Communications Interception and Digital Searches in an Age of Encryption and Spyware: Are Canada's Laws Fit for Purpose?

A Report for the National Security and Intelligence Committee of Parliamentarians (NSICOP)

Vivek Krishnamurthy[*]
Draft—August 30, 2023

[*] I am grateful to Daniella Febbraro, a 2023 graduate of the University of Ottawa's Faculty of Law, Common Law Section, and to Leonhard Knebel, a law student at Ludwig-Maximillian University in Munich, Germany and graduate of Bavaria's First State Examination in Law, for their research assistance.

INTRODUCTION

This paper evaluates the adequacy of Canada's legal framework for authorizing the use of on-device investigative tools ("ODITs"—commonly known as "spyware") to intercept encrypted communications and retrieve data from encrypted devices for security & intelligence purposes.

Recent technological developments, notably the rise of end-to-end encrypted communications and of "full disk" encryption on computers and laptops, have led to security & intelligence and law enforcement agencies to rely on ODITs to fulfill the role once played by telephonic wiretapping and searches of physical premises. The role that ODITs plays in intelligence gathering and criminal investigations is likely to grow in the coming years as encryption becomes more prevalent, and quantum communications technologies come into wider use.

ODITs, however, pose much graver dangers to the constitutional and human rights of Canadians and foreign citizens alike than the techniques they replace. Even so, Canada's laws governing the use of such tools by government agencies have not kept up with these technological developments.

This paper will begin by providing an overview of the technological trends that are leading to the increasing use of ODITs by government agencies before turning to evaluate Canada's legal framework for authorizing the use of these fearsome tools. The legal analysis will consider relevant provisions of Canada's *Criminal Code,* the *CSIS Act,* and the *CSE Act,* in view of the close relationship that exists between law enforcement and security & intelligence agencies in many contexts. The paper will conclude by examining recent legal reforms in Germany which may provide Canada with an example to emulate in updating our laws to meet the challenges posed by a rapidly changing technological environment.

1. TECHNOLOGICAL AND HISTORICAL CONTEXT

Some historical context regarding the ability of government agencies to intercept communications is helpful in evaluating whether Canada's laws governing such activities are well-suited to our current technological reality. It remains easier today for government agencies to intercept communications in real time and access stored communications data that almost any other time in the last century. However, the rising prevalence of

encryption has made it relatively more difficult for such agencies to conduct digital investigations as compared to a decade ago.

An important reason why encryption is more prevalent today that a decade ago is as a reaction to Edward Snowden's exposé of unlawful mass surveillance activities conducted by the US National Security Agency.[1] It is an overstatement to say that things are "going dark" for government agencies due to the rise of encryption, however.[2] As explained below, such agencies have greater access to communications metadata than at most any other time in the last century. Furthermore, the alarming, widespread availability of "spyware" that can defeat most encryption technologies means that government agencies continue to be able to engage in targeted digital surveillance.[3] The challenge we face is how to appropriately govern the use of these terrifying new surveillance technologies, given they are likely to become more important over time with the anticipated growth of quantum communications technologies.

1.1. "Welcome to the 1980s"

One way to understand why government agencies have an easier time in intercepting and analyzing communications data today than at nearly any other time since the invention of the telegraph is to turn the clock back to 1980s, when the telephone was the dominant real-time communication technology.

The architecture of the conventional telephone network made it easy for government agencies to intercept phone calls and gather up what we now call communications metadata.[4] The

---

[1] Klint Finley, "Encrypted Web Traffic More Than Doubles After NSA Revelations," *Wired*, accessed August 28, 2023, https://www.wired.com/2014/05/sandvine-report/; Anthony Cuthbertson, "Snowden 'Sped Up Encryption' by Seven Years," *Newsweek*, April 26, 2016, https://www.newsweek.com/snowden-sped-encryption-seven-years-452688.

[2] Jonathan Zittrain et al., "Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Center Research Publication 2016-1, 2016, https://dash.harvard.edu/handle/1/28552576.

[3] Asaf Lubin, "Selling Surveillance," SSRN Scholarly Paper (Rochester, NY, 2023), https://doi.org/10.2139/ssrn.4323985.

[4] The Electronic Frontier Foundation, a leading digital rights organization based in San Francisco, describes metadata as follows:

> Metadata is often described as everything except the content of your communications. You can think of metadata as the digital equivalent of an envelope. Just like an envelope contains information about the sender, receiver, and destination of a message, so does metadata.

conventional telephone network has a centralized architecture where every line connects to a phone exchange.[5] Interception equipment could easily be installed at these exchanges. Indeed, all major telephone switching equipment manufacturers incorporated "lawful interception" capabilities into their products.[6] This is to help their customers (the former government-owned telephone monopolies) comply with legal requirements requiring them to incorporate interception capabilities into their switching equipment.[7] Furthermore, the fact that phone companies billed their customers based on the numbers they called (i.e., local vs. long distance) and the duration of those conversations created a set of records that government agencies could obtain from a few centralized entities to determine who is speaking with who.[8]

There were, however, significant logistical constraints on the ability of government agencies to intercept and analyze telephone communications in bulk. Phone calls had to be recorded on magnetic tape, and human analysts had to listen to them to determine what they said.[9] Indeed, throughout the 1980s, CSIS maintained a procedure of erasing tape recordings of phone conversations it had intercepted—presumably so the tapes could be reused—which led to the destruction of recordings of

---

> Metadata is information about the digital communications you send and receive. Some examples of metadata include:
> - the subject line of your emails
> - the length of your conversations
> - the time frame in which a conversation took place
> - your location when communicating (as well as with whom)

Electronic Frontier Foundation, "Why Metadata Matters," accessed August 30, 2023, https://ssd.eff.org/module/why-metadata-matters.

[5] "PSTN Network Topology," in *Wikipedia*, April 19, 2023, https://en.wikipedia.org/w/index.php?title=PSTN_network_topology&oldid=1150624186; "What Is PSTN and How It Works | Complete Guide [2022]," Telnyx, accessed August 28, 2023, https://telnyx.com/resources/what-is-pstn.

[6] "Lawful Interception (LI)," ETSI, accessed August 28, 2023, https://www.etsi.org/technologies/lawful-interception.

[7] Office of the Privacy Commissioner of Canada, "Response to the Government of Canada's Lawful Access Consultations (May 5, 2005)," July 8, 2005, https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_la_050505/.

[8] Note: in the domestic law enforcement context, such information could be gathered by the police using a production order, rather than a warrant. See Tele-Mobile Co. v. Ontario, 2008 SCC 12.

[9] The 2006 German film "The Lives of Others" ("Das Leben der Anderen") depicts, among other things, the vast scale of human and physical resources required for the Stasi, the despised East German intelligence agency, to conduct widescale telephonic surveillance of its own citizens in the 1980s.

conversations between the plotters of the 1985 Air India bombing.[10]

By contrast, digital storage is so cheap today that any data collected for any investigative purpose can be retained indefinitely from a cost perspective.[11] Moreover, digital tools such as voice recognition, machine translation, and analytics powered by artificial intelligence provide government agencies with automated tools to sift through reams of intercepted digital data, and identify items of interest that require further analysis by their personnel.[12] Indeed, from a logistical and cost perspective, it is feasible today for a government agency to intercept every digital communication sent to or from a given country, and to analyze those communications using automated tools for whatever happens to be of interest to the investigative authorities. For all these reasons, our age has been called the "golden age of surveillance" both by Prof. Peter Swire of Georgia Institute of Technology, who served as the Director of the U.S. National Intelligence Review Group on Intelligence and Communications Technologies during the Obama Administration,[13] and by Bruce Schneier of the Harvard Kennedy school, who is one of the world's leading security technologists.[14] This evaluation holds despite the slight decrease in the ability of government agencies to intercept and analyze digital data posed by the growing prevalence of encryption.

---

[10] "Erasing Wiretap Evidence Was 'default' CSIS Policy, Air India Inquiry Told," CBC News, September 19, 2007, https://www.cbc.ca/news/canada/erasing-wiretap-evidence-was-default-csis-policy-air-india-inquiry-told-1.631443.

[11] The cost of storing one hour of CD quality audio has fallen from $20,150 in 1985 to just 0.91¢ today. Author calculations based on "Historical Cost of Computer Memory and Storage," Our World in Data, accessed August 30, 2023, https://ourworldindata.org/grapher/historical-cost-of-computer-memory-and-storage.

[12] Vivek Krishnamurthy, "With Great (Computing) Power Comes Great (Human Rights) Responsibility: Cloud Computing and Human Rights," *Business and Human Rights Journal* 7, no. 2 (June 2022): 226–48, https://doi.org/10.1017/bhj.2022.8.

[13] Peter Swire, "The FBI Doesn't Need More Access: We're Already in the Golden Age of Surveillance," Just Security, November 17, 2014, https://www.justsecurity.org/17496/fbi-access-golden-age-surveillance/.

[14] Bruce Schneier, "Internet Has Delivered a 'Golden Age of Surveillance,'" *Schneier on Security* (blog), April 11, 2014, https://www.schneier.com/news/archives/2014/04/schneier_internet_ha.html.

1.2. The Rise of Encryption

There are growing concerns in some quarters that the increasing prevalence of encryption is frustrating the ability of government agencies from the law enforcement and security & intelligence communities to carry out their missions.[15] Evaluating these concerns requires some understanding of how encryption works. It also requires examining how much of a barrier encryption poses to the ability of government agencies to carry out their missions, given the availability of powerful new technologies that can undermine encryption.

Current encryption technologies can be divided into two major categories. The first category encrypts "data at rest" when it is stored on a digital storage medium.[16] For example, Apple's FileVault and Data Protection technologies encrypts the data stored on Macintosh computers and iOS devices by default.[17] Correspondingly, when government agencies seize such devices, they are unable to access the data stored upon them unless they are able to obtain the encryption password or use ODITs to undermine the encryption protections.[18]

The second category of these technologies encrypts "data in transit" as it is moving from a sender to recipient.[19] The most common form of encryption of "data in transit" is known as "transport-level security." This is the kind of encryption that is used to protect the security of Internet banking or of cloud-based services such as Gmail or Microsoft Office 365. The use of TLS prevents wiretaps of an internet connection (whether it is a cable, fiber optic, or cellular connection) from returning any intelligible data. Rather, the operator of the wiretap would obtain scrambled

---

[15] Stewart Baker, "How Long Will Unbreakable Commercial Encryption Last?," Lawfare, September 20, 2019, https://www.lawfaremedia.org/article/how-long-will-unbreakable-commercial-encryption-last.

[16] This brief description of how encryption works is based on the Electronic Frontier Foundation's excellent introductory guide. See Electronic Frontier Foundation, "What Should I Know About Encryption?," accessed August 30, 2023, https://ssd.eff.org/module/what-should-i-know-about-encryption.

[17] "Encryption and Data Protection Overview," Apple Support, accessed August 30, 2023, https://support.apple.com/guide/security/encryption-and-data-protection-overview-sece3bee0835/web.

[18] Ellen Nakashima and Reed Albergotti, "The FBI Wanted to Unlock the San Bernardino Shooter's IPhone. It Turned to a Little-Known Australian Firm.," *Washington Post*, April 14, 2021, https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/.

[19] Electronic Frontier Foundation, "What Should I Know About Encryption?"

data that is essentially impossible to decipher even with the use of the most powerful supercomputers.[20]

TLS is important to protecting the security and privacy of internet users against electronic eavesdropping, but data transmitted via TLS can be obtained by government agencies by other means. For example, the police may obtain a search warrant directed at Google requiring them to turn over the contents of my email account if I am suspected of a crime.[21] Likewise, the police can go to my bank to obtain my financial records even though my internet banking session was protected using TLS.

The other common form of encryption of "data in transit" is known as end-to-end encryption. This form of encryption prevents any intermediary between two parties from accessing the content of our communications.[22] For example, a message sent between two people using Signal, a popular end-to-end messaging platform, is rendered unintelligible to the operators of the Signal network, and to the many telecommunications companies who play a role in moving electronic messages between two parties.[23]

End-to-end encryption poses a more significant challenge to government agencies than TLS, because such agencies cannot obtain a copy of such communications from a service provider, as in the case of a cloud service such as Gmail or Dropbox. Depending on their architecture, government agencies may be able to obtain metadata from the operator of such services or an internet service provider about users of these services, but as we will see below, the communications themselves can only be obtained using "spyware."

Metadata is "data about data," and it is extremely valuable to all kinds of investigators. By contrast to the contents of a communication, which consist of what is said (whether by voice

---

[20] One estimate suggests that it would take a billion, billion years for a supercomputer using "brute force" techniques to crack the widely used AES-128 encryption algorithm. Mohit Arora, "How Secure Is AES Against Brute Force Attacks?," EE Times, accessed August 30, 2023, https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/.

[21] Google, "Requests for User Information FAQs - Transparency Report Help Center," accessed August 30, 2023, https://support.google.com/transparencyreport/answer/9713961.

[22] Electronic Frontier Foundation, "What Should I Know About Encryption?"

[23] John Snow, "Signal Is Secure, as Proven by Hackers," Kaspersky Daily, August 24, 2022, https://usa.kaspersky.com/blog/signal-hacked-but-still-secure/26949/.

or text), metadata consists of such information as the identities of the parties to the communication, their phone numbers or IP addresses, the duration of their communication, and information such as the subject line of an email, or the number of text messages exchanged between two parties.[24]

Metadata can be revealing of our most intimate characteristics. For example, a list of email addresses with whom you have corresponded reveals the individuals with whom you associate. To the extent that those individuals share certain characteristics (such as a common racial or sexual identity), much can be inferred about who you are.

Even so, there will be times that investigators will need access either to data stored on a device or to the contents of an encrypted communication for legitimate investigative purposes. For example, a criminal investigation into child sexual exploitation material (CSAM) will eventually require access to the underlying material in an unencrypted format, for the purposes of laying criminal charges and as evidence in a trial. It is not enough for such investigators to have access to metadata showing that a suspect is exchanging files with other known CSAM traffickers; at some point, access to the underlying data is required. This brings us to consider the policy options available to legislators to deal with the challenges posed by the rise of encryption.

2. DEALING WITH ENCRYPTION: THE MENU OF POLICY OPTIONS

There are three policy options available to governments to deal with the challenges posed by encryption of "data at rest" and "data in transit" to security & intelligence and law enforcement operations.

2.1. Banning Encryption

The first is to significantly restrict the use of advanced encryption technologies. In effect, one could mandate a return to the status quo that prevailed prior to the Snowden revelations, when encryption of data at rest and in transit were the exception, rather than the rule. For example, the Indian government recently banned 14 encrypted messaging apps, on grounds that they were

[24] Electronic Frontier Foundation, "Why Metadata Matters."

used by "terrorists" in the disputed territory of Jammu and Kashmir.[25]

Notwithstanding the significant constitutional issues associated with banning this class of technologies outright, or with significantly restricting their use,[26] legal restrictions on encryption are unlikely to advance the aims of the security & intelligence and law enforcement communities. Encryption technology is now widespread, and the genie cannot be put back in the bottle. Anyone who wishes to protect the security and privacy of its data and its communications will flout any restrictions on encryption to achieve their aims.

Moreover, whatever security benefits are gained from government agencies having an easier time in conducting investigations are more than offset by the cybersecurity risks posed to Canadian society by restricting encryption.[27] Advanced encryption technologies are essential to protecting the privacy and security of vital communications and the integrity of data by such important institutions as banks, hospitals, and educational institutions. Correspondingly, the notion of banning encryption to enhance public security is aptly characterized as a cure that is worse than the disease.

2.2. Mandating Exceptional Access

A second, less extreme option is to mandate certain technology companies to engineer "exceptional access points" into their encrypted communications and data storage systems to facilitate the work of government agencies.[28] Proponents of such measures

---

[25][25] "Govt Bans 14 Messaging, Calling Apps," Hindustan Times, May 1, 2023, https://www.hindustantimes.com/india-news/indian-government-bans-14-mobile-messaging-and-calling-apps-over-terrorist-communication-concerns-101682964848626.html.

[26] Steven Penney and Dylan Gibbs, "Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter," *McGill Law Journal* 63, no. 2 (n.d.): 201–45.

[27] Mieke Eoyang and Michael Garcia, "Weakened Encryption: The Threat to America's National Security," Third Way, accessed August 30, 2023, https://www.thirdway.org/report/weakened-encryption-the-threat-to-americas-national-security. Vivek Krishnamurthy, Devony Schmidt, and Amy Lehr, "Cybersecurity and Human Rights: Understanding the Connection," in *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals*, ed. Jonathan Andrew and Frédéric Bernard (Gordonsville: Hart Publishing, an imprint of Bloomsbury Publishing, 2021).

[28] Harold Abelson et al., "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of*

refer to them as providing government agencies with access to a "golden key" that can open digital locks in circumstances where they are warranted by law,[29] while their detractors refer to them as "backdoors" that create vulnerabilities that undermine the privacy and cybersecurity of all users of such services.[30]

While it seems reasonable at first glance to provide government agencies with technical means to overcome encryption when duly authorized by law, mandating "exceptional access points" into encrypted systems is very likely to undermine our national security as well as the privacy and cybersecurity of all Canadians.[31] Whenever a weak point is created in an electronic system with the intent of providing access to security & intelligence and law enforcement organizations operating under appropriate legal authorities, those same weak points can be exploited by adversaries ranging from foreign states to cyber criminals to engage in activities ranging from espionage to electronic warfare. As the Harvard Law School professor Jack Goldsmith put it, "every offensive cyber weapon is a potential chink in our cyber defence."[32]

Goldsmith's paradox applies with particular force given the lack of diversity in the hardware and software ecosystems that currently exist. Just like our foreign adversaries and the criminal and terrorist organizations we wish to undermine, we all use the

---

Cybersecurity, November 17, 2015, tyv009, https://doi.org/10.1093/cybsec/tyv009. Ioannis Kouvakas, "Changes to UK Surveillance Regime May Violate International Law," Just Security, August 22, 2023, https://www.justsecurity.org/87615/changes-to-uk-surveillance-regime-may-violate-international-law/.

[29] Editorial Board, "Opinion | Compromise Needed on Smartphone Encryption," *Washington Post*, October 3, 2014, https://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html.

[30] "Issue Brief: A 'Backdoor' to Encryption for Government Surveillance," *Center for Democracy and Technology* (blog), March 3, 2016, https://cdt.org/insights/issue-brief-a-backdoor-to-encryption-for-government-surveillance/.

[31] Abelson et al., "Keys under Doormats." Eoyang and Garcia, "Weakened Encryption." Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide," May 2018, https://tspace.library.utoronto.ca/handle/1807/94803.

[32] Jack Goldsmith, "Cyber Paradox: Every Offensive Weapon Is a (Potential) Chink in Our Defense -- and Vice Versa," Lawfare, April 12, 2014, https://www.lawfaremedia.org/article/cyber-paradox-every-offensive-weapon-potential-chink-our-defense-and-vice-versa.

same computing hardware and software to achieve our ends. Heads of state and the leaders of terrorist organizations all communicate on Meta's WhatsApp platform, for example, and Canadian government computers run Microsoft Windows just as those of organized cybercriminal groups. Correspondingly, the security risks of introducing "exceptional access points" into these systems far exceeds the benefits of doing so.

2.3. ODITs: the least bad option?

This brings us to the third policy option, which is to develop an appropriate legal framework to govern the use by security & intelligence and law enforcement agencies of digital tools that are colloquially known as "spyware" to bypass encryption and obtain data directly from the digital devices where they are stored.

ODITs run the gamut from "keyloggers" that monitor every keystroke a user inputs into a computer,[33] to such terrifying and controversial tools as the NSO Group's infamous Pegasus software suite, which allows its operators to retrieve every bit of data from an infected smart phone and turn its microphone, camera, and GPS into a fearsome real-time surveillance device.[34]

What all ODITs share in common is that they exploit errors and weaknesses in the programming and design of modern computing hardware and software to permit their operators to undermine a host of security precautions, including encryption.[35] While it is well-nigh impossible to use "brute force" techniques to decrypt a message that has been secured using modern encryption techniques, to err is human, and every computing device on the market contains vulnerabilities that permit sophisticated actors to bypass the most advanced cybersecurity

---

[33] "Keyloggers: How They Work & How to Detect Them - CrowdStrike," crowdstrike.com, accessed August 30, 2023, https://www.crowdstrike.com/cybersecurity-101/attack-types/keylogger/.

[34] Stephen Shankland, "Pegasus Spyware and Citizen Surveillance: Here's What You Should Know," CNET, accessed August 30, 2023, https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/.

[35] These weaknesses are known as "zero-day vulnerabilities" in the jargon of cybersecurity. "What Is a Zero-Day Attack? - Definition and Explanation," usa.kaspersky.com, June 30, 2023, https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit; Ravie Lakshmanan, "NSO Group Used 3 Zero-Click IPhone Exploits Against Human Rights Defenders," The Hacker News, April 20, 2023, https://thehackernews.com/2023/04/nso-group-used-3-zero-click-iphone.html.

protections that are currently in place. Correspondingly, copies of messages that have been sent using end-to-end encryption and which are stored on an encrypted device can be retrieved directly from a device using these advanced ODITs.[36]

Some of these tools require investigators to have physical possession of an encrypted device. This was the case with the software the FBI obtained from an Australian company called Azimuth to bypass the encryption that was used to protect the contents of an iPhone used by the deceased suspect of a terrorist attack in San Bernardino, California in 2015.[37] By contrast, tools like the NSO Group's Pegasus and the (now defunct) Hacking Team's Galileo suite permit their users to access the contents of a digital device remotely.[38] What is more, Pegasus contains well-documented capabilities that allow its operators to remotely turn on a user's microphone and camera and to monitor their communications on a real-time basis.[39]

The capabilities of tools like Pegasus are far more invasive of individual privacy than conventional wiretapping tools. To return to our example from the 1980s, an RCMP wiretap could monitor one's phone conversations, but this technology could not be used to listen into the conversations that one has in their home, or in a public park. Nor could a telephone wiretap be used to search every document in a suspect's residence, or read their mail, or take surreptitious photos and videos of them all day and night. Yet the most powerfully ODITs bundle all of these investigative techniques into a single tool.

ODITs like Pegasus have been implicated in serious abuses by governments with human rights records as varied as Spain and Saudi Arabia. In Spain, the intelligence services used Pegasus without appropriate legal authorization to monitor the communications of elected representatives in Catalonia who have

---

[36] Vincent Manancourt and Mark Scott, "Spyware Scandal Revives Push against Government Access to Encrypted Messages," *POLITICO* (blog), July 19, 2021, https://www.politico.eu/article/spyware-scandal-revives-push-against-government-access-to-encrypted-messages/.
[37] Nakashima and Albergotti, "The FBI Wanted to Unlock the San Bernardino Shooter's IPhone. It Turned to a Little-Known Australian Firm."
[38] Joseph Cox, "The FBI Spent $775K on Hacking Team's Spy Tools Since 2011," *Wired*, accessed August 30, 2023, https://www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011/.
[39] Ben Lovejoy, "Pegasus Screenshots Show It Secretly Activating Mic and Camera," 9to5Mac, August 5, 2022, https://9to5mac.com/2022/08/05/pegasus-screenshots/.

advocated for the region's independence from Spain.[40] Meanwhile, the Saudi authorities used Pegasus to spy on the dissident journalist Jamal Khasoggi, who was brutally murdered and dismembered by a team of Saudi intelligence agents in the kingdom's consulate in Istanbul.[41] Numerous other abuses of such tools have been exposed, notably their use by authoritarian governments to spy on journalists, dissidents, and even the heads of state of nuclear-armed nations.[42]

ODITs possess fearsome capabilities, and there is an urgent need to regulate the global trade in a vast variety of ODITs that are offered for sale by private entities.[43] Even so, ODITs currently represent the least bad of the three options available to deal with the challenges posed by pervasive encryption to the investigative capabilities of government agencies.

Compared to restricting encryption capabilities or mandating the inclusion of exceptional access points into encrypted systems, the use of ODITs creates fewer systemic cybersecurity risks—at least in our current technological moment. ODITs are certainly dangerously rife with the possibility of misuse, however they are targeted by their nature. That is to say, the operator of a ODIT must choose who they target with the technology, whereas the first two options create vulnerabilities in the systems used by everyone to permit security & intelligence and law enforcement agencies to achieve their investigative aims.

There is also an ongoing arms race between the developers of ODITs, and companies such as Apple, Meta, and Microsoft—who develop the world's most commonly-used computer hardware and software—to patch vulnerabilities that are used to make ODITs faster than ODIT manufacturers can find them.[44] This "arms race"

---

[40] Sarah Anne Aarup, "Pegasus Spyware Targets Top Catalan Politicians and Activists," *POLITICO* (blog), April 18, 2022, https://www.politico.eu/article/pegasus-spyware-targets-top-catalan-politicians-and-activists/.

[41] Ronen Bergman and Mark Mazzetti, "Israeli Companies Aided Saudi Spying Despite Khashoggi Killing," *The New York Times*, July 17, 2021, sec. World, https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html.

[42] "Pegasus: French President Macron Identified as Spyware Target - BBC News," accessed August 30, 2023, https://www.bbc.com/news/world-europe-57907258.

[43] Lubin, "Selling Surveillance."

[44] Taylor Armerding, "Apple's $1 Million Bug Bounty Could Launch Arms Race For Zero Days," Forbes, accessed August 30, 2023, https://www.forbes.com/sites/taylorarmerding/2019/08/15/bug-bounties-go-big/.

imposes some limits on the scale and prevalence with which ODITs can be deployed, as compared to the widescale cybersecurity risks that weakening encryption presents.

The reliance of government agencies on ODITs is likely to increase should quantum communications technologies come into wider use. Quantum communications systems leverage a principle of particle physics known as "entanglement" that makes it impossible for anyone to surreptitiously intercept communications as they make their way from a sender to a recipient.[45] In lay terms, attempting to intercept a quantum communication while it is being transmitted would automatically alert both the sender and the recipient that someone is trying to listen in, and prevent the transmission from taking place. Correspondingly, the only feasible way to intercept quantum communications is by installing ODITs on the devices that will be used by users to send and receive them —such as the keyboards on which such messages are typed, or the monitors on which the contents of such messages are displayed.[46]

For the foreseeable future, it is likely that security & intelligence and law enforcement agencies will need to rely upon ODITs to obtain access to encrypted digital communications. Correspondingly, the question facing policymakers is how to regulate these technologies that are so rife with the possibility of misuse to prevent their abuse. While it is beyond the scope of this paper to consider how the manufacture and sale of these technologies should be regulated, the final section will suggest some possible avenues of reform to Canada's relevant laws. However, the next section sketches out the current state of our laws that regulate the use of these technologies by government agencies.

3. CANADA'S INADEQUATE LAWS

This section examines Canada's current legislative framework for authorizing the use of ODITs. It is based entirely on public source material, including a review of the relevant statutes and court decisions interpreting them.

---

[45] Elizabeth Fernandez, "Practical Physics: How Quantum Uncertainty Will Make Our Communications Secure," *Big Think* (blog), October 18, 2022, https://bigthink.com/the-future/quantum-communications-secure/.
[46] Personal communication with Anne Broadbent, University Research Chair in Quantum Information Processing, University of Ottawa, November 14, 2022.

Unlike other leading democracies, Canada has not reformed its laws governing communications interception and other digital searches to address the profound challenges posed by law enforcement and security & intelligence agencies' use of ODITs. The current statutory framework for authorizing the use of these terrifyingly powerful tools is fragmented, and lacks appropriate oversight, transparency, and accountability mechanisms.

This section begins with an overview of the relevant *Criminal Code* provisions that authorize domestic law enforcement agencies to deploy ODITs for criminal investigative purposes. Even though NSICOP's role is to provide oversight of Canada's security & intelligence agencies, it is important to review the statutory authorities that permit domestic law enforcement agencies to deploy ODITs in their investigations, given the close collaboration that exists between law enforcement and security & intelligence agencies. It then proceeds to examine the provisions of the CSIS and *CSE Act*s that authorize the use of such tools by Canadian intelligence agencies.

3.1. *Criminal Code*

Part VI of the *Criminal Code* lays out the procedure for law enforcement agencies to use to intercept communications. It also establishes a series of offences that prohibit the interception of communications by anyone (whether a law enforcement official or not) when the established procedures are not followed.[47] These provisions apply to prospective interceptions of communications (e.g., wiretapping), rather than retrospective interceptions (e.g., a warrant to obtain emails stored by Google).[48]

In summary, the *Criminal Code* prohibits the interception of communications without the issuance of a warrant, save for certain exceptional circumstances. These requirements effectuate the guarantee provided by s. 8 of the *Charter of Rights and Freedoms* prohibiting unreasonable searches and seizures.

The general procedure for obtaining judicial authorization to intercept electronic communications is provided in sections 185 and 186. An application must be made to a Superior Court judge by the Provincial or Federal Attorneys-General (or their deputies or certain other designated officials) to a judge of a Superior

[47] *See Criminal Code*, s. 183.

[48] R v Jones, 2017 SCC 60 at para 69.

Court. To grant such an application, a Superior Court judge must be satisfied that:

1. There are reasonable grounds to believe that interception may assist the investigation of an offence;
2. It would be in the best interests of the administration of justice to give the authorization; and
3. Other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed, or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

The final criterion, known colloquially as an "exhaustion" requirement, does not apply to certain offences, such as terrorism-related and organized crime offences.[49]

Should the judge be satisfied that the agents of the state have met their burden, the judge may authorize the interception of communications for a period of 60 days. Such interceptions can be renewed or extended to a maximum of three years. (See sections 185(2), 185(3), 186(6), 186(7)). What is more, these general provisions permit a judge to issue related warrants or orders at the same time, if the judge is satisfied that they relate to the execution of the authorization. For example, a judge could issue a search warrant under section 487, or a warrant for a tracking device under section 492.1, at the same time as authorizing the interception of communications under this provision.

In addition to these general procedures, the *Criminal Code* sets forth several special and exceptional procedures to authorize the interception of communications. Three merit discussion here.

First, section 184.2 permits the interception of communications with the consent of one of the parties to the communication. This provision requires an agent of the state to apply to a judge for authorization, and demonstrate reasonable grounds to believe that (1) an offence has been or will be committed and (2) that information concerning the offence will be obtained through the interception sought.

Second, and relatedly, section 184.1 permits agents of the state to intercept private communications without a warrant to prevent bodily harm, so long as one of the parties to the communication

[49] *Criminal Code,* s. 185 (1.1).

consents to the interception, and there are reasonable grounds to believe that the party consenting to the interception is at risk of bodily harm.

Third, and most significantly, sections 184.4, 188, and 196 set forth provisions permitting the police to intercept communications without a warrant in certain emergency situations. Section 184.4 permits such interceptions if there are reasonable grounds to believe that:

1. the urgency of the situation is one where authorization could not be obtained with reasonable diligence;
2. the interception is immediately necessary to prevent an offence that would cause serious harm; and
3. one of the parties to the communication is the person likely to commit the offence.

Section 196.1 requires the authorities to provide notice to any person who was the "object" of an interception under section 184.4 within 90 days, subject to a procedure by which the Crown can ask a judge to delay such notifications to up to three years to protect an ongoing criminal investigation. For its part, section 188 permits a judge to whom an application has been made under sections 185-86 (the general communications interception provisions) to authorize such interceptions in writing for a period of up to 36 hours, when there is an urgent situation that would prevent an authorization from being obtained with reasonable diligence.

3.1.1. Discussion

What are we to make of these provisions? How can we tell whether they are adequate to the challenge of regulating the fearsome capabilities of ODITs in the hands of Canadian law enforcement authorities?

As noted earlier, Part VI of the *Criminal Code* applies to prospective interceptions of communications, rather than retrospective searches of stored communications. This reflects the former technological reality whereby intercepting communications in real time, such as by conducting a wiretap, was a very different act then obtaining records of past communications, such as by searching a suspect's home for incriminating letters. Part VI subjects real-time interceptions of communications to stringent safeguards on the theory that such

interceptions are the most serious invasion of privacy imaginable by the state in the exercise of its criminal law enforcement power.

Modern technologies such as ODITs scramble these assumptions. To begin with, ODITs blur the distinction between the prospective interception of communications, and the retrospective retrieval thereof, because the same tools are used to accomplish both aims. What is more, some of the most widely used ODIT software suites, such as the NSO's Pegasus spyware, incorporates numerous capabilities into a single package – from the real-time interception of communications to capabilities that permit a user's digital device to be turned into a real-time surveillance machine.[50] Furthermore, ODITs permit their users to access all of an individual's stored data – whether it is stored on the device itself, or accessible via a cloud computing service to which the device is connected. In lay terms, if an ODIT like Pegasus is installed on my phone, not only can you search the contents of my phone, but you could also search of my Gmail and Dropbox accounts as well, because they are all connected to my phone.

The *Criminal Code*, as it currently stands, does not reflect any of these technological realities. We now know from the ETHI Committee report into the RCMP's use of ODITs that such tools were used in 32 investigations targeting 49 devices in the period between 2017 and 2022.[51] We also know that the process for obtaining authorization for the use of these capabilities is convoluted. Given the current structure of the *Criminal Code*, law enforcement organizations must obtain multiple authorizations that invoke multiple provisions of the Code to use these tools.

One can argue that this complexity serves a protective function, inasmuch as it may be difficult for law enforcement agencies to put together an application to authorize the use of ODITs that will pass judicial muster. At the same time, however, the fact that so many scattered provisions of the *Criminal Code* must be used undermines transparency and accountability. Public reporting on the use of Part VI of the *Criminal Code* is based on which provisions of the Code are invoked.[52] Correspondingly, the lack of

---

[50] Shankland, "Pegasus Spyware and Citizen Surveillance."
[51] House of Commons, *Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues: Report of the Standing Committee on Access to Information, Privacy and Ethics* (November 2022) (Chair: John Brassard) at 22 ("ETHI Committee Report").
[52] Public Safety Canada, "2020 Annual Report on the Use of Electronic Surveillance," February 23, 2022,

specific provisions that are keyed to the use of these highly invasive tools makes it difficult for legislators and the public alike to understand how and when they are used in a criminal law context.

What is more, current *Criminal Code* provisions are not adequately keyed to the degree of invasion of privacy that certain ODIT capabilities pose. Consider video surveillance, which is governed by Section 487.01 of the *Criminal Code*. It is one thing for the authorities to install a covert video camera in a particular location for investigative purposes, but quite another for law enforcement to use ODITs to turn on the camera on a suspect's phone at will as they move through their environment.[53] Correspondingly, the *Criminal Code* needs to be updated and amended to reflect the nature of the capabilities that modern surveillance and investigative tools present, and the degree of interference with the right to privacy that they also pose.

3.2. *CSIS Act*

Like the *Criminal Code*, the *CSIS Act* contains no specific provisions dealing with the Service's use of ODITs. Unlike warrants to authorize the use of ODITs under the aegis of the *Criminal Code*, which require the invocation of multiple provisions to capture the operations of these tools, the *CSIS Act* provides the Service with broad yet general legal authorities in the service of its mission of protecting against threats to the security of Canada. The breadth and generality of these provisions make it difficult to determine how and when the Service employs ODITs, and whether the privacy rights of Canadian and foreign targets of CSIS investigations are being adequately protected when such tools are used.

Section 12 of the *CSIS Act* provides the Service with the power to collect, analyse, and retain information and intelligence "by investigation or otherwise" if it has reasonable grounds to suspect that an activity constitutes "a threat to the security of Canada."[54] If CSIS has reasonable grounds to so suspect, it can take measures, within or outside of Canada, to reduce the threat.[55] Such measures must be reasonable and proportional in the circumstances, and

---

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2022-nnl-rprt-lctrnc-srvllnc/index-en.aspx#sec2.

[53] ETHI Committee Report, p. 25.

[54] *CSIS Act*, section 12.

[55] *CSIS Act*, section 12.1.

they must comply with the *Charter.*[56] To the extent that CSIS measures impinge on *Charter* rights, the Service must obtain a judicial warrant to authorize such measures.[57]

In such cases, CSIS may apply to a judge for a warrant pursuant to the approval of the Minister of Public Safety and Emergency Preparedness.[58] A judge may issue such a warrant if they are satisfied that there are reasonable grounds to believe that a warrant is indeed required, and that one of three other conditions apply:

1. other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed,
2. that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures, or
3. that without a warrant it is likely that information of importance with respect to the threat to the security of Canada would not be obtained.[59]

If the relevant conditions are satisfied, a judge may issue a warrant authorizing CSIS to "intercept any communication or obtain any information, record, document, or thing" and, for that purpose:

1. enter any place or open or obtain access to any thing
2. search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or
3. install, maintain or remove any thing.[60]

These provisions would appear to provide CSIS with the ability to use ODITs to intercept communications in real-time and collect data from digital devices using a single authorization. While it is commendable that s. 21(1) of the *CSIS Act* incorporates an exhaustion requirement, the Act currently provides no guidance to the Service, its overseers, or the public on the circumstances in which different kinds of digital investigative capabilities may be legitimately used. Furthermore, there is currently no publicly available information on the use of ODITs by CSIS, which poses

[56] *CSIS Act*, section 12.1(3.1).
[57] *CSIS Act*, ss. 12.1(3.2).
[58] *CSIS Act*, s. 21(1).
[59] *CSIS Act*, s. 21(2).
[60] *CSIS Act*. s. 21(3).

challenges from both a transparency and accountability perspective.

3.3. *CSE Act*

Enacted in 2019, the *CSE Act* regulates Canada's signals intelligence agency. Little is known of the CSE's activities or capabilities, although it is likely that an agency of their size and sophistication is able to bypass the security protections of modern digital devices to access their contents.[61] In other words, it is likely that CSE possesses capabilities similar to those offered by the NSO Group's Pegasus spyware suite or its principal competitors, whether those have been procured on the open market or developed in-house.

While the passage of the *CSE Act* introduces some much-needed safeguards for the privacy of Canadians, it is not clear that the Act in its current form is up to the challenge of protecting the privacy rights of Canadians and foreigners alike in view of the fearsome capabilities of modern ODITs.

The *CSE Act* prohibits the Establishment from targeting any person in Canada or Canadians worldwide in the course of its operations,[62] but the information of such persons can be obtained by the CSE "incidentally" in the course of operations directed at foreign targets. [63] Indeed, such information about Canadians or persons in Canada, including intercepted private communications, can be disclosed by the CSE if it is essential to international affairs, defence, security, or cybersecurity, or if the disclosure is necessary to help protect the Canadian information infrastructure.[64]

The *CSE Act* requires the Establishment to ensure that measures are in place to protect the privacy of Canadians and of any persons in Canada,[65] but the Act does not require the Establishment to give any regard to the privacy of foreigners—even though the right to privacy is a universal human right.

---

[61] Dave Seglins, "Canada's Electronic Spy Agency's Cyberwarfare Toolbox Revealed," CBC News, March 23, 2015, https://www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978.

[62] *CSE Act*, section 22(1).

[63] *CSE Act*, section 23(4).

[64] *CSE Act*, section 43 and 44.

[65] *CSE Act*, section 24.

Unlike domestic law enforcement agencies and CSIS, which must obtain judicial authorization to engage in activities that presumptively interfere with *Charter* rights—such as digital device searches and communications interception—the activities of the CSE are authorized by the Minister of National Defence—either acting alone, with the approval of the Intelligence Commissioner, or pursuant to a request from the Minister of Foreign Affairs.

While as a signals intelligence agency CSE is understood to collect communications in bulk for analysis, the *CSE Act* appears to empower the Establishment to use ODITs if necessary. Specifically, section 26(2) permits CSE to "install[, maintain[], copy[], distribut[e], search[], modify[], disrupt[], delet[e] or intercept[] anything on or through the global information infrastructure" for the purposes of foreign intelligence operations. Section 31(b) empowers the CSE to engage in the same activities in conducting defensive or active cyber operations, while section 41 permits the Minister of National Defence to authorize such activities in emergencies. Little is known about how the CSE uses such authorities, however, and whether they have been invoked by the CSE for the use of capabilities associated with modern ODITs.

4. CONCLUSION

If ODITs are likely to remain the "least worst" option for security & intelligence and law enforcement agencies to deal with the challenges posed by encryption for the foreseeable future, how should Canada's laws be reformed to grapple with this reality? As demonstrated in the previous sections, the capabilities of ODITs pose much greater risks to the Charter and human rights of Canadians and foreigners alike than conventional investigative techniques. Correspondingly, our laws need to be reformed to appropriately govern the use of these technologies and restrict them to situations where they are truly needed.

Germany offers Canada a compelling example of how to reform our *Criminal Code* as well as the *CSIS* and *CSE Act*s to ensure that these powerful investigative tools are used only in appropriate circumstances.[66] The German Code of Criminal Procedure (StPO, to use its German abbreviation) was amended in 2017 to introduce

[66] The discussion below relies heavily on research and legal analysis conducted by my research assistant, Leonhard Knebel.

three new provisions that reflect how law enforcement conducts investigations in our digital age.[67]

First, section 100b of the StPO governs "intrusions" by law enforcement into IT systems to gather data stored on such a system. Law enforcement requests under this provision are evaluated not by the local courts and judges that authorize most other searches under the StPO, but rather by a specialist chamber of three judges who are forbidden to preside over criminal trials while they are serving in this capacity. Specialist judges are generally disfavored in the common law tradition,[68] but the knowledge that such judges may have regarding the operation and the invasiveness of the tools that are used to effectuate "intrusions" may allow them to better scrutinize the legitimacy and proportionality of authorization requests made under this provision.

Second, Section 100a of the StPO, which governs telecommunication surveillance, was recently amended to cover not just the real-time interception of communications, but the retrieval of encrypted communications stored on an online device. This provision of the StPO is available only for investigations of serious crimes and upon the satisfaction of an exhaustion requirement similar to those found in Part VI of the *Criminal Code*. In effect, this provision treats the retrieval of stored, encrypted communications on a digital device as the functional equivalent of a real-time wiretap, and subjects the former to the same legal protections as the latter. By contrast, under current Canadian law, a search of an electronic device is subject to the same legal regime as the search of any other place or thing – that is to say, it is not subject to an exhaustion requirement as with real-time communications interceptions.

Third, section 100c of the StPO, which governs audio and visual surveillance, specifically contemplates the use of ODITs to remotely activate an electronic device's microphone and a camera as a surveillance modality. What is more, section 100c effectuates

---

[67] Jenny Gesley, "Germany: Expanded Telecommunications Surveillance and Online Search Powers," web page, Library of Congress, September 7, 2017, https://www.loc.gov/item/global-legal-monitor/2017-09-07/germany-expanded-telecommunications-surveillance-and-online-search-powers/. An unofficial English translation of the relevant provisions of the stop is available at https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.

[68] Chad M. Oldfather, "Judging, Expertise, and the Rule of Law," SSRN Scholarly Paper (Rochester, NY, March 30, 2011), https://papers.ssrn.com/abstract=1799568.

the protections enshrined in Section 13 of Germany's Basic Law (essentially its *Charter of Rights and Freedoms*), which prohibit video surveillance inside residences as violative of the right to the inviolability of the home.

Recent German legal reforms also offer inspiration on how to reform the CSIS and *CSE Act*s to regulate the use by these agencies of powerful ODITs.

Germany's Law on the Federal Foreign Intelligence Service (BND-G) was amended in 2021 to specifically regulate "intrusion into IT systems" in its operations. Section 34 regulates the use of ODITs and related capabilities directed at foreign citizens in the operations of the BND—Germany's Foreign Intelligence Service. The use of such capabilities must be authorized by the President of the BND pursuant to an individual intelligence order that specifies, among other things, (1) the purpose of the collection of information, (2) the individual, group, or IT system targeted by the operation, (3) the approach, extent, and duration of the intrusion, and (4) a rationale for the operation.

In using such tools in their operations, the BND cannot target the "most sensitive areas of private life." Given that Germany's Basic Law applies to the German government in its operations around the world,[69] s. 34 of the BND-G recognizes and respects the right even of foreign intelligence targets to privacy in matters such as their family and romantic lives. Furthermore, s. 34 prohibits the use of ODITs to target confidential relationships such as those between a priest and a penitent, or a journalist and a source, unless the individuals in question are suspected of a serious crime or of threatening the security of Germany, the European Union, or of NATO.

As this Committee considers how to reform Canadian laws to reflect the digital reality in which we live, much inspiration can be drawn from how Germany has recently amended its laws to better balance the human rights of people everywhere with the

---

[69] Marcin Rojszczak, "Extraterritorial Bulk Surveillance after the German BND Act Judgment," *European Constitutional Law Review* 17, no. 1 (March 2021): 53–77, https://doi.org/10.1017/S1574019621000055. By contrast, Canadian courts have declined to extend the operation of the Charter of Rights and Freedoms outside of Canada in similar circumstances. See Leah West, "'Within or Outside Canada': The Charter's Application to the Extraterritorial Activities of the Canadian Security Intelligence Service," *University of Toronto Law Journal* 73, no. 1 (November 1, 2022): 1–52, https://doi.org/10.3138/utlj-2021-0105.

legitimate investigative needs of its government's investigative agencies.