

[422] See for example, *R v Rogers Communications*, 2016 ONSC 70. Note, in other contexts, use of an intermediary may be more intrusive, as it would permit the collection of richer datasets with less practical effort on the side of state agencies.

[423] *R v Rogers Communications Partnership*, 2014 ONSC 3853, paras 1-3. See also: *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16 and contrast:

[424] *R v Rogers Communications*, 2016 ONSC 70.

[425] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div), but see *R v Rogers Communications*, 2016 ONSC 70, contra.

[426] See discussion at footnote 236, on p 53, *supra*.

[427] Office of the Privacy Commissioner of Canada, "Transparency Reporting by Private Companies", June 2015,

Unlike drug detection dogs, deployment of IMSI Catchers will not be constrained to appropriate boundaries in the absence of prior judicial authorization, or even an explicit legislative regime. Letting law enforcement agencies rely on the common law ancillary search power as lawful authority for IMSI Catcher deployment would therefore be highly inappropriate in light of the lack of any demonstrable necessity, the sensitivity of the data obtained (i.e. the intrusiveness of the search), and the high potential for over-reach through collateral and intentional impact. Including IMSI Catcher use within the ancillary powers doctrine would amount to granting such agencies carte blanche to determine proper parameters of such surveillance. On the other hand, requiring independent lawful authorization would provide an avenue for the courts or parliament to proactively address the potential for excess inherent in this surveillance technology, as was the case in Germany, while forestalling the missteps that occurred in the United States prior to the recent adoption of internal policy and judicial constraints.[428]

iii. The Charter & Minimal Permitted Authorization Standard

In addition to requiring judicial authorization as a pre-requisite for IMSI Catcher deployment, the *Charter* is likely to impose additional limitations on the use of these devices. It likely requires that the constitutional standard established in *Hunter v Southam* as a pre-requisite evidentiary basis for privacy violation be met. This would entail establishing 'reasonable belief' that a crime has been (or will be) committed and that the anticipated privacy invasion will provide evidence of that crime. In addition, respect for *Charter* principles requires the imposition of additional minimal safeguards to ensure that IMSI Catcher deployment remains reasonable. This sub-section examines these two requirements before turning to a comprehensive set of best practices in **Section Four**.

We note at the outset that many of the powers explored above would not meet this constitutional minimum. Notably, the Transmission Data and 'Object Tracking' powers highlighted in Table 1, above, do not employ a sufficiently robust evidentiary standard, allowing for authorization to occur on the basis of 'reasonable suspicion' in lieu of 'reasonable belief'. All of the electronic surveillance powers canvassed above, however, fall short in that they lack specific safeguards necessary to curtail the more intrusive features of IMSI Catchers. The Part VI framework most closely approximates these safeguards, but each of the available authorization regimes would require the imposition of at least some additional safeguards.

---

https://www.priv.gc.ca/information/research-recherche/2015/transp_201506_e.pdf; Access Now, "Transparency Reporting Index", Last Updated February 18, 2016, https://www.accessnow.org/transparency-reporting-index/.

[428] See **Section Three: A** and **Section Two: A**, above, for a description of these developments.

Baseline Constitutional Standard of Proof: Reasonable Grounds to Believe

The 'reasonable suspicion' standard is significantly less rigorous than the baseline standard of 'reasonable belief'. This means that it is "inexorabl[e] … that more innocent persons will be caught under a reasonable suspicion standard than under the reasonable and probable grounds standard."[429] (Note this does not mean that more innocent non-targeted individuals can be *collaterally* impacted, only that the standard is permissive enough so that more innocent individuals will become legitimate 'targets' for privacy invasion). A reasonable suspicion can arise where it is possible that a privacy invasion might provide evidence of an offence, without taking into account whether such an outcome is in fact *probable*.[430] In recognition of this greater breadth of intrusiveness, the lower standard is only available where the privacy invasion contemplated is minimal.[431]

As noted above, the *Criminal Code's* metadata interception framework applies to transmission data (section 492.2) and to tracking data (492.1), each of which might potentially be relied upon by state agencies seeking to authorize IMSI Catcher use. This framework allows state agencies to intercept tracking data related to an object or transmission data on the basis of a reasonable suspicion, while requiring reasonable belief for the interception of tracking data from an object closely associated with an individual.[432] IMSI/IMEI-based tracking or subscriber identification is more invasive than historical uses of these powers and should therefore be premised on a reasonable belief standard, at minimum. Before turning to an analysis of IMSI Catchers specifically, it is useful to place historical case law relating to the use of the reasonable suspicion standard in sections 492.1 and 492.2 in its modern context.

The historic justification for employing a lower 'reasonable suspicion' standard when intercepting calling records under section 492.2 (typically by use of a 'digital number recorder' or "DNR") was summarized by the Québec Court of Appeal in *R v Cody*, the leading case on the matter:

> … DNR records are used to confirm previous intelligence and to support physical surveillance being carried out simultaneously. For instance, if the subject of physical surveillance is lost, phone calls made by the subject on his cell phone can be used to indicate the area of the city or the county that the subject is in, enabling the surveillance team to recommence physical surveillance of the subject with little delay. … DNR

[429] *R v MacKenzie*, [2013] 3 SCR 250, 2013 SCC 50, para 85.

[430] *R v MacKenzie*, [2013] 3 SCR 250, 2013 SCC 50, para 74. See discussion in *R v MacDonald*, [2014] 1 SCR 37, 2014 SCC 3, per Moldaver and Wagner, JJ, concurring but not on this point.

[431] *R v AM*, [2008] 1 SCR 569, 2008 SCC 19, para 86; *R v Nguyen*, 2004 BCSC 76, paras 26, 30; *R v Mahmood*, 2011 ONCA 693, para127 – 131.

[432] Infra, **Section One**.

> records, also can lead eventually to other, more specific, methods of investigation. For instance, wiretapping and searches can be carried out, with warrants, once the DNR information confirms or corroborates associations between suspected persons.
>
> … DNR records … are what can be referred to as "indicators of lifestyle", indicators of the lifestyle of the subject. This is similar to the information which is collected by observing the subject through physical surveillance - what stores or restaurants he frequents, where he goes for a haircut, where his children go to school.[433]

The key factors here relate to the fact that 492.2 does not reveal information beyond what can be confirmed by physical surveillance of an individual, or that the information revealed relates to less sensitive aspects of life such as which restaurants an individual prefers, who cuts her hair, and who she associates with. Other decisions have stated that while information typically obtained by 492.2 can reveal intimate lifestyle details, this only occurs when the information itself is correlated with other (often publicly available) information such as by looking up destination telephone numbers or addresses from which phone calls were made.[434] The fact that telecommunications services are a regulated activity and that any location information obtained by section 492.2 DNRs is typically 'coarse' have also been pointed to as underpinning the purportedly less intrusive nature of this power.[435]

While it is questionable whether this type of associational or tracking data was ever *truly* as non-invasive as some courts have claimed, social and technical changes since that time have placed mobile devices at the centre of our lives. The consequence is that there is an increased invasive capacity associated with surveillance mechanisms which target such devices.[436] This invasive capacity is even more significant when modern data mining techniques are accounted for.[437] Even a single call record (who phoned whom and from where) has now been shown to be capable of, and even likely to, reveal sensitive biographical information.[438] For example, one study

---

[433] *R v Cody*, 2007 QCCA 1276, para 14, 16, quoting the court below, at *R v Whitman-Langille*, [2004] QJ No 14164 (Que SC), paras 5, 7 and 20, with approval.

[434] *R v Mahmood*, 2011 ONCA 693, paras 127-131.

[435] *R v Mahmood*, 2011 ONCA 693, paras 127-131.

[436] *R v Foster*, 2013 ONCJ 723, para 36: "The overwhelming and ubiquitous use of cellphones, the advance cellphone technology and the extent of information that can be obtained about cellphones and the people who use them may permit such information to reveal personal information and biographical information about the users such as the identification of movement, who the person associates with and the frequency of such contact."

[437] An Amicus brief signed by close to 20 experts technical experts recently outlined two of these analytic capacities: social graphing and predictive analytics: Brief *Amici Curiae* of Experts in Computer Science and Data Science in Support of Appellant Under Seal, March 31, 2014, in *Under Seal v Holder*, Case No 13-16732, United States Court of Appeal for the Ninth Circuit, https://www.eff.org/document/experts-computer-and-data-science-amici-brief-0. See also: Declaration of Professor Edward W. Felten: https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf

[438] Brief *Amici Curiae* of Experts in Computer Science and Data Science in Support of Appellant Under Seal, March 31, 2014, in *Under*

analyzed 33,688 unique numbers contacted on mobile devices by the 546 study participants over a 5 month period. The study found a very high incidence of facially sensitive information revealed by single calls within this data set, concluding:

> The degree of sensitivity among contacts took us aback. Participants had calls with Alcoholics Anonymous, gun stores, NARAL Pro-Choice, labor unions, divorce lawyers, sexually transmitted disease clinics, a Canadian import pharmacy, strip clubs, and much more. This was not a hypothetical parade of horribles. These were simple inferences, about real phone users, that could trivially be made on a large scale.[439]

In addition, the fragmented approach to assessing privacy expectations, which assess units of information such as DNR records in isolation of the richer information that these records will ultimately reveal when combined with common sources of information, has been rejected.[440] Such developments and evidence regarding modern usage of mobile devices has challenged the historical claim that associational information such as that intercepted by DNRs under section 492.2 of the *Criminal Code* is, indeed, non-intimate and by extension that it can be constitutionally obtained by means of a reasonable suspicion authorization.

The geo-location data intercepted or obtained by devices installed under section 492.1 of the *Criminal Code* (and also sometimes inferred from use of number recorders under section 492.2) has also received historically permissive treatment under the assumption that such data is non-sensitive. Section 492.1 was initially adopted in response to the Supreme Court of Canada's decision in *R v Wise*, [1992] 1 SCR 527, which recognized that the use of tracking devices to electronically track individuals travelling in public spaces implicates the *Charter* and requires judicial authorization. The tracking device employed in *Wise* to track the public movements of a suspect's car were held to attract lower expectations of privacy on the basis that the location information it disclosed was very coarse, related to a regulated activity (operation of a motor vehicle), and could only work effectively as an aide to physical surveillance, and not as an independent source of tracking:

> It has been seen that there is a reduced expectation of privacy by those using a motor vehicle. In addition, the intrusion on any remaining expectation of privacy as a result of the device used in this case is minimal. This particular beeper was a very rudimentary extension of physical surveillance. It must be remembered as well that

---

Seal v Holder, Case No 13-16732, United States Court of Appeal for the Ninth Circuit, https://www.eff.org/document/experts-computer-and-data-science-amici-brief-0, pp 17-22.

[439] Jonathan Mayer & Patrick Mutchler, "MetaPhone: The Sensitivity of Telephone Metadata", *Web Policy*, 12 March, 2014, http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

[440] See discussion in **Section Three: C-ii.**

> the device was attached to the appellant's vehicle, not to the appellant. How very different a device such as this is, in its operation and in its effect on the individual, from a hidden video camera or an electronic monitor that surreptitiously intercepts private communications.[441]

This reasoning exhibits several commonalities with the rationale for classifying 492.2 as a 'less intrusive' power. The location information obtained is coarse, and only capable of supplementing physical surveillance. The activity being monitored is regulated (in this instance, driving a car).

Much as with information regularly intercepted under 492.2 authorization, recent technical, social and academic developments have increasingly recognized the more intrusive nature of location information. A clear explanation of this sensitivity can be found in a decision of the United States Court of Appeal for the District of Columbia Circuit (narrowed on appeal):

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts.[442]

The pervasive availability of geo-locational information emitted by most mobile devices has increased the invasiveness of the resulting picture that can be painted of individuals' lives. Further, the precision of geo-location information emitted by today's mobile devices is such that tracking can occur independently of any physical surveillance. Finally, while access to telecommunications services is a regulated activity in Canada, the nature of the regulation is different in nature from that relating to vehicles. Telecommunications regulation attracts to the activities of service providers, not individuals, whereas vehicle regulation relates specifically to vehicle operation by the individual whose privacy is being invaded. It is an inapt analogy to

---

[441] *R v Wise*, [1992] 1 SCR 527, per Cory, J, pp 533-536.

[442] *US v Maynard*, 615 F.3d 544 (US DC Circ, CA), p. 562. Narrowed on appeal in *US v Jones*, (2012) 565 US __ (Supreme Court of the United States).

say that regulation of telecommunications service providers can in some way reduce the privacy expectations of customers of those services as those customers have not undertaken regulated activities.[443] It is perhaps these differences that have underpinned Parliament's decision to bifurcate section 492.1 in amendments to the *Criminal Code* adopted in Bill C-13. As detailed above, the newly bifurcated section 492.1 retains the lower 'reasonable suspicion' standard when tracking data associated with an object is intercepted, but eschews it in favour of the higher reasonable belief standard when this information is emitted by a device closely associated with an individual.[444]

With these limitations of the historical case law in mind, it is important to note that IMSI Catchers obtain sensitive information and are more intrusive in nature than other devices used under sections 492.1 and 492.2 in the examples from the case law referenced above. The capacities of Digital Number Recorders were described by the Ontario Court of Appeal in *R v Fegan* as such:

> A digital number recorder (DNR) is activated when the subscriber's telephone is taken "off the hook". Electronic impulses emitted from the monitored telephone are recorded on a computer printout tape which discloses the telephone number dialled when an outgoing call is placed. The DNR does not record whether the receiving telephone was answered nor the fact or substance of the conversation, if any, which then ensues. When an incoming call is made to the monitored telephone, the DNR records only that the monitored telephone is "off the hook" when answered and the length of time during which the monitored telephone is in that position.[445]

The information intercepted by IMSI Catchers, by contrast, is emitted at all times by mobile devices as the individuals associated with them traverse public or private spaces. While DNRs are 'number specific', IMSI Catchers are not and intercept all identifiers transmitted within range. The persistent nature of IMSI/IMEIs as identifiers also means that they can provide an ongoing source of information regarding the account holder with whom they are associated. More to the point, however, IMSI Catchers are most properly assessed as a geo-location tool as state agencies will almost exclusively uses these devices to identify an individual or set of individuals in a single or multiple

---

[443] *R v Mahmood*, 2011 ONCA 693, paras 128,

[444] Note that while the fact that Parliament has set a particular standard for a particular interception should not in and of itself undermine normative expectations of privacy, the Ontario Court of Appeal has twice relied upon the fact that section 492.2 adopts a reasonable suspicion standard as evidence that this standard provides appropriate constitutional protection under section 8 of the *Charter*: *R v Mahmood*, 2011 ONCA 693, paras 130-131; *R v M(B)*, [1998] 42 OR (3d) 1 (CA), para 62.

[445] *R v Fegan*, [1993] 13 OR (3d) 88 (CA), para 19; *R v Cody*, 2007 QCCA 1276, para 11.

locations. Therefore their authorization more appropriately falls within 492.1.[446]

As a tracking tool, IMSI Catchers operate with precision.[447] Once set up in a particular location or set of strategic locations, the tracking they facilitate need not be used as a supplement to physical surveillance, but can operate independently. Moreover, the identifying capacity that intercepted mobile identifiers provide is well beyond what can be obtained by physical surveillance alone. Further, the mass surveillance capacity of these devices facilitates a magnitude of tracking that could not be done with physical surveillance alone – all individuals in a given locale are geo-located. Also, IMSI/IMEI are closely associated with mobile devices that individuals keep on their person at all times. Courts have held, perhaps questionably, that the adoption by parliament of a particular standard for a particular type of activity can act as recognition that such a standard is constitutionally required by section 8.[448] In Bill C-13, Parliament has recognized that tracking of individuals implicated greater privacy expectations and demands a higher standard as a precursor to privacy invasion. This should be seen as further evidence that geo-location of individuals constitutes an intrusive activity that requires higher levels of privacy protection under the *Charter*.

A final factor that affects the intrusiveness of IMSI Catchers is that these devices indiscriminately obtain location information from public *and* private places. While movement through public spaces may or may not attract lower expectations of privacy, this is not the case for information located inside the home.[449] Yet IMSI Catchers will often reveal the identity and location of individuals within private domiciles. Even where a state agency seeks to deploy an IMSI Catcher against a specific, known target, the agency is unlikely to know where the individual's device will be located at the time the IMSI Catcher is deployed, meaning the information obtained, as recently noted by a US court:

> … when law enforcement contemplates tracking a cell phone, they may not know whether the phone is located in a private residence, which stands at the "very core"

---

[446] Some US courts have reached similar conclusions: *In the Matter of Application for Cell Tower Records Under 18 USC 2703(d)*, 90 F.Supp.3d 673, (2015)(S Dist Texas)(though cell site simulator obtains similar data to a tower dump, it requires a probable cause tracking warrant); *United States v Espudo*, 954 F.Supp.2d 1029, (2013)(S Dist Calif)("Therefore, a warrant to obtain real-time cell site location data may only be granted if the Government makes a showing of probable cause."); *Tracey v State*, 152 So.3d 504, (2014) (Supreme Court of Florida)(access to real-time cell-site information attracts reasonable expectation of privacy, requires probable cause based warrant); *Commonwealth v Augustine*, 467 Mass. 230 (2014)(Supreme Court of Massachusetts)(reasonable expectation of privacy in production of two weeks of historical cell-site information requiring probable cause-based warrant).

[447] See discussion, in **Section One**, above, of: 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, http://www.nature.com/articles/srep01376.

[448] *R v Lee*, 207 ABQB 767, para 283; *R v M(B)*, [1998] 42 OR (3d) 1 (CA), para 62; *R v Mahmood*, 2011 ONCA 693, paras 130-131.

[449] *R v Tessling*. [2004] 3 SCR 432, 2004 SCC 67.See also: Ian R Kerr & Jenna McGill, "Emanations, Snoop Dogs and Reasonable Expectations of Privacy", (2007) 52(3) *Crim L Q* 392.

> of the Fourth Amendment, or is traveling down a public highway…[450]

Historically, this was not a factor when assessing the intrusiveness of a digital number recorder, as telephones were inextricably linked (often publicly, in a telephone book) to a physical address, as opposed to an individual. The location of the target of a digital number recorder would therefore be known in most instances. Further, as noted above, IMSI Catchers obtain information from a given geographical area, which is likely to include both public and private spaces. Even if a state agency's target is known to be moving through a public place at the time of authorization, the device is likely to obtain identifiers from private spaces in the vicinity, thus collaterally impacting on heightened informational privacy interests.

The intrusiveness of these devices is such that the lower 'reasonable grounds to suspect' standard is insufficient to protect the privacy interests affected when such devices are deployed. It should surprise no one that two US courts recently rejected the lower reasonable suspicion standard as capable of constitutionally authorizing IMSI Catcher use.[451] As only section 492.1 of the *Criminal Code's* metadata interception framework employs the more protective reasonable and probable grounds standard, a reading of these overlapping powers that is consistent with *Charter* principles,[452] would ensure that IMSI Catcher authorization occurs further to this power alone.

Charter Principles of Incrementalism, Minimal Intrusion & Narrow Tailoring

Courts in the United States and in Canada have increasingly recognized the need to impose additional protections in order to minimize the collateral impact that is inherent in searches comparable to those that occur upon IMSI Catcher deployment. As detailed above, a US District Court for the Northern District of Illinois imposed the following conditions as a means of "reasonably balance[ing] the competing interests of effective law enforcement and people's Fourth Amendment privacy interests"[453] that are implicated when IMSI Catchers are used:

- agencies must make reasonable and demonstrable efforts to minimize the capture of non-targeted individuals when deploying IMSI Catchers by localizing the IMSI Catcher more closely around the targeted individuals, where possible, and by refraining from deploying IMSI Catchers where significant numbers of innocent people will be present alongside the specific target(s) in question;

---

[450] *State v Tate*, 357 Wis 2d 271 (2014) (Supreme Court of Wisconsin), pp 23-24.

[451] *Maryland v Andrews*, (2016) *Md App LEXIS 33, File No 1496 (Md Ct of Special Appeals). See also: *United States v Lambis*, (2016) 1:15-cr-00734-WHP, 2016 US Dist LEXIS 90085 (Sth Dist NY).

[452] *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16, paras 20-21.

[453] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

- all data captured by an IMSI Catcher other than data identifying the mobile device used by the target of the deployment must be destroyed "immediately" and, regardless, no less than within 48 hours of capture. This destruction must be explicitly verified to the Court that authorized use of the IMSI Catcher; and
- a categorical prohibition on any law enforcement use of data acquired from use of an IMSI Catcher beyond what is necessary to identify and isolate the mobile phone information of the target.[454]

Such conditions are in line with the principle of "minimal intrusion" on privacy that lies at the heart of section 8 of the *Charter* and is essential to its full realization.[455]

Contemplating the principle of minimum intrusion in the context of a comparable, but less intrusive, tower dump production order, the Ontario Superior Court of Justice established a set of instructive guidelines for safeguarding privacy interests in *R v Rogers Communications*.[456] Tower dumps typically entail production orders compelling service providers to disclose data collected by cell towers in a given region over a set period of time. As IMSI Catchers are designed to emulate cell tower functionality, the resulting data sets share similarities. Tower dump data sets can include more than digital identifiers – they can include, for example, calling records (who phoned who when) in addition to identification documents. On the other hand, IMSI Catchers can more accurately geo-locate and track the individuals they identify. Both types of searches are inherently broad in nature, with high collateral privacy impact as numerous non-targets are affected for each intended target.[457] In order to offset this broad collateral impact, the court identified the following relevant guidelines:

- state agencies must independently justify each location from which data is sought. For example, each cell site/tower from which data is sought must be independently justified by its connection to the investigative objective in question;[458]

---

[454] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

[455] *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 SCR 425 per Wilson, J, dissenting on a different point, para 100 ("...the criteria set forth in *Hunter* must be substantially if not completely met... The criteria...are as follows: ... (d) a requirement that the only documents which are authorized to be seized are those which are strictly relevant to the offence under investigation"); *Wakeling v United States of America*, [2014] 3 SCR 549, 2014 SCC 72 (a residual and continuing expectation of privacy persists after collection occurs by means of intrusive electronic surveillance mechanisms); *R v Rogers Communications*, 2016 ONSC 70, paras 40-41, 44, 48; *R v Vu*, [2013] 3 SCR 657, 2013 SCC 60, para 22 ("an authorized search must be conducted in a reasonable manner. This ensures that the search is no more intrusive than is reasonably necessary to achieve its objectives."

[456] *R v Rogers Communications*, 2016 ONSC 70, paras 63-63.

[457] *R v Rogers Communications*, 2016 ONSC 70, para 25.

[458] *R v Rogers Communications*, 2016 ONSC 70, para 65, b).

- state agencies must justify each type of data sought – for example, calling records from individuals outside the cell site areas for which there is justification to search (i.e. individuals making incoming calls to someone within a targeted area) should not be included. If it is known that the target only made short one minute phone calls, only records relating to one minute phone calls should be provided by the service provider. Similarly, service provider-generated reports should be relied upon in lieu of underlying datasets to reduce the amount of unnecessary customer data exposed;[459]

- tower dump records sought must be closely linked to the objective of the privacy intrusion. For example, if the objective of the tower dump is to geo-locate mobile devices present in specific areas, then credit card records, which are wholly unrelated to the geo-location objective, should not be disclosed. If the objective is to identify which phones were used in 5 known locations at 5 known times, then only information relating to devices present at all 5 should be provided;[460] and

- in general, tower dumps must embody the principles of incrementalism and minimal intrusion on privacy and be narrowly tailored, including only data sets reasonably and probabilistically linked to the offence.[461]

While the Ontario court in *Rogers* chose not to impose conditions on retention or secondary use of non-targeted data,[462] its conditions reflect the same principles and safeguards imposed by the Illinois District Court in the context of IMSI Catchers. For example, while the *Rogers* order imposed many of the targeting and minimization conditions at the collection phase, the Illinois district court necessarily imposes these safeguards as *ex post* conditions on retention and use as the IMSI Catcher context provides no avenue for targeted collection as there is no service provider that can act as a filter.

The recognition of retention and subsequent use limitations would be in line with Canadian *Charter* principles as well as with those in other jurisdictions. For example, the German Constitutional Court has explicitly held in a comparable context (relating to automatic license plate recognition devices, which raise similar considerations to IMSI Catchers in their indiscriminate collection of identifiers) that retention of 'non-

[459] *R v Rogers Communications*, 2016 ONSC 70, para 65, c), d) e) and f), and para 58.

[460] *R v Rogers Communications*, 2016 ONSC 70, para 65, e).

[461] *R v Rogers Communications*, 2016 ONSC 70, para 65, a) b) and g).

[462] *R v Rogers Communications*, 2016 ONSC 70, paras 59-60.

hit' (i.e. non-targeted) individuals' data violates privacy rights protected by the German Basic Law.[463] As noted by the Illinois district court mentioned above,

> 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.[464]

The risk that non-targeted information collaterally obtained by IMSI Catchers will be used is far from trivial. Once state agencies obtain and retain such data they can subsequently rely on information sharing and re-use laws such as thsoe enacted by Bill C-51, which authorized sharing of information with other government agencies for a sweepingly broad set of objectives once that information is legitimately obtained.[465] One central safeguard against the misuse of IMSI Catcher records is therefore an obligation on the part of state agencies to delete all non-targeted and non-identification data which they have captured collaterally, which should be done as expeditiously as possible. Moreover, limiting use of such data to what is strictly necessary in order to identify and isolate the specific target should permit law enforcement to achieve their legitimate objectives while preventing IMSI Catcher deployments from effectively becoming fishing expeditions. It should not be surprising that such obligations were found to be necessary to "reasonably balance the competing interests of effective law enforcement and people's Fourth Amendment privacy interests."[466]

Section Four: Best Practices for IMSI Catcher Use in Canada

This final section outlines a series of best practice recommendations for IMSI Catcher use in Canada. These best practices are informed by constitutional principles as well

---

[463] BvR 2074/05 of 11.3.2008.

[464] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

[465] Kent Roach & Craig Forcese, "Bill C-51 Backgrounder #3: Sharing Information and Lost Lessons from the Maher Arar Experience", *SSRN*, 18 February 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2565886; Canadian Internet Policy & Public Interest Clinic, OpenMedia.ca & Canadian Journalists for Free Expression, "A Primer", April 2015, https://cippic.ca/uploads/BillC51-APrimer.pdf.

[466] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div). Internal policies from the US Departments of Justice and Homeland Security have imposed comparable restrictions on retention and use of non-target data obtained by IMSI Catcher use: Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download; Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf; as does the IMSI Catcher authorization regime adopted in the German Criminal Procedure Code: Criminal Procedure Code (Strafprozessordnung)(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, sub-section 101i.

as by legislative, judicial and policy controls imposed in comparable contexts in Canada and on IMSI Catcher use in other jurisdictions.

In terms of best practices, this section first addresses the need for essential transparency measures in the form of statistical reporting, individual notification requirements, and compliance with *Radiocommunication Act* obligations to publicize devices such as IMSI Catchers that make use of spectrum. Second, it then identifies a series of limitations on the use of IMSI Catchers rooted in the principle of proportionality. Finally, we review a series of minimization requirements necessary to curtail the more excessive and invasive features of IMSI Catcher use.

The realization of these best practices can be achieved through a variety of policy vehicles. Some of its conditions can be imposed by courts directly at the authorization stage, others may be more appropriately adopted as a matter of legislation or policy. Perhaps the clearest way to address IMSI Catcher use would be to explicitly legislate its authorization within Part VI of the *Criminal Code*, which is currently used to regulate other invasive electronic surveillance techniques such as wiretapping and surreptitious audio recording. Explicit encoding in this manner would, on the one hand, ensure proper safeguards are in place for IMSI Catcher use. On the other hand, it would clarify the currently ambiguous and overlapping framework for IMSI Catcher legal framework that is explored above by creating an explicit avenue for authorization. Finally, it would criminalize the use of IMSI Catchers for non-law enforcement purposes, and which raise significant potential for criminally motivated privacy invasion.[467]

Parliamentary intervention is therefore the preferred mechanism for resolving this uncertainty, rather than attempting to do so through the courts on a case-by-case basis or relying on internal policies such as those adopted by the United States Departments of Justice and Homeland Security. In either scenario, the inherent privacy risks posed by IMSI Catchers require that courts strive for proportionality and balance before authorizing their use, including a contextual assessment of the

[467] In this respect, it should be noted that malicious or for-gain use of IMSI Catchers likely already violates the criminal code prohibition on the interception of radio-based telephone communications (section 184.5). Section 184 of the *Criminal Code* criminalizes the interception of *private* communications without authorization and, as detailed in **Section Three: B-iii**, the application of this section to IMSI Catcher deployment in identification mode is ambiguous and unclear specifically because it is unclear whether the digital identifiers intercepted by IMSI Catchers constitute 'private' communications under Canadian law. Section 184.5 of the *Criminal Code*, by contrast, applies to the interception of *all* radio-based (ie mobile) communications regardless of whether these are 'private' or not: *R v Watts*, 2000 BCPC 191; *Watts v Klaemt*, 2007 BCSC 662; *R v Nguyen*, 2001 ABPC 52. As section 184.5 only criminalized malicious or 'for gain' interception, it will likely play and at-best limited role in regulating the use of IMSI Catchers by state agencies. However, this provision can play a role in controlling mis-use of these devices by non-state actors and may also apply to the activities of foreign state actors within Canada.

collateral harm or risk to non-targeted individuals as a result of their deployment.

A. Transparency Measures to Ensure Accountability

This section proposes three main recommendations aimed at making the use of IMSI Catchers Canada more transparent and publicly accountable, summarized in **Table 3**:

Accountability & Transparency Mechanisms	***Brief Description***
Statistical Reporting	Statistical reporting obligation analogous to requirements for other invasive forms of electronic surveillance in Part VI of the *Criminal Code* and adapted for the particular characteristics of IMSI Catcher surveillance
Individual Notification	Obligation to provide individual notification to all individuals subject to IMSI Catcher surveillance, as well as (to the extent possible and while minimizing further invasions of privacy) notification to non-targeted individuals
Radiocommunication Act Compliance	Compliance with general requirement to seek government certification for radio spectrum devices like IMSI Catchers and compliance with any ministerial requirements to limit the possibility of harmful interference

Table 3: Accountability & Transparency Mechanisms

Historically, statistical reporting and individual notification requirements have played a prominent role in Canada's statutory electronic surveillance regime, which is set out in Part VI of the *Criminal Code*. However, more recent electronic surveillance powers added to the *Criminal Code* have lacked both of these obligations, and it is unclear that IMSI Catcher use will fall within Part VI of the *Criminal Code* as currently formulated. Moreover, even under Part VI, there is no explicit obligation to report or notify affected individuals of IMSI Catcher use distinctly from other, more generic Part VI activities such as wiretapping. This is a shortcoming, and the recent trend away from including statistical reporting obligations in electronic surveillance powers creates a distorted picture of state surveillance practices generally. This shortcoming is all the more concerning in its application to invasive tools such as IMSI Catchers.

i. Statistical Reporting

While not yet a constitutional imperative,[468] statistical reporting is a precondition to a meaningful public understanding of the scope and parameters of state electronic

[468] *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16.

surveillance and, by extension, to ensuring its ongoing proportionality and accountability.[469] Indeed, the recent trend towards enacting electronic surveillance powers without the inclusion of any statistical reporting obligations whatsoever has led to a highly distorted picture of the scope and nature of state surveillance practices in Canada.[470] This is because individuals' personal information and activities have shifted toward digital networks, providing state agencies with rich repositories of recorded information that can be useful for investigative purposes and other ends. However, such information often falls outside of the Part VI regime, either because that regime is only presumed to protect the 'content' of communications (rather than metadata) or because it is obtained by means other than 'interception' (such as when it is obtained directly from a service provider who is storing it).[471] As a result, the collection and use of this information is not subject to the same notice and reporting requirements as other forms of invasive surveillance, like a wiretap for example. Yet metadata is often just as revealing as the 'content' of communications, and sometimes even more so.[472] This sensitivity is compounded by its ubiquity, arising both from the pervasive collection of this information by third parties, and by the form this data takes, which can facilitate intensive analytics that reveal novel information not even known by the communicating parties themselves. Such data is not only sensitive and revealing of private life, but constitutes the bulk of modern state surveillance data collection.[473] Yet all of this surveillance now falls outside the state's general statistical reporting obligations. The result is that it has become difficult for the public, civil society, and legislators alike to understand and hold the state accountable for its surveillance practices.

A statistical reporting obligation relating to IMSI Catcher use, specifically, can help ensure that state agencies' use of the devices remains within appropriate boundaries while enhancing public confidence. A key problem with IMSI Catchers is their rapidly decreasing cost. Historically, the expense of such devices meant they were generally

---

[469] See, for example: Necessary & Proportionate Coalition, *Necessary & Proportionate Principles*, (May 2014), https://necessaryandproportionate.org/principles, Principle 9.

[470] Nicholas Koutros & Julien Demers, 2013. "Big Brother's Shadow: Historical Decline in Electronic Surveillance by Canadian Federal Law Enforcement", (2013) 11(1) *Can J of L & Tech* 79, SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220740.

[471] See discussion at infra, **Section Three: B-iii**. See also: *R v TELUS Communications Co*, [2013] 2 SCR 3, 2013 SCC 16.

[472] See for example: Necessary & Proportionate Coalition, *Necessary & Proportionate Principles*, (May 2014), https://necessaryandproportionate.org/principles, "Changing Technology and Definitions".

[473] See, for example: Naomi Gliens, 2012, "New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance", *American Civil Liberties Union*, 27 September, 2012, https://www.aclu.org/blog/new-justice-department-documents-show-huge-increase-warrantless-electronic-surveillance, demonstrating migration of state surveillance techniques away from wiretapping (which, in Canada, include an individual notice and statistical reporting obligation) and towards other forms of information gathering.

reserved for rare instances such as where national security was at stake.[474] However, as the cost of surveillance devices plummet, state agencies begin to deploy them with far greater frequency and to achieve significantly more mundane objectives.[475] The Baltimore police department, for example, has deployed IMSI Catchers in hundreds of investigations where no national security threat was evident at all,[476] including an investigation of an alleged theft of "15 chicken wings and three subs" by a restaurant employee.[477] Little is known regarding the scope of use by Canadian agencies, as state agencies have yet to officially confirm use of these devices at all. However, one court decision that has been made public confirms that these devices are no longer reserved for national security situations and that they have been used for more mundane criminal investigations as well as for such tasks as locating a missing person.[478] While the invasive potential of IMSI Catchers is problematic even where their use is infrequent, routine deployment of such devices exacerbates this potential greatly while simultaneously multiplying the number of innocent, non-targeted, individuals affected. Statistical reporting obligations are essential to identifying these types of issues and generally tracking the effectiveness and proportionality of these devices.

Statistical reporting is a prominent feature of IMSI Catcher use in both Germany and the United States. In the United States, statistical reporting obligations are central components of the *Pen Register Statute* metadata interception regime, which in part underpins IMSI Catcher deployment.[479] Germany imposes statistical reporting obligations specifically on the use of IMSI Catchers by its intelligence agencies.[480] Statistical reporting is not constitutionally required under Canadian law.

---

[474] In Canada, for example, law enforcement had access to specialized equipment capable of tracking mobile devices with find-grained accuracy – likely IMSI Catcher technology – in 2008 but, at that time, the technology was only available for national security investigations: *R v Riley*, [2008] 174 CRR (2d) 288, 234 CCC (3d) 181 (ONSC), para 47: "I note, however, that the mere fact that a cell phone call involving Riley is intercepted does not tell the police what his location is. Cellular location does no more than provide the 'neighbourhood' of the call, which can be several miles square. While analog cellular services permitted tracking a cellular hand set to a physical location, the advent of digital technology has made this more difficult. In the case of Telus, for example, radio frequency equipment cannot be used to hone in on a cell phone. There is specialized equipment that does permit this, but it is only available in Canada for national security use. Of course, the content of a communication involving Riley might be of assistance in locating him."

[475] 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.

[476] 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/.

[477] Courtney Mabeus, 2016, "Battlefield Technology Gets Spotlight in Maryland Courts: Secrecy and Defence Concerns Surround Cell Phone Trackers", May 3, 2016, *Capital News Service*, http://cnsmaryland.org/interactives/spring-2016/maryland-police-cell-phone-trackers/index.html.

[478] Jordan Pearson, 2016. "The RCMP Surveilled Thousands of Innocent Canadians for a Decade", June 10, 2016, *Motherboard (VICE)*, https://motherboard.vice.com/read/the-rcmp-surveilled-thousands-of-innocent-canadians-for-a-decade.

[479] Obligations encoded in 18 USC § 3126 (Attorney General will report to Congress annually the number of orders sought).

[480] Aidan Wills & Mathias Vermeulen, (2011). "Parliamentary Oversight of Security and Intelligence Agencies in the European Union," European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2011, PE 453.207, http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf.

Nevertheless, given the highly invasive nature of IMSI Catchers and, particularly, their unique tendency for collateral impact on the privacy of non-targeted individuals, a policy-based obligation to provide regular statistical reporting on IMSI Catcher deployment would greatly enhance public understanding of contemporary mobile device surveillance and meet other important policy objectives. Statistical reporting of such information has a high public interest value and would help to realize the federal government's "commitment to openness and transparency."[481] Moreover, regular reporting of this kind is needed at a basic level in order to assess and challenge matters of public interest – namely the lawfulness and the desirability of investigative programs.[482] In the absence of such basic data the public is unable to develop a meaningful awareness of the circumstances under which its members may be subject to surveillance, rendering both political and legal contestation of these practices effectively impossible.[483]

Such reporting should include sufficient detail and granularity for the public to make meaningful judgments about the state and scope of electronic surveillance in Canada and allow individuals to understand, at a basic level, the ways in which that surveillance may impact their lives. Statistical reporting on IMSI Catcher use should therefore provide the same kinds of information required under section 195 of the *Criminal Code* for other forms of electronic surveillance, modified for the unique functionalities of IMSI Catchers. For example, it should include the number of applications made for authorizations and the number granted; the specific offences for which authorizations were given and the number of authorizations given in respect of each; the number of persons arrested, criminal proceedings commenced, and proceedings which resulted in a conviction where IMSI Catcher data was adduced as evidence; the number of persons arrested whose identity became known to a peace officer as a result of IMSI Catcher use, and so on.[484] It should also include reporting related to the classes of places and the geographic scope of IMSI Catcher deployment, the number of non-targeted individuals affected by the authorization, and any conditions on the authorization or minimization efforts undertaken to prevent harm to those individuals.

---

[481] OPC Annual Report, Privacy Act, Section 4: Review of the Royal Canadian Mounted Police – Warrantless Access to Subscriber Information, https://www.priv.gc.ca/information/ar/201314/201314_pa_e.pdf.

[482] *R v Mentuck*, [2001] 3 SCR 442, 2001 SCC 76; *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23; *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31; *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, [2013] 3 SCR 733, 2013 SCC 62.

[483] Michael Geist, "Secret Memo Reveals RCMP Records on Requests for Subscriber Data 'Inaccurate and Incomplete'", *Michael Geist*, 2 March, 2015, http://www.michaelgeist.ca/2015/03/secret-memo-reveals-rcmp-records-requests-subscriber-data-inaccurate-incomplete/; OPC Annual Report, Privacy Act, Section 4: Review of the Royal Canadian Mounted Police – Warrantless Access to Subscriber Information, https://www.priv.gc.ca/information/ar/201314/201314_pa_e.pdf.

[484] *Criminal Code,* RSC 1985, c C-46, section 195.

ii. Individual Notice Obligation

Much like statistical reporting obligations, individual notice requirements are currently only constitutionally mandated in narrow and specific circumstances.[485] However, individual notice obligations are often the only mechanism by which an individual is able to learn that their privacy has been violated by the government. Where surveillance does not reveal criminal conduct and thus does not result in criminal charges (and, hence, does not trigger the accompanying disclosure obligations), the surreptitious nature of electronic surveillance prevents innocent individuals from realizing that their privacy has been invaded. The outcome is that, absent an individual notice obligation, only privacy violations which actually reveal evidence of criminal conduct are likely to be uncovered and challenged in court.[486] As a result, properly formulated individual notice obligations constitute a critical accountability mechanism in the context of electronic surveillance practices.[487]

An individual notice obligation is another important step toward instilling public confidence regarding government use of IMSI Catchers, and would provide a critical safeguard to ensure that the devices are not deployed in inappropriate circumstances. In some instances, such as when non-targeted IMSIs are not retained,[488] this form of notification can be realized by issuing 'time and place' announcements, indicating the geographic region, time and duration of a given deployment, which would permit affected individuals to know whether they were affected. For example, an IMSI Catcher may be deployed at an apartment building or school for an extended period of time if a suspect spends significant amounts of time at either locale. In other contexts, such as where specific non-targeted individuals become known to state agencies, direct individualized notice would be more appropriate. In either instance, notification would only occur in a manner that would

---

[485] *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16, para 85; *Wakeling v United States of America*, 2014 SCC 72, paras 67 and 72.

[486] *R v Rogers Communications*, 2016 ONSC 70; *Wakeling v United States of America*, 2014 SCC 72, paras. 67 and 72; *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16.

[487] See for example: Necessary & Proportionate Coalition, *Necessary & Proportionate Principles*, (May 2014), https://necessaryandproportionate.org/principles, Principle 8 and The Global Principles on National Security and the Right to Information (Tshwane Principles), June 12, 2013, https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf, Principle 10, sub-clause E (4).

[488] Direct individualized notification should not occur, for example, where doing so would require additional investigative measures to link digital identifiers to specific individuals or additional retention measures. For comparable restrictions on notification applied in a different electronic surveillance context, see: *Criminal Procedure Code (Strafprozessordnung)*(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, sub-section 101 (4)("Notification shall be dispensed with where overriding interests of an affected person that merit protection constitute an obstacle thereto. ... Investigations to determine the identity of a person listed in the first sentence are to be carried out only if this appears necessary taking into account the degree of invasiveness of the measure in respect of the person concerned, the effort associated with establishing their identity, as well as the resulting detriment for such person or other persons.").

account for the need to preserve ongoing investigations.

Individual notice obligations have not been constitutionally required except where private communications are intercepted in the absence of prior judicial authorization. However, in light of the high number of individuals whose privacy is collaterally affected each time an IMSI Catcher is deployed, the *Charter* may require a more robust reporting obligation,[489] at least where deployment is without prior authorization but even where such authorization is obtained.[490] Part VI, which regulates the interception of private communications, includes an obligation to notify targets of wiretaps in a timely manner.[491] To the extent Part VI applies to IMSI Catcher use, the individual notice obligation would apply by extension. In Germany, the obligation to notify both the target as well as certain others affected by a surveillance operation is an integral and explicit component of the IMSI Catcher authorization regime.[492] The United States Departments of Justice and Homeland Security, which now treat IMSI Catchers as tracking devices, also impose an individual notice obligation onto the use of IMSI Catchers.[493] Each of these notice obligations are subject to some form of notice delay, so as to prevent legitimate investigations from being inadvertently curtailed by premature notification.[494]

---

[489] For example, it has now been confirmed that IMSI Catchers have been deployed to locate missing persons (by the RCMP; Jordan Pearson, 2016. "The RCMP Surveilled Thousands of Innocent Canadians for a Decade", June 10, 2016, *Motherboard (VICE)*, https://motherboard.vice.com/read/the-rcmp-surveilled-thousands-of-innocent-canadians-for-a-decade) and in exigent circumstances where no prior judicial authorization was obtained (by the Vancouver Police Department, see **Update Box 1**).

[490] *R v Rogers Communications*, 2016 ONSC 70; *Wakeling v United States of America*, 2014 SCC 72, paras. 67 and 72; *R v Tse*, [2012] 1 SCR 531, 2012 SCC 16.

[491] *Criminal Code*, RSC 1985, c C-46, sub-section 196(1) requires notification to occur within 90 days of the expiration of the authorized interception period, extendable upon application to a judge for a maximum of three years (sub-sections 185(2)-(4)).

[492] *Criminal Procedure Code (Strafprozessordnung)*(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, sub-section 101 (4), clause 8 and sub-section (5)(notification of the target of an IMSI Catcher must occur "as soon as it can be effected without endangering the purpose of the investigation, the life, physical integrity and personal liberty of another, or significant [investigative] assets") .

[493] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download; Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p 3 (DoJ) and 4 (DHS), respectively: ("as a matter of policy, law enforcement agencies must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure…"). *Federal Rules of Criminal Procedure*, Rule 41(f)(2)(C) ("Within 10 days after the use of the tracking device has ended, the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked…").

[494] *Criminal Code*, RSC 1985, c C-46, sub-sections 185(2)-(4) (state may apply to the authorizing judge for an extension to the statutory notification period if it is in the interests of justice to do so, up to a maximum of three years); *Rules of Criminal Procedure*, Rule 41(f)(3)(a judge may delay the notice requirement "if the delay is authorized by statute."); *Criminal Procedure Code (Strafprozessordnung)*(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, sub-section 101(5) (Notification shall occur "as soon as it can be effected without endangering the purpose of the investigation, the life, physical integrity and personal liberty of another, or significant [investigative] assets" and the reasons for any such delay shall be documented. Any such delay that

Each of these notice obligations are deficient, however, in that they only require that the intended target of an IMSI Catcher deployment be notified, taking no measures to notify other affected individuals (whether by means of geographic or direct individualized notification). An additional avenue for facilitating individual knowledge of surveillance could be found in section 12 of the *Privacy Act*, RSC 1985, c P-21, which grants individuals the right to access any of their personal information that is collected and retained by government agencies, subject to exceptions.[495] Where state agencies are permitted to retain digital identifiers of non-targets, the *Privacy Act* access right could provide a workable framework for facilitating individual notice on an 'opt in' basis. Digital identifiers collected would be held in a specific information bank and individuals could query these banks with their digital identifiers to determine if they have been the object of an IMSI Catcher deployment. Such a mechanism, in conjunction with a 'geographic notification' mechanism, would create the requisite individualized accountability mechanism without the adverse consequences that might result were state agencies obligated to undertake additional invasive investigatory steps for the sole purpose of notifying individuals affected by an IMSI Catcher deployment.

iii. Complying with Spectrum Usage Transparency Obligations

Finally, IMSI Catcher use should not be exempted from oversight or certification under the *Radiocommunication Act*. The *Act* prohibits the use of uncertified radio devices in Canada, with the Ministry of Innovation, Science and Economic Development Canada (ISED, formerly Industry Canada) responsible for the certification process. As argued above, IMSI Catchers are radio devices within the meaning of the Act that do not fall within any of the exceptions which might permit state agency use of such a device without prior certification.[496] While there have been a number of confirmed (but not officially confirmed) and documented instances of IMSI Catcher use in Canada, ISED has confirmed in response to a query from the *Globe and Mail* that it has received no such certification requests:

---

exceeds 12 months must be approved by a judge. A judge may permanently dispense with notification where "there is a probability bordering on certainty that the requirements for notification will not be fulfilled, even in future"). See also: Necessary & Proportionate Coalition, *Necessary & Proportionate Principles*, (May 2014), https://necessaryandproportionate.org/principles, Principle 8 (Notification should occur as soon as possible unless a judge determines that notification "would seriously jeopardize the purpose for which the [surveillance] is authorized, or there is an imminent riks of danger to human life").

[495] The most salient exception is section 22, which permits state agencies to refuse access to any information collected for the purpose of carrying out an investigation of an offence. However, the constitutionality of this broad exception is questionable, as it fails to take into account the public interest in making such a disclosure and does not require any demonstration that disclosure of requested information will harm any legitimate law enforcement objective in any manner. See *R v Mentuck*, [2001] 3 SCR 442, 2001 SCC 76; *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [2010] 1 SCR 815, 2010 SCC 23; *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31; *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers*, Local 401, [2013] 3 SCR 733, 2013 SCC 62.

[496] See discussion at **Section Two: C-iii, 'Risk that Possession & Use Violates Radiocommunication Act'**.

> International Mobile Subscriber Identity (IMSI) catchers are a class of radio apparatus, as they use standard radio signals to communicate with surrounding devices. Their possession or use would need to be authorized (…) [but] no such authorizations have been provided to date.[497]

This lack of certification must be remedied. Moreover, if for some reason IMSI Catchers are found to fall within one of the exceptions to certification found in the *Radiocommunications Act*, this exception should be modified to clarify that IMSI Catchers require certification.

Certification operates as an important transparency measure. It provides with a list of device models being sold or used to state agencies in Canada, allowing for the public to proactively assess the nature of devices used by state agencies in Canada. This is particularly important in light of the documented ability of this equipment to interfere with Canadian phone conversations, including emergency 911 calls.[498] Nor is there any justification to avoid such transparency measures. As described comprehensively in **Section Two**, transparency regarding the existence of these devices poses no threat to state agencies seeking to use such devices, and the lack of transparency regarding their regulation runs directly counter to the public interest. Indeed, the United States Federal Communications Commission, which, is responsible for overseeing spectrum usage in the United States, requires IMSI Catcher vendors to register all IMSI Catcher devices prior to commercial sale or use by non-federal government agencies. The list of these devices is publicly available on the FCC's website, subject to minor redactions intended to protect trade secrets, as explained by FCC Chairman Tom Wheeler:

> Equipment certification is required to ensure that products that use radio spectrum comply with the Commission's technical rules. Certification is required before such a product can be imported or marketed in the United States, except that equipment marketed to or used solely by the federal government is not subject to the Commission's rules or certification. Placing conditions on the equipment certification is intended to ensure that use of such equipment is constrained to law enforcement. …
>
> Harris Corporation has applied for and been granted certification for several devices, all of which are posted on the Commission's web site. A list of the certified devices and the links to the grants of certification are attached. Portions of the applications are withheld from public inspection as permitted under the Commission's rules because they include

[497] Matthew 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/.

[498] Freeze, (2016). "RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals", *The Globe and Mail*, April 18, 2016, http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memo-reveals/article29672075/.

> trade secrets. Digital Receiver Technology, Inc. applied for and was granted certification for similar devices which are also included in the attached list. The same conditions are included on the grants of certification for these devices.[499]

This position is in stark contrast to the conduct of Canadian agencies, which have claimed they cannot even acknowledge the existence of IMSI Catchers without compromising their utility.

B. Ensuring Proportionate & Narrowly Tailored Conditions of Use

As inherently intrusive electronic surveillance devices, IMSI Catchers should not become a tool for daily policing but should be reserved for situations that are sufficiently serious. In addition, as IMSI Catchers replicate functionality of cell towers, there will often be far less intrusive means of achieving the same investigative objective by leveraging a mobile network's existing capabilities. As such, an investigative necessity obligation should be included in any comprehensive attempt to regulate IMSI Catcher usage. Finally, prior to each IMSI Catcher deployment, a judge ought to first determine that a high evidentiary burden has been met. In order to ensure that IMSI Catchers are only employed in a proportionate and narrowly tailored manner, certain pre-conditions to their use must be in place. These circumstances are summarized in **Table 4**, and expanded upon below:

Narrowly Tailored & Proportionate	***Brief Description***
Enumerated & Serious Crimes	IMSI Catcher use should only be available for the investigation of a statutorily enumerated list of serious criminal offences, and not for any other state objective[500]
Investigative Necessity	IMSI Catcher use should only be available to law enforcement where other investigative mechanisms are not likely to suffice[501]
Judicially Determined Reasonable Belief	IMSI Catcher usage must only be permitted where an informed judge has determined that reasonable & probable grounds to believe that an offence has or will be committed, and that the anticipated privacy intrusion will yield evidence of the offence in question exist[502]

Table 4: Proportionate & Narrowly Tailored Conditions of Use

[499] Federal Communications Commission Chairman Tom Wheeler, (2015). Letter to Senator Bill Nelson," United States Government, April 13, 2015, retrieved January 11, 2016, https://apps.fcc.gov/edocs_public/attachmatch/DOC-333229A1.pdf.

[500] This list could be comparable to that included in Part VI of the *Criminal Code*, RSC, 1985, c C-46, section 183 which defines "offence" as a finite list of offences for the purposes of Part VI, and criminalizes wiretapping for other purposes, subject to some exceptions.

[501] *Criminal Code*, RSC , 1985, c C-46, Part VI, paragraph 186(1)(b).

[502] Similar obligations are imposed by Part VI of the *Criminal Code*. The exception would be where exigent circumstances exist.

Imposing these pre-conditions on IMSI Catcher use will help to mitigate the more intrusive features of these devices by ensuring the devices are only deployed in circumstances deemed to be proportionate.

Unauthorized IMSI Catcher use should be criminalized and authorized use of the devices should be linked exclusively with investigation of serious criminal offences. Such a limitation is imposed by Part VI of the *Criminal Code* on the use of other intrusive types of electronic surveillance.[503] Explicitly incorporating IMSI Catcher authorization into Part VI would restrict state use of these devices to situations involving an existing list of permissible offences already deemed by Parliament as appropriate for invasive electronic surveillance tools.[504] However, the objective can be achieved by more flexible means. Unauthorized IMSI Catcher use could be criminalized independently, and the list of permissible offences can be established by means of regulation.[505] The objective is to limit IMSI Catcher use in advance to a specific list of offences.

Imposing a 'serious crime' restriction will prevent such devices from being used in disproportionate circumstances, as has occurred in some other jurisdictions. In the absence of such restrictions, US-based policing services have begun using these devices for investigations of minor offences, including petty theft, where the collateral privacy impact is difficult to justify.[506] It will also provide an important safeguard that would limit the availability of these devices in abusive situations where the temptation to use them might otherwise be high. For example, there is often significant pressure and a tendency to adopt disproportionate measures where political protests are anticipated,[507] including the pre-textual use of minor infractions or even the introduction of disproportionate new laws to achieve short term disruption of legitimate political expression or to violate civil liberties in other

---

[503] *Criminal Code*, RSC, 1985, c C-46, section 183, "offence". See also, Necessary & Proportionate Coalition, *Necessary & Proportionate Principles*, (May 2014), https://necessaryandproportionate.org/principles, Principle 5, clauses 1-2.

[504] Incorporating IMSI Catcher authorization into Part VI will also provide an easy vehicle to apply existing exceptions to the general provisions limiting use to enumerated criminal offences, such as where exigent circumstances exist, or in the foreign intelligence context. (see, for example, *National Defence Act*, RSC 1985, c N-5, section 273.69. However, such exceptions must also be compliant with minimum *Charter* requirements (see for example, Tamir Israel, in Michael Geist, Ed, Privacy & Surveillance in Canada in the Post Snowden Era, (Ottawa: University of Ottawa Press, 2015), https://cippic.ca/uploads/Ch3_ForeignIntelligence-2015.pdf).

[505] For example, *Radiocommunication Act (Subsection 4(4) and Paragraph 9(1)(b) Exemption Order, No 2015-1*, SOR/2015-36, which permits the RCMP to use jamming devices without first seeking certification under the *Radiocommunications Act*, provides a limited (albeit overly broad) list of permissible purposes for such use (sub-section 3(1)).

[506] Courtney Mabeus, 2016, "Battlefield Technology Gets Spotlight in Maryland Courts: Secrecy and Defence Concerns Surround Cell Phone Trackers", May 3, 2016, *Capital News Service*, http://cnsmaryland.org/interactives/spring-2016/maryland-police-cell-phone-trackers/index.html; 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/.

[507] See for example, *Good v Toronto (Police Services Board)*, 2016 ONCA 250; *Canadian Civil Liberties Association v Toronto Police Service*, 2010 ONSC 3525; *Bérubé c Québec (Ville de)*, 2014 QCCQ 8967, para 96, 112.

ways.[508] The use of IMSI Catchers in the context of political protests raises heightened concerns, as such devices could easily undermine anonymous political expression.[509] Providing a finite list of enumerated offences would help pre-empt the misuse of such devices in these types of scenarios.

Imposing an investigative necessity obligation will similarly constitute a pragmatic best practice that will help mitigate the more intrusive features of IMSI Catchers. Investigative necessity is not a constitutional requirement, but is, again, included in Canadian regulations seeking to ensure invasive electronic surveillance techniques are used in proportionate circumstances.[510] Given that IMSI Catchers replicate functionality of the mobile communications network, the same information sought by means of an IMSI Catcher deployment will often be available through other, less intrusive means by using existing mobile network infrastructure.[511] These less intrusive options are significantly more protective of privacy interests in that their use allows for searches that greatly reduce the collateral impact on non-targets in ways that are not available when an IMSI Catcher is deployed.[512] Further, when relying on a service provider to obtain the same digital identifiers as would be obtained by means of an IMSI Catcher, there is no disruption to mobile communications in the area of deployment. Parliament has recognized the benefit of minimizing such disruption in other contexts, when regulating cellular 'jamming' devices.[513]

Finally, we argue above that the *Charter* mandates prior judicial authorization as a pre-requisite to any IMSI Catcher deployment.[514] This must be informed authorization – the authorizing judge must be made explicitly aware that the intended electronic

---

[508] *Bérubé c Québec (Ville de)*, 2014 QCCQ 8967, paras 6-7. *Designation of Public Works*, O Reg 233/10; Anna Mehler Paperny, 2010. "Toronto Police Knew They Had No Extra Arrest Power", June 29, 2010, *The Globe and Mail*, http://www.theglobeandmail.com/news/toronto/toronto-police-knew-they-had-no-extra-arrest-powers/article1623566/; Jennifer Yang, 2010. "G20 Law Gives Police Sweeping Powers to Arrest People", June 25, 2010, *Toronto Star*, https://www.thestar.com/news/gta/g20/2010/06/25/g20_law_gives_police_sweeping_powers_to_arrest_people.html; The Honourable R Roy McMurtry, 2011, "Report of the Review of the *Public Works Protection Act*, *Submitted to the Minister of Community Safety and Correctional Services*, April 2011, http://www.mcscs.jus.gov.on.ca/sites/default/files/content/mcscs/docs/ec088595.pdf.

[509] 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.

[510] *Criminal Code*, RSC , 1985, c C-46, Part VI; See also: Necessary & Proportionate Coalition, *Necessary & Proportionate Principles*, (May 2014), https://necessaryandproportionate.org/principles, Principle 5 clause 3.

[511] See **Table 2: Relevant Production Orders** and surrounding discussion in **Section Three: B-ii "Substantial Equivalence: Achieving IMSI Catcher objectives by less intrusive means"**.

[512] *R v Rogers Communications*, 2016 ONSC 70, paras 58 and 65 (e).

[513] *Radiocommunication Act (Subsection 4(4) and Paragraph 9(1)(b)) Exemption Order No 2015-1*, SOR/2015-36, sub-section 3(2): "Every reasonable effort must be made to restrict the jammer's interference with or obstruction of radiocommunications to the smallest physical area, the fewest number of frequencies, the appropriate power level and the minimum duration required to accomplish the intended purpose."

[514] See discussion in **Section Three: C-ii**.

surveillance includes the use of an IMSI Catcher, as well as of the technical and privacy implications thereof. While there has been no evidence of such obfuscation in Canada, state agencies in other jurisdictions have repeatedly presented IMSI Catchers to authorizing judges as less intrusive 'tracking devices' or 'metadata recorders'.[515] In such circumstances, the authorizing judge may not fully recognize the need for additional safeguards to mitigate the risk to non-targeted individuals. It is therefore critical that courts are aware of the devices' full range of technical capabilities and complete set of intended deployment objectives, as well as the extent to which the device is expected to impact non-targeted individuals prior to authorizing a request. The US Departments of Justice and Homeland Security, in internal policies, have adopted a number best practices designed to ensure authorizing judges are aware of the implications of IMSI Catcher use:

> … applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.
>
> 1. Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine information pertaining to the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. If investigators will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this also.
>
> 2. An application or supporting affidavit should inform the court that the target cellular device (e.g., cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider. The application may also note, if accurate, that any potential service disruption to non-

[515] 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; 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/; Stephanie K. Pell and Christopher Soghoian, 2014. "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 l of Law & Tech* 1, http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf, pp 35-37; 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: "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."

> target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.[516]

Under Canadian law, requiring a comparable description would be in line with the general obligation to make full, fair and frank disclosure when seeking surveillance authorization on an *ex parte* basis.[517] Additionally, we argue above that the *Charter* imposes a high evidentiary standard for deployment of invasive electronic surveillance tool such as an IMSI Catcher.[518] This requires, at minimum, that authorization for deployment be premised on reasonable grounds to believe an offence has or will be committed, and that the anticipated privacy invasion will yield evidence of that offence.

C. Minimization Requirements to Reduce Collateral Privacy Impact

Even where conditions for proportionate authorization (as set out above) are met, steps must still be taken to minimize the unavoidable impact on non-targeted third parties. Recognizing that IMSI Catchers intrude on the privacy of many non-targeted individuals by design, almost every legislative, policy or judicial attempt to address their use abroad has involved targeting and *ex post* minimization measures that aim to mitigate this collateral impact. Canadian judges have the discretion to insert conditions when authorizing electronic surveillance, but it is not currently general practice to do so. However, in the particular context of IMSI Catchers, such measures are justified and should be imposed either as a condition of authorization or by legislation.

Table 5 provides an overview of a number of targeting and minimization requirements designed to limit the impact of IMSI Catchers on non-targeted third parties:

---

[516] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p 6; Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download, p 6.

[516] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download, p 5.

[517] See *R v Araujo*, [2000] 2 SCR 992, 2000 SCC 65. See also <DHS Policy>, p 6: "In all circumstances, candor to the court is of paramount importance. When making any application to a court, DHS law enforcement personnel must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Law enforcement personnel must consult with the prosecutors in advance of using a cell-site simulator, and applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used."

[518] See **Section Three: C-iii 'Baseline Constitutional Standard of Proof: Reasonable Grounds to Believe'**.

Targeting & Minimization	*Brief Description*
Collection & Scope Limitations	Take steps to minimize collateral privacy and functionality impacts by, for example, avoiding deployment of IMSI Catchers at areas/times where it is known many non-targeted individuals will be present,[519] or by carefully minimizing the range of an IMSI Catcher upon deployment to the smallest radius possible[520]
Retention Limitations	Obligation to delete all non-targeted and non-identification data collaterally captured in an expeditious manner, ideally within 48 hours[521]
Use Limitations	Data obtained can only be used to identify the target. Collaterally captured data can only be used to confirm that it is not associated with a target[522]

Table 5: Minimization & Targeting Obligations for IMSI Catcher Use

These mechanisms are critically important in order to ensure that where justification for an IMSI Catcher deployment exists, the impact on third parties is minimized.

Imposing specific limitations on the scope of deployment can limit collection of non-targeted data and is consistent with the constitutional principles of incrementalism and minimal intrusion on privacy.[523] This can be achieved by carefully minimizing the geographic range of an IMSI Catcher upon deployment to the smallest radius possible, by ensuring that deployment will not occur in areas where it can be anticipated that many non-targets will be present, and ensuring that each location

[519] *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

[520] *R v Rogers Communications*, 2016 ONSC 70, para 65 a) – b).

[521] *Criminal Procedure Code (Strafprozessordnung)*(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, sub-section 101i (2); Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p 6; Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download; *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

[522] *Criminal Procedure Code (Strafprozessordnung)*(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, sub-section 101i; Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p 6 (no affirmative investigative use of any non-target data except to distinguish non-targets or with separate court approval); Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download; *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

[523] *R v Rogers Communications*, 2016 ONSC 70, paras 40-41, 56, 58 and 65.

for proposed deployment is justified, to the extent possible.[524] Such measures are not only necessary to meet constitutional principles of minimal intrusion, but can also meet important public policy objectives by limiting the functional disruption that is an inevitable by-product of IMSI Catcher deployment in 'identification mode'. While IMSI Catchers are not jamming devices, their use interferes with the operation of mobile devices within range in a manner that is comparable, and state agency use of jamming devices is conditioned on comparable targeting obligations:

> Every reasonable effort must be made to restrict the jammer's interference with or obstruction of radiocommunications to the smallest physical area, the fewest number of frequencies, the appropriate power level and the minimum duration required to accomplish the intended purpose.[525]

In general, the targeting assessment will always be context-specific, involving considerations such as location, time of day, and the presence of crowds or densely populated areas in order to determine whether the search sought is ultimately proportionate.

As even these measures can only reduce, but not eliminate, substantial collateral privacy impact, *ex post* minimization requirements are also necessary. While retention and use limitations are not a restriction frequently imposed by Canadian courts, such restrictions are specifically necessary in the context of IMSI Catcher use. As discussed in previous sections, the dynamic and persistent nature of mobile digital identifiers mean that they are often persistently associated with a given subscriber or device, and can be used to associate many different types of information with the device's owner or subscriber. Location data in particular can lead to detailed and revealing inferences about a person's beliefs, activities, and relationships. Allowing the unregulated retention of the high volume of non-targeted data obtained each time an IMSI Catcher is deployed can have significant and far-reaching implications for privacy. Further, if IMSI Catchers are used for non-investigative purposes, such as where there is an exigent risk of serious harm (or, for example, to find a missing person),[526] deletion protocols analogous to those recommended above for non-targets should equally apply to the *targets* of IMSI Catcher surveillance. For example, in the case where equipment is used to locate an individual, all data should be deleted as soon as he or she is located. Where an IMSI Catcher is used to identify a device or a device's owner, the records should be deleted

---

[524] *R v Rogers Communications*, 2016 ONSC 70, para 65 a) – b); *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div).

[525] *Radiocommunication Act (Subsection 4(4) and Paragraph 9(1)(b)) Exemption Order No 2015-1*, SOR/2015-36, sub-section 3(2).

[526] Note that it is our position that IMSI Catchers should be used exclusively for the investigation of serious offences or where there is an exigent risk of serious harm.

once the individual has been identified.

Above, we argue that *Charter* principles could require the imposition of strict retention and use limitations when authorizing IMSI Catcher use.[527] Most other jurisdictions which have sought to regulate IMSI Catcher use have recognized the need for such limitations on the devices' use. This includes restrictions adopted by means of internal policies imposed by the United States Departments of Justice and Homeland Security.[528] The Department of Justice's policy mandates the deletion of IMSI Catcher data collected to locate a *known* mobile device "as soon as that device is located, and no less than once daily" while mandating deletion of data collected by an IMSI Catcher for the purpose identifying an unknown device "as soon as the target cellular device is identified, and in any event no less than once every 30 days."[529] The Department of Homeland Security's policy imposes additional obligations, including an "auditing program" to ensure that data is indeed deleted in a timely manner.[530] The statutory framework for IMSI Catcher authorization adopted by the German criminal code likewise mandates that data of non-targeted "third persons" must "be deleted without delay" once the target mobile device sought is identified.[531]

A close corollary to the obligation to delete records which are no longer necessary for the purpose which they were collected is the need to strictly limit the potential uses of data about non-targeted individuals. The relationship between these two principles is illustrated in a 2015 Policy Directive of the United States Department of Homeland Security:

> An application for the use of a cell-site simulator should inform the court about how law enforcement intends to address deletion of data not associated with the target device. The application should also indicate that law enforcement will make no affirmative investigative use of any non-target data absent further order of the

[527] See discussion at **Section Three: C-iii 'Charter Principles of Incrementalism, Minimal Intrusion & Narrow Tailoring'**.

[528] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p 6; Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download, p 6.

[529] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, http://www.justice.gov/opa/file/767321/download, p 6.

[530] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p 7.

[531] *Criminal Procedure Code (Strafprozessordnung)*(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, sub-section 101i (2).

court, except to identify and distinguish the target device from other devices.[532]

Collaterally captured data on non-targeted individuals should be strictly limited in terms of its use to the sole function of confirming that the data is not in fact associated with the target of surveillance, thus identifying it for deletion. The only exception to this rule arises in the case of exculpatory evidence, which should be retained by law enforcement officers to the extent that they are aware of its existence. [533] The German statutory framework imposes a similar restriction, limiting use of any IMSI Catcher obtained data to determining the specific digital identifiers associated with a mobile device or the location of a device, while indicating that non-target third person data "may not be used for any purpose beyond the comparison of data in order to locate the device ID and card number sought, and the data is to be deleted without delay once the measure has been completed."[534]

Beyond the fact that these minimization protocols may be constitutionally required, they also reflect more general principles enshrined within existing Canadian privacy law. The *Privacy Act*, RSC 1985, c P-21, a quasi-constitutional statute, provides certain ancillary protections which supplement constitutional privacy protections, and applies to federal policing and other investigative bodies.[535] Specifically, the *Act* prevents state agencies from collecting personal information "unless it relates directly to an operating program or activity of the [agency]."[536] Federal law enforcement agencies may therefore only collect personal information necessary "to satisfy a legitimate law enforcement purpose."[537] In addition, the *Privacy Act* imposes restrictions on the retention of personal information, which must be disposed of in accordance with various directives and guidelines.[538] Use and disclosure of personal information for purposes unrelated to a

---

[532] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, p 6. The Department of Justice's policy imposes similar restrictions on use.

[533] Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved December 1, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, see footnote 6.

[534] *Criminal Procedure Code (Strafprozessordnung)*(StPo)(Germany), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I), http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, sub-section 101i (2).

[535] The *Privacy Act* is viewed as quasi-constitutional: *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403; *Lavigne v Canada (Office of the Commissioner of Official Languages)*, [2002] 2 SCR 773, 2002 SCC 53.

[536] *Privacy Act*, RSC 1985, c P-21, section 4.

[537] OPC Case Summary Privacy Act #2012-13-02, *Criminal Background Check on Tenant*, November 21, 2013, https://www.priv.gc.ca/cf-dc/pa/2012-13/pa_201213_02_e.asp.

[538] *Privacy Act*, RSC 1985, c P-21, sub-section 6(3).

specific program is also regulated,[539] and provincial public sector privacy statutes impose similar obligations onto provincial investigative agencies. Placing limitations such as those outlined in **Table 5** would be consistent with these legislative limits, as they have been designed to limit the collection, use, and retention of non-targeted mobile identifiers to what is necessary to identify or track the actual target of the search—that is to say, the legitimate object of the law enforcement purpose animating the interception.[540] In the absence of any policy or legislative changes that require the minimization protocols set out above, courts should nevertheless consider imposing such restraints when issuing an authorization for IMSI Catcher use to "ensure that privacy interests … are protected."[541]

Imposing explicit targeting and minimization requirements either through legislation or by judicial discretion at the IMSI Catcher authorization stage would therefore mitigate the otherwise significant and disproportionate collateral impact such devices tend to impose on non-targeted individual privacy, without unduly impeding state agencies in their efforts to achieve their legitimate objectives.

[539] *Privacy Act*, RSC 1985, c P-21.

[540] *In Re Use of Automated License Plate Recognition Technology by the Victoria Police Department*, Investigative Report F12-04, (BC IPC, 2012), pp 10, 23-24.

[541] *R v Gerrard*, [2003] OJ No 420, (ONSC), para 49; *R v Rogers Communications*, 2016 ONSC 70; *In Re An Application for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, (2015)(N Dist Illinois, West Div)..

Conclusion

Privacy is a fundamental right: it is essential to the proper functioning of any free and democratic society and, without it, people are less willing to speak or associate with others whom are regarded as 'risky' or 'deviant', or to explore ideas that might not be in line with mainstream beliefs.[542] They are less willing to communicate private, intimate, and sometimes embarrassing things to friends, family, and partners. In effect, the ability to move and speak without fearing unwarranted government surveillance is a basic condition of liberal democracies; a persistently monitored public is never truly free from its government.

This report, *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada*, has focused on how IMSI Catchers operate and the implications of these devices' use by Canadian authorities. It began by providing an overview of the devices' technical capabilities and concluded by identifying how state agencies could use the information collected by IMSI Catchers to subsequently re-identify otherwise (pseudo)anonymous activities. These activities included visiting different physical locations as well as communicating on the Internet using a mobile device. Subsequently, the report explored how IMSI Catchers are used and the efforts by members of the public to unmask such uses in jurisdictions including the United Kingdom, United States, and Canada. In both Canada and the United States, some information regarding the use of these devices has finally entered the public record, but only after significant efforts by civil society and journalists and after decades of secret use. Even after all these efforts, much remains unknown regarding the conditions under which these devices are used in Canada, in particular. Indeed, even after a substantial public record establishing IMSI Catcher use, many Canadian agencies remain unwilling to officially confirm such use, possibly as a result of non-disclosure agreements imposed onto them by IMSI Catcher vendors. This ongoing secrecy has the effect of delaying important public debates concerning these devices.

After exploring these transparency efforts, the report then explored the regulation of IMSI Catchers in the United States, Germany, and Canada. After conducting a brief comparative summary of restrictions imposed onto IMSI Catcher use by internal policies, legislatures and courts in the United States and Germany, it turned to

[542] Jon Penney, 2016, "Chilling Effects: Online Surveillance and Wikipedia Use", (2016) 31(1) *Berkeley Tech L J* 117, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645; Human Rights Watch & American Civil Liberties Union, "With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law & American Democracy", July 2014, *Human Rights Watch*, https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf; Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", (2016) *Journalism & Mass Communications Quarterly*, doi: 10.1177/1077699016630255; PEN America, 2015, "Global Chilling: The Impact of Mass Surveillance on International Writers", January 5, 2015, http://pen.org/global-chill.

analyzing the legal framework that might guide Canadian government agencies in their use of IMSI Catchers. It concludes that there are many potential powers that state agencies might rely upon in authorizing IMSI Catcher use, each with varying levels of privacy protection. Ultimately it is unclear which of these powers Canadian agencies will rely upon in different circumstances, further confounding attempts to analyze whether such use is properly constrained by law in Canada. The report then examines the potential *Charter* implications of IMSI Catcher use, concluding that some prior judicial authorization would be required for the lawful use of these devices, and additional safeguards may be constitutionally required.

The Report concludes by suggesting a number of best practices that should be adopted in order to ensure IMSI Catcher use remains reasonably proportionate in Canada. These best practices are distilled from safeguards imposed on these devices by other jurisdictions, from Canadian laws regarding other invasive electronic surveillance tools, and from *Charter* principles. They include:

- transparency measures designed to ensure the Canadian public is aware of and can track the use of these devices, which are anticipated to become more commonplace as device costs continue to drop;

- conditions intended to help ensure these devices are only deployed in proportionate circumstances; and

- minimization and targeting mechanisms designed to help limit the impact of these devices on non-targeted individuals.

Given the potential for IMSI Catchers to massively track Canadians who have done nothing wrong other than be near the surveillance device, it is imperative to ensure the aforementioned measures are in place. Moreover, given the uncertainties surrounding the multiple possible lawful authorization of IMSI Catchers in Canada it is critical that more transparency and accountability be demanded. The Governments of Canada have already adopted many of the proposed transparency and control mechanisms in relation to other invasive electronic surveillance techniques, such as wiretaps, and has done so without significantly impeding their ability to investigate crime. Extending this framework of protections, with some modification, to IMSI Catchers would be a logical step. Doing less will leave Canadians subject to modes of government surveillance that are highly intrusive, opaque in their use and usefulness, and non-transparent in terms of practical investigatory benefits. The lawful investigation and prosecution of criminal activities must be conducted in the clarity of public light so that justice is seen, and understood, as being done: cloaking

investigations and criminal proceedings in shadow only undermines trust and accountability in the justice process, and weakens citizens' belief in the trustworthiness of government authorities and the rule of law more generally. Moreover, putting in place such controls is essential to curtail the intrusive nature of IMSI Catchers which, by design, impact on the privacy of many for each legitimate target.