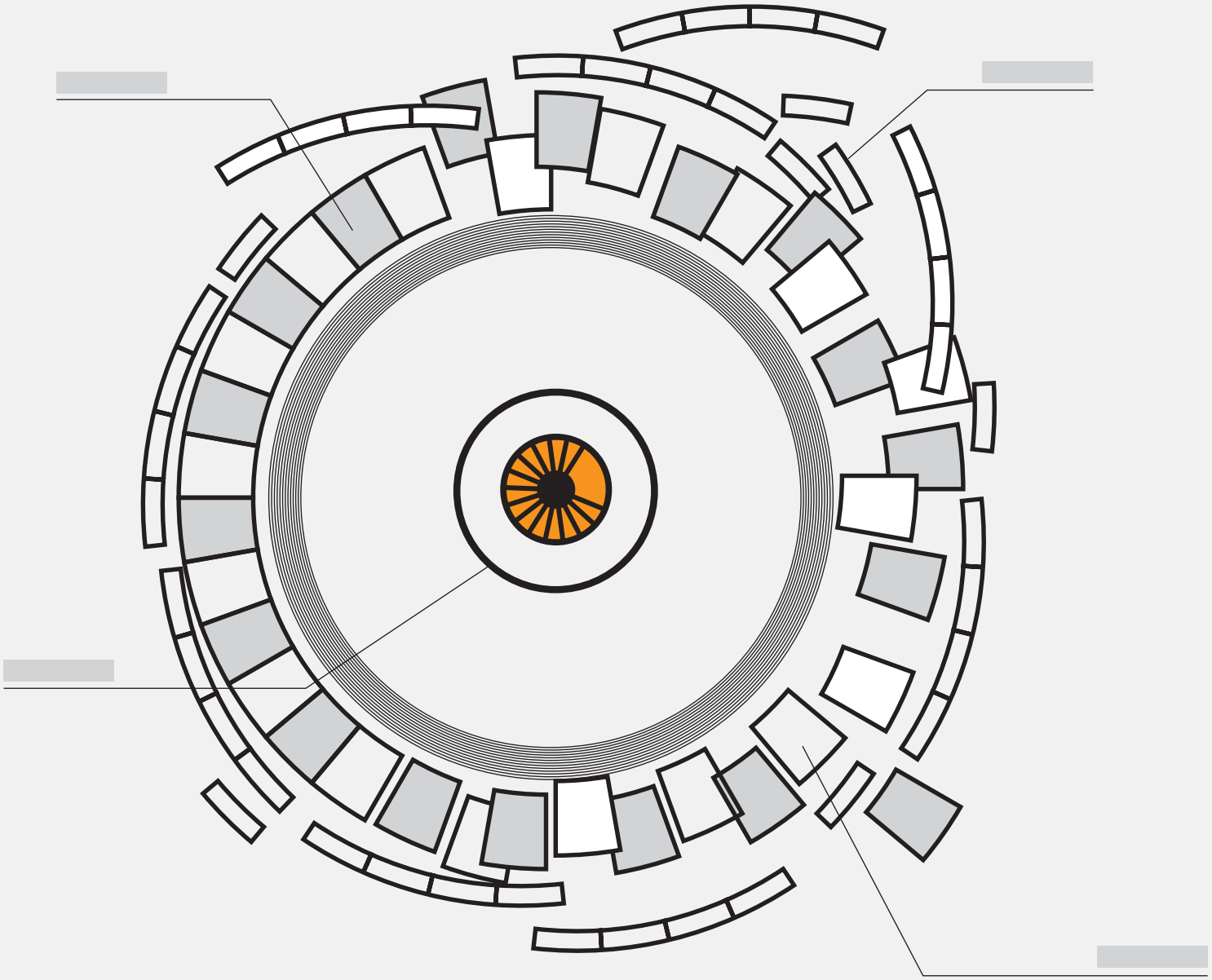

INSTALLING FEAR

A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications

By Cynthia Khoo, Kate Robertson, and Ronald Deibert

Research report #120
June 2019

THECITIZENLAB
munk school OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF TORONTO

This page is deliberately left blank

Copyright

Electronic version first published by Citizen Lab in 2019. This work can be accessed through https://citizenlab.ca.

Citizen Lab engages in research that investigates the intersection of digital technologies, law, and human rights.

Document Version: 1.0

Do you need help?

If you are in immediate danger, call 9-1-1 or your local emergency police department.

A Canada-wide directory of victim services, shelters, and other local organizations is available at the following web address:
http://www.justice.gc.ca/eng/cj-jp/victims-victimes/vsd-rsv/sch-rch.aspx

The Government of Canada maintains a list of information related to family violence, including a list of the specific resources available in provinces or territories, here:
http://www.justice.gc.ca/eng/cj-jp/fv-vf/help-aide.html

If you are concerned about your digital security or believe your device has been or is likely to become compromised, see the list of digital security guides and resources provided at the end of this report, in Appendix A.

This report does not provide legal advice. The intended audience of this report includes legal professionals, educators, technologists, social workers, journalists, and advocates in Canada. It is provided for general information purposes only, and it is not legal advice or a substitute for legal advice. Information contained in this report is accurate and current to the best of our knowledge on the date that it was published, but readers should be aware that the laws, their application, and court processes can change frequently and sometimes without notice. Anyone dealing with the legal issues discussed in this report is strongly encouraged to meet with a lawyer to review their rights, options, and legal obligations. Any use made of the information contained in this report is not the responsibility of the authors and does not create a client relationship with either the authors or the Citizen Lab.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

About the Authors

Cynthia Khoo is a Research Fellow and former Google Policy Fellow at the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto. She is a lawyer called to the Bar of Ontario, specializing in the intersection of technology and human rights. She is also completing an LL.M. (Concentration in Law and Technology) at the University of Ottawa, where she interned at the Canadian Internet Policy and Public Interest Clinic, and holds a J.D. from the University of Victoria Faculty of Law.

Kate Roberson is is a Citizen Lab Research Fellow, and a criminal defence lawyer at Markson Law in Toronto. Her practice includes both trial and appellate work, focusing on a range of criminal law cases, including white collar crime, sexual offences, and computer-based investigations and crime. She previously acted as a provincial Crown prosecutor in Ontario, and as a Law Clerk at the Supreme Court of Canada. She holds a J.D from the University of Toronto's Faculty of Law.

Ronald Deibert is a Professor of Political Science, and Director of the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto. He received his Master's from Queen's University and his Ph.D from the University of British Columbia. In 2013 he was appointed to the Order of Ontario.

Acknowledgements

The authors would like to extend their thanks and gratitude to a number of people who have provided support, feedback, and insights over the course of researching and writing this report.

In particular, we are grateful to Christopher Parsons, Siena Anstis, Suzie Dunn, Maya Ganesh, Pam Hrick, Tamir Israel, Miles Kenyon, Jeffrey Knockel, Etienne Maynier, Adam Molnar, and Rhiannon Wong, for their invaluable insights as reviewers of this report.

Our wholehearted thanks to Lex Gill for spearheading this project in its initial stages.

We also extend our appreciation to Chelsey Legge, who supported this research in its initial stages as a clinical student through the International Human Rights Program at the University of Toronto.

Thank you to Mari Zhou, who designed this document.

We are indebted to our colleagues Jakub Dalek, Bennett Haselton, Miles Kenyon, Jeffrey Knockel, Adam Molnar, and Christopher Parsons for their findings detailed in an accompanying report published by the Citizen Lab, “The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry.”

We are further grateful to the individuals and organizations which gave us the opportunity to share early versions of this work and provided input, including participants in the “Evaluating Stalkerware” workshop at the 2018 Citizen Lab Summer Institute.

Finally, the authors would like to offer our sincere thanks to Open Society Foundations, John D. and Catherine T. MacArthur Foundation, Ford Foundation, the Sigrid Rausing Trust, and the Oak Foundation, as well as the Office of the Privacy Commissioner of Canada’s Contributions Program, whose generous funding made this report possible.

Corrections And Questions

Please send all questions and corrections to the authors directly at:

cynthia@citizenlab.ca
kate@citizenlab.ca

Suggested Citation

Cynthia Khoo, Kate Robertson, and Ronald Deibert. “Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications,” Citizen Lab Research Report No. 120, University of Toronto, June 2019.

Contents

Contents

Information Boxes

Table of Acronyms

ACM	Association for Computing Machinery
AMP	Administrative Monetary Penalty
API	Application Programming Interface
AWS	Amazon Web Services
CASL	Canada's Anti-Spam Legislation
CCPSA	*Canada Consumer Product Safety Act*
CEDAW	*Convention on the Elimination of All Forms of Discrimination Against Women*
DFV	Domestic and Family Violence
DIY	Do-It-Yourself
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EULA	End-User License Agreement
FIPPA	*Freedom of Information and Protection of Privacy Act*
GBPHR	*Guiding Principles on Business and Human Rights*
GDPR	General Data Protection Regulation
GPS	Global Positioning System
ICCPR	*International Covenant on Civil and Political Rights*
ICESCR	*International Covenant on Economic, Social and Cultural Rights*
IEEE	Institute of Electrical and Electronics Engineers
IIMS	Intentional Infliction of Mental Suffering
IPS	Intimate Partner Surveillance
IPV	Intimate Partner Violence
NNEDV	National Network to End Domestic Violence
OIPC BC	Office of the Information and Privacy Commissioner for British Columbia
OIPRD	Office of the Independent Police Review Director
OPC	Office of the Privacy Commissioner of Canada
PIPA	*Personal Information Protection Act*
PIPEDA	*Personal Information Protection and Electronic Documents Act*
SMS	Short Message Service
STS	Science and Technology Studies
ToS	Terms of Service
TRIPS	*Agreement on Trade-Related Aspects of Intellectual Property Rights*
UDHR	Universal Declaration of Human Rights
UDID	Unique Device Identifier
UNCRC	United Nations Convention on the Rights of the Child
UNICEF	United Nations International Children's Emergency Fund
VPN	Virtual Private Network

This page is deliberately left blank

Executive Summary

This report provides an in-depth legal and policy analysis of technology-facilitated intimate partner surveillance (IPS) under Canadian law. In particular, the analysis focuses on a growing marketplace of spyware products that exists online and in major software application (app) stores. These apps are designed to facilitate remote surveillance of an individual's mobile device use with the surveillance often being covert or advertised as such. Despite increasing recognition of the prevalence of technology-enabled intimate partner abuse and harassment, the legality of the creation, sale, and use of consumer-level spyware apps has not yet been closely considered by Canadian courts, legislators, or regulators.

Spyware and other forms of technology that facilitate IPS are sometimes referred to as **stalkerware**. In some circumstances, stalkerware technology is used in an intimate relationship to conduct powerfully intrusive covert or coerced surveillance of an intimate or former partner's mobile device without their knowledge. Once installed, stalkerware apps allow an operator to access an array of intimately personal information about the surveillance target. The apps can enable real-time and remote access to text messages, emails, photos, videos, incoming and outgoing phone calls, GPS location, banking or other account passwords, social media accounts, and more. Stalkerware apps are sometimes used covertly while, in other circumstances, the technology is used openly to intimidate, harass, or extort the surveillance target.

Hundreds of spyware apps relevant to IPS are available at the consumer level. Research conducted in Canada and internationally suggests that a significant proportion of women who experience intimate partner violence, abuse, and harassment also report experiences with a range of technology-facilitated abuse, including surveillance and abuse that is enabled by the powerful mobile device spyware apps that are the focus of this report. Despite this troubling context, few reported cases involving spyware-enabled IPS have appeared in Canadian courts, and spyware companies, which profit from the sale of these apps, appear to operate in the Canadian marketplace without being hindered by criminal or regulatory law enforcement.

This report conducts an in-depth analysis of the criminal, regulatory, and civil law consequences of using, creating, selling, or facilitating the sale of stalkerware technology in Canada. The analysis concludes that the creation, use, and sale of spyware apps that enable covert surveillance of mobile devices can potentially

violate numerous criminal, civil, privacy, and regulatory laws in Canada. With respect to the criminal law, notably, purchasing and selling spyware that is primarily useful for surreptitiously intercepting private communications (as many of the major consumer-level spyware products do), likely constitute a criminal offence in Canada. These offences expose vendors and operators of spyware products to the risk of criminal law consequences, such as jail.

Operators of stalkerware are also subject to civil liability if they are found to have perpetrated a tort (wrongful act). Targeted individuals may bring a cause of action (lawsuit) against an operator on legal grounds of: invasion of privacy, public disclosure of private facts, breach of confidence, and intentional infliction of mental suffering (IIMS). We also briefly discuss non-intentional torts and assess the emerging novel tort of harassment as a potential additional response to stalkerware.

Our legal analysis found that the act of making and selling—as opposed to using—spyware products likely also runs afoul of both criminal and product liability law with respect to dangerous or defective product design. We also review the applicability of non-binding instruments such as the *United Nations Guiding Principles on Business and Human Rights* and industry efforts at self-regulation, including ethical codes and internal worker resistance in the technology sector. We consider, briefly, the limited applicability of intellectual property laws to impeding the creation and dissemination of stalkerware.

Canadian consumer privacy and data protection law, governed by the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), and substantially similar provincial legislation, includes several provisions regarding informed consent, notice, and appropriate purposes that would apply to stalkerware businesses and likely render their activities unlawful. We find that PIPEDA includes three potential exceptions, or loopholes, that may allow stalkerware vendors to circumvent accountability. We recommend that the Office of the Privacy Commissioner of Canada or federal and provincial legislators take action to close these potential gaps.

App stores and web platforms that sell apps to consumers also play a role as intermediaries that can facilitate sales of stalkerware through their platforms. Despite active efforts by companies such as Apple and Google to enforce app developer policies and agreements against such apps, research shows evidence of a continued, albeit decreased, presence and availability of stalkerware on popular app stores. We recommend that all app stores clarify their relevant policies and

revise developer terms of agreement regarding user privacy, consent, security, and malicious behaviour to expressly state that such protective policies apply to the individual whose data is being collected, processed, or disclosed by the app in every case, instead of referring simply to a generic 'user'. The generic term 'user' can inappropriately or incorrectly be interpreted as referring to the stalkerware operator rather than the targeted individual.

Despite the available data about the prevalence of IPS and technology-facilitated abuse and harassment in Canada and its impact on victims and gender equality rights more broadly, there appears to be a significant measurable gap between what the law dictates about such conduct and whether legal remedies are readily available to victims in practice. One complicating factor is that many spyware apps market themselves as, or are genuinely intended as, apps for ostensibly legitimate purposes, such as child and employee monitoring. Such apps are then repurposed into stalkerware for abusive purposes. Similar repurposing occurs with non-spyware apps or built-in phone features such as a GPS tracker, which abusive operators may manipulate or repurpose into stalkerware. We discuss this dual-use nature of spyware technologies, and critique the legitimacy of dual-use spyware even where such technology is used to surveil children or employees.

The report concludes by recommending a range of measures that relate to public legal education, law reform, heightened investigative and regulatory scrutiny of consumer spyware markets, and enhanced training and resources for law enforcement, regulators, and other justice system participants who are tasked with enforcing Canada's laws. Given stalkerware's inherent dangers and invasive capabilities and the documented association between stalkerware apps and intimate partner violence and gender-based abuse, justice system participants and the private technology sector bear a responsibility to establish and reinforce a web of meaningful restraints that address and remedy the harms of stalkerware, both in law and in practice.

Our purpose in this report is to contribute to greater substantive efforts to address technology-facilitated gender-based abuse in Canada, beginning with the harms and violence that stalkerware enables through its covert or exploitative surveillance of targeted individuals. The critical analysis provided in this report is designed to enhance public understanding of legal remedies, policy considerations, and human rights concerns associated with stalkerware. The report is also designed to provide assistance to policymakers, legal professionals, academics, community workers, and advocates who are trying to support victims or navigate the complex implications of this technology.

Introduction

In this report, we examine commercial spyware applications that can facilitate surveillance of an individual's daily and online activities through their mobile device. When used in the context of intimate partner violence, abuse, or harassment, or gender-based abuse, this technology is referred to as **stalkerware**. Such software grants an operator unauthorized remote access to a device and often compromises it without the knowledge or consent of the device owner, the targeted individual. On this basis, stalkerware may be considered a form of malware, against which digital devices and personal data must be secured.

While the use of stalkerware often occurs surreptitiously, there are times where the surveillance target may have limited knowledge that the stalkerware operator has some access to their personal information, but the operator engages in a form of surveillance that goes far beyond the scope of the target's knowledge or consent. In other contexts, the use of stalkerware applications may occur with the full knowledge of the surveillance target, but the operator uses the stalkerware application itself as a fear-inducing form of criminal harassment. It is important to recognize each of these three distinct contexts because where a target's privacy is invaded, the laws that govern and regulate such conduct generally require meaningful and informed consent from the target—not reluctant or partial agreement that is the product of intimidation, coercion, or exploitation of a position of power.

Stalkerware apps are part of a broader web of technology-facilitated, gender-based abuse and violence against women and girls.[1] From a legal perspective, stalkerware applications are closely connected to other forms of surveillance devices—such as tracking devices, hidden microphones, and nanny cams—which are used in the course of intimate partner violence, abuse, and harassment. The use of stalkerware apps is also similar to technology-facilitated abuse that occurs through the exploitation of the native features of Internet-based communications platforms and smart devices, which are not primarily directed towards abusive surveillance, but are nevertheless vulnerable to being exploited for the purpose of intimate partner surveillance and coercive control. As the Internet of Things has expanded the extent to which technology is interwoven with daily life, the opportunities for surveillance

1 Online and technology-facilitated violence, abuse, and harassment can take many forms. Such abuse can include, but is not limited to, cyberstalking, harassment, hacking, denial-of-service attacks, the use of gender-based slurs, the publication of private and identifiable personal information—often home addresses ("doxing")—impersonation, extortion, rape and death threats, electronically enabled trafficking, and sexual exploitation or luring of minors. See, for example, *R. v. A (BL), 2015 BCPC 203* and *R. v. J.T.B., 2018 ONSC 2422*.

using such technologies has also expanded, such as using smart home devices to perpetrate intimate partner surveillance and abuse.[2] Stalkerware applications are also linked to other more traditional forms of surveillance behaviour in the intimate partner violence context. These traditional forms include control or monitoring of shared banking services and phone accounts and disrupting access to a mobile device within a home that would otherwise be used to call 911 or a local police service for help.

This report focuses primarily on the particular form of technology-facilitated violence, abuse, and harassment that is enabled by the creation, sale, installation, and/or use of spyware that is used to remotely monitor a targeted person's activities and locations by compromising their mobile device. However, much of this analysis is applicable to other forms of intimate partner surveillance.

While we have elected to use predominantly gender-neutral terminology in this report, the use of stalkerware applications may be understood as part of a larger societal dynamic of gender-based violence and abuse, including violence against women and girls.[3] This abuse may occur within the context of intimate partner violence, abuse, and harassment in a pre-existing relationship, or the technology may be used to target ex-partners or acquaintances. Discrimination on the basis of gender identity, gender expression, sexual orientation, disability, race, ethnicity, Indigenous status, age, religion, and other factors also compounds, exacerbates and complicates experiences of gender-based violence, abuse, and harassment.[4]

Online and technology-facilitated violence, abuse, and harassment may include the following harms:

- Physical harm, such as stress-related illness, injury, and physical trauma;[5]

2 The New York Times, "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse," *The New York Times* (23 June 2018) <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>; Takara Small, "How Smart Home Systems & Tech Have Created A New Form Of Abuse," *Refinery 29* (9 January 2019) <https://www.refinery29.com/en-ca/2019/01/220847/domestic-abuse-violence-harassment-smart-home-monitoring>.

3 A federal study of deaths resulting from domestic violence in Canada between 2010 and 2015 found that women accounted for 79% of adults killed, while men accounted for 86% of accused attackers: Zosia Bielski, "Federal report finds 476 people died of domestic violence in Canada between 2010 and 2015," *The Globe and Mail* (6 December 2018) <https://www.theglobeandmail.com/canada/article-federal-report-finds-476-people-died-of-domestic-violence-in-canada/>.

4 Citizen Lab (Munk School of Global Affairs, University of Toronto), Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović (2 November 2017) <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf>.

5 For example, the link between intimate partner violence and spyware is evident in reported cases in the USA "where perpetrators used spyware to track down partners, with the result of them murdering those individuals and sometimes also their children": Diarmaid Harkin, Adam

- Psychological or emotional harm, such as experiences of shame, stress, fear, loss of dignity, costs to social standing, and trauma-induced psychological illness;
- Financial harm, including costs related to legal support, online protection services, missed wages, and professional consequences; and
- Consequential harms that flow from the interference with human rights and civil liberties, including increased need for health care, judicial, and social services; impediments to the exercise of free expression, the right to privacy, and other human rights central to one's autonomy and human dignity; and disturbance to the sense of peace and security required to fully participate in economic, social, and democratic life.[6]

A cross-Canada survey of programs that support women and children who have escaped or are living in violent situations noted 18 forms of technology-facilitated abuse, including: breaking into and monitoring instant-messaging accounts (46%); breaking into e-mail, social media, and other online accounts (72%); impersonating the targeted individual or someone they know over e-mail, another online platform, or other technology (69%); breaking into the victim's computer to monitor activities and extract information (61%); installing spyware and keystroke loggers (31%); non-consensual intimate image and video distribution (60% and 31%, respectively); covert surveillance and surreptitious recording of the target through a hidden camera or webcam (31%); and location tracking via GPS or another means (50%).[7]

The problem of technology-facilitated abuse towards women and girls is not limited to Canada. In 2014, National Public Radio (NPR) surveyed 72 domestic violence shelters in the United States about cyberstalking and found that 85% of shelters were "working directly with victims whose abusers tracked them using GPS," while 75% of shelters were "working with victims whose abusers eavesdropped on their conversation remotely — using hidden mobile apps."[8] These findings align with "a

Molnar, and Erica Vowles, "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," (2019) *Crime Media Culture* at p. 5.

6 Citizen Lab (Munk School of Global Affairs, University of Toronto), Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović (2 November 2017) <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf> at 2-3 (footnotes omitted).

7 Cynthia Fraser, Rhiannon Wong & NNEDV Safety Net Project, "Organizational Technology Practices For Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children," *Safety Net Canada* (2013) <https://bcsth.ca/wp-content/uploads/2016/10/Organizational-Technology-Practices-for-Anti%E2%80%90Violence-Programs.-Protecting-the-Safety-Privacy-Confidentiality-of-Women-Youth-Children_BCSTH-SNC-2013.pdf> at p. 19.

8 Aarti Shahani, "Smartphones Are Used To Stalk, Control Domestic Abuse Victims," *National Public Radio* (15 September 2014) <http://www.npr.org/sections/alltechconsid-

2012 survey of 750 victim services agencies, [which found that] 75% of domestic violence survivors experience tracking of their location through their cell phones or a GPS device."[9] Moreover, as Danielle Citron has noted, "[t]he National Network to End Domestic Violence found that 71% of domestic abusers monitor survivors' computer activities, and 54% of abusers tracked survivors' cell phones with stalking apps;" furthermore, a "2014 study sponsored by Digital Trust found that more than 50% of abusive partners used spyware or some other form of electronic surveillance to stalk victims."[10]

Academics, researchers, and advocates in the field of intimate partner violence, abuse, and harassment have noted the dearth of resources and training among support workers, police services, and the legal system more broadly to address technology-facilitated gender-based abuse and harassment.[11] In some cases, systemic bias or experiences of police violence create additional barriers that limit women's options in seeking the support of law enforcement.[12]

Our purpose in this report is to contribute to greater substantive efforts to address technology-facilitated gender-based violence, abuse, and harassment in Canada, beginning with the harms and violence that stalkerware enables through its covert or exploitative surveillance of targeted individuals.

---

ered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abusevictims>.

9 Danielle Keats Citron, "Spying Inc.," (2015) 72(3) *Washington and Lee L Rev* 1243 at 1251.

10 *Ibid*.

11 "Even when stalking victims suspect that their phones are being monitored, their complaints to law enforcement are seldom pursued. Police departments often lack the forensic equipment necessary to examine mobile devices for stalking apps. Reports often go nowhere because domestic violence and stalking are low priorities for law enforcement. Police officers receive little training on the relevant laws and the technology necessary to investigate such crimes. Because both the law and the technology are not well understood, law enforcement does little beyond advising victims to get rid of their phones. Resources to fund digital forensic investigations are especially scarce at the state and local level. Then too, the lack of cooperation between jurisdictions may prevent the apprehension of stalkers": Danielle Keats Citron, "Spying Inc.," (2015) 72(3) *Washington and Lee L Rev* 1243 at 1249 (footnotes omitted; see also at 1250-51); and Citizen Lab (Munk School of Global Affairs, University of Toronto), Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović (2 November 2017) <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSR-VAG-CitizenLab.pdf> at 16.

12 The extent to which domestic abuse occurs within law enforcement families is also important to note in examining law enforcement responses to technology-facilitated abuse. See: CBC News, "Study urged of domestic violence among police," *CBC News* (8 January 2013) <https://www.cbc.ca/news/canada/nova-scotia/study-urged-of-domestic-violence-among-police-1.1360548>; and Melissa Jeltsen and Dana Liebelson, "The Super Predators," *HuffPost* (21 June 2017) <https://highline.huffingtonpost.com/articles/en/police-domestic-violence/>. Some studies have indicated that women in around 40% of police officer families experience domestic violence: Rafaqat Cheema, "Black and Blue Bloods: Protecting Police Officer Families from Domestic Violence," (2016) 54 *Fam Ct Rev* 487. See also: Joseph Cox, "Military, FBI, and ICE Are Customers of Controversial 'Stalkerware'," *Motherboard* (23 February 2018) <https://motherboard.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware>.

Information Box 1: A Note on Terminology in Discussing Technology, Gender, and Violence

In discussing forms of intimate partner violence, abuse, and harassment, as well as gender-based violence, abuse, and harassment, the relevant literature, scholarship, and resources have adopted a range of terms to describe the issue in question.[13] Such terms include, for example, 'gender-based abuse', 'intimate partner violence', 'intimate partner abuse', 'domestic violence', 'domestic abuse', 'family violence', and 'domestic and family violence' (DFV). We recognize that these terms reflect different nuances and connote qualitatively distinct meanings in communicating the harms, dynamics, and impacts of this form of violence and abuse. We do not make any determinations regarding such distinctions; rather, we seek here to explain our own terminology choices for the purpose of this report.

Where we discuss violence or abuse between intimate partners or former partners, we have elected to use the term "intimate partner violence, abuse, and harassment" to indicate a spectrum of harmful behaviours within which certain activities may fall. However, throughout the report we also use the terms "intimate partner abuse" and "intimate partner violence," in part for greater concision and to capture both meanings in the event they are not considered interchangeable. We also use the terms "gender-based violence," "gender-based abuse," and "gender-based violence, abuse, and harassment" where the subject of discussion is not limited to the context of intimate or former partners.

The introduction of technology and the Internet as tools with which to perpetrate further violence and abuse has also given rise to many terms to describe the particular intersection of technology and gender-based violence. Such terms include, for example, 'technology-facilitated coercive control',[14] 'technology-facilitated domestic and family violence', 'technology-facilitated gender-based abuse', and 'technology-facilitated violence'. In this report, we use the term "technology-facilitated gender-based abuse" or "technology-facilitated gender-based violence" to indicate as broadly as possible the range of issues and harmful behaviours located at the intersection of technology, gender, and violence.

Where we discuss the issue or activity of individuals tracking or monitoring intimate or former partners, we use the term "intimate partner surveillance" (IPS). We also at times use the term "stalkerware-facilitated abuse" or "stalkerware abuse" to highlight the role of this type of technology, as the central focus of this report, in contributing to intimate partner and gender-based violence, abuse, and harassment.

In referring to victims and survivors of intimate partner or gender-based violence, abuse, and harassment, we at times rely on the legal term of art relevant to the analysis being undertaken. For example, the criminal law section may refer to the "complainant," while the data protection analysis may speak of "data subjects." For the most part, however, we refer to the "targeted person" or the "targeted individual" to indicate the person who is being subjected to surveillance through stalkerware. Neither the use of these terms, nor any reference to a "victim," should be read to suggest removal of agency from individuals who have experienced gender-based or intimate partner violence, abuse, or harassment.

13 See generally the scholarship highlighted in the literature review at the end of this Introduction, in Section E.

14 Molly Dragiewicz, et al, "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms," (2018) 18(4) *Feminist Media Studies* 609.

A. Structure of this Report

The remainder of this introductory section provides background information about what stalkerware is, what it can do, and how it is deployed. We also explain the research methodology used in this report.

The analysis in this report is divided into four parts, each of which examines a different form of liability for harm caused by stalkerware. The parts are arranged into the following categories: (1) an operator's *use* of stalkerware, (2) actors who *create and develop* stalkerware, (3) actors who *sell* stalkerware, and (4) third-party intermediaries who *facilitate the sale* of stalkerware. Our goal is to present a comprehensive review of the legal issues that arise in connection with stalkerware and the abuse it engenders. However, unless expressly stated, discussion of a particular area of law does not necessarily equate to endorsing the use of that law to address the harms arising from stalkerware and related gender-based or intimate partner violence, abuse, and harassment. This is because public policy or broader considerations may make it inadvisable to turn to a particular area of law to remediate the stalkerware problem.

Part 1 (Using Stalkerware) provides a legal analysis of the use of stalkerware by individuals. The use of stalkerware technology may contravene numerous criminal laws in the Canadian *Criminal Code*, and may constitute a number of torts that may render an operator of stalkerware technology liable for civil damages.

Part 2 (Creating and Developing Stalkerware) focuses on the creation and development of stalkerware. This section discusses relevant human rights obligations, self-regulation within the technology sector, and corporate social responsibility, and situates stalkerware against a social and political backdrop of rising calls for ethical conduct and stronger human rights accountability from the technology sector. This section then analyzes stalkerware through the lens of criminal liability, product liability, and intellectual property law.

Part 3 (Selling Stalkerware) analyzes the legal issues associated with sale of stalkerware as a commercial business. This section attends to the civil and criminal liability of stalkerware vendors and of developers who sell their software to customers directly. This section focuses, in particular, on the statutory and regulatory obligations that Canadian law places on businesses under privacy and data protection laws, which are heavily implicated by the commercial sale of stalkerware technology.

Part 4 (Third-Party Distribution and Intermediary Sales of Stalkerware) analyzes the legality of third-party distribution and facilitation of the sale of stalkerware, which raises the issue of intermediary liability. This section examines the potential liability of app stores (such as those provided by Google, Apple, Amazon, and Microsoft), where users are able to purchase stalkerware apps through those platforms.

Part 5 (Critical Discussion and Analysis) sets out a legal and policy analysis of stalkerware as a *dual-use* technology (technology that may be intended or used for legitimate or benevolent ends, but that is equally capable of or is repurposed for illegal, harmful, or unethical practices). This part also assesses the ability of Canadian law to respond to the harms that are associated with stalkerware apps. Additionally, Part 5 provides a brief legal analysis of spyware issues that are adjacent to stalkerware, such as cases where commercial spyware is used to monitor children or employees.

Part 6 (Recommendations) provides a set of proposed recommendations to establish and reinforce a web of meaningful restraints around stalkerware in Canada, which would help to prevent the harms and abuses that such technology engenders when it is used in the ways described in this report.

Appendix A, enclosed with this report, provides a compilation of digital security guides and resources for individuals who have been victimized by or fear they may be victimized by stalkerware-facilitated abuse, or who are otherwise concerned with the digital security of their devices and online accounts.

Appendix B, also enclosed, provides references to a number of academic, journalistic, and community resources encompassing policy, scholarly, advocacy, and research work that has been done in the area of stalkerware technology and gender-based violence, abuse, and harassment.

B. What Is Stalkerware?

The label ‘stalkerware’ describes how an app is used rather than how an app is necessarily designed and intended to function. Many of the features set out in the following bulleted list are seen in commercial spyware apps. These features showcase the purpose and prospective harms of stalkerware—namely that such software is intentionally designed to monitor and track a targeted individual by compromising their mobile device without their knowledge or consent. However, these clear cases form only one end of a spectrum of apps that may be used in

similarly abusive ways. At the other end of the spectrum, for example, are otherwise innocuous apps such as Find My iPhone, which are genuinely designed and intended to provide the functionality of helping users locate their lost phones. However, abusers can exploit such apps' functionalities to track a targeted individual, effectively making the apps stalkerware.

Depending on the specific company, stalkerware apps advertise a range of features. The Citizen Lab identified that, in aggregate, stalkerware apps claim to monitor and grant access to the following types of information:

- SMS text messages and iMessages (including message history and messages that were deleted from the device after the app was installed);
- Current and historical mobile location data, GPS records;
- Call logs, including call log history;
- Contact lists;
- Calendar and events;
- List of all installed applications on the device;
- A list of Wifi networks that the individual is logged into;
- Photos and videos;
- Email accounts;
- Web-browsing history (e.g., sites visited, number of visits, and bookmarks);
- Social media accounts and their private contents, including apps such as Twitter (including lists and direct messages), Tinder (including profiles, matches, liked/super-liked/skipped lists), and Instagram (including messages);
- Third-party messaging app data associated with WhatsApp (including deleted threads), Kik, Snapchat, Facebook Messenger, WeChat, LINE, Google Hangouts, and Telegram; and
- Device information, such as phone model, Android version, device ID (UDID number), and internal memory.[15]

Some applications include additional invasive features, such as the ability to log all keystrokes entered on a device or to restrict device capabilities (e.g., by remotely blocking incoming calls or access to certain websites). In some cases, the

15 For more details on the specific capabilities of the stalkerware apps that the Citizen Lab examined, see the table under "Stalkerware Capabilities" in Part 1 of the Citizen Lab's accompanying report, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry."

applications allow an operator to receive alerts based on the target's geographic location ("geofencing") or the input of specific keywords. Other invasive capabilities enabled by this software can include eavesdropping on phone calls through a "silent call" function and remotely activating the targeted device's microphone or camera to record or view the surroundings of the targeted person.

Still more features include an SMS spoof function, which lets the stalkerware operator send outgoing SMS text messages through the targeted device and under the device owner's identity. These messages do not appear in the device's message history, which conceals them from the targeted—and in this case, impersonated—individual.

Information Box 2: Classification of Stalkerware Technology specifies and describes the different categories of apps that operators may use in abusive manners to stalk, harass, or intimidate a targeted individual, whether or not the app was initially designed for that purpose. Throughout the rest of this report, we use the term "stalkerware" as an umbrella term to refer to apps across the entire spectrum, and distinguish between those categories where it is relevant to the legal or policy analysis.

Information Box 2: Classification of Stalkerware Technology

Generally speaking, there are three main classes of technologies that can be used as stalkerware:

1. **Intimate partner spyware** apps include apps that are intentionally designed to facilitate covert surveillance of an intimate partner's mobile device.
2. **Repurposed spyware apps** include apps that are intentionally and primarily designed for the purpose of covertly surveilling another individual's activities on their mobile device, but which are not explicitly marketed for intimate partner surveillance. These applications include those that are marketed as programs designed to monitor employees or children.
3. **Other repurposed technologies with stalkerware functionality (Class 3 Stalkerware)** include tracking and monitoring software that is not generally intended to operate in a surreptitious manner or for surveillance purposes. Instead, these applications are repurposed to be used for surveillance of an individual through their mobile device. Apps in this class include those designed with tracking functions, such as Find My Friends or Find My iPhone.

For the purposes of this report, we refer to the abusive exploitation of all three classes of technology for intimate partner surveillance or harassment as the use of **stalkerware**. Our analysis focuses throughout this report on the legality and ethics associated specifically with using such apps as stalkerware for intimate partner surveillance, in most cases to the exclusion of claimed legitimate uses. However, further discussion of

the "dual-use" nature of repurposed surveillance apps is also provided where relevant, including heightened scrutiny of uses such as monitoring children or employees (see, in particular, Part 5, Section A).

While hundreds of stalkerware apps or apps with stalkerware functionality are available online, the analysis in this report draws on desk research, and in some cases examinations, of several high-profile stalkerware and spyware apps and companies. Many of these applications and companies have been examined by academic researchers and the media. These applications include (in alphabetical order): Cerberus, FlexiSPY, Highster Mobile, Hoverwatch, Mobistealth, mSpy, PhoneSheriff and TeenShield (by Retina-X Studios), TrackView, and TheTruthSpy.

Many of these companies currently advertise or formerly advertised their products specifically for the purpose of covert and undetectable monitoring, including in the context of "catching your cheating spouse."[16] While many stalkerware apps marketed their capabilities to monitor current and former partners in the past, apps repurposed for stalkerware now tend to be marketed towards facilitating child or employee monitoring and tracking.

C. How Is Stalkerware Deployed?

The technical design of a stalkerware app dictates how and where the operator of the app accesses their target's device, private information, data, and call and messaging logs. Apps typically require the operator to have at least temporary physical access to the targeted person's device and/or knowledge of the device user's password if the device is locked. Such access and knowledge allow the operator to disable potential security notices and give all requested device permissions to the stalkerware app upon installation. After being installed, apps are typically designed so the operator can conceal their presence on the targeted individual's device: the stalkerware tends not to appear in the device's apps menu or on the home screen, and does not indicate when it is tracking the target individual's activities and exfiltrating their data. Such surreptitiousness can result in the victim's device being indefinitely infected and compromised without the targeted person realizing that the operator has turned the device into a surveillance platform against them.

In order to achieve maximum functionality, some Android applications require the stalkerware operator to have "root" access to the target's mobile device. Such access provides extensive control over the device's operating system beyond what the device allows in its default state. On an iPhone, a similar activity is known as "jailbreaking;" this bypasses Apple's restrictions on installing unauthorized

16 Danielle Keats Citron, "Spying Inc.," (2015) 72(3) *Washington and Lee L Rev* 1243 at 1246-47. See also this FlexiSPY blog post criticizing competitor mSpy for lacking "true" concealment: <https://blog.flexispy.com/flexispy-vs-mspy-one-isnt-invisible/>; TheTruthSpy, "All-in-One Catch Cheating Spouse by TheTruthSpy": <http://thetruthspy.com/catch-cheating-spouses-with-thetruthspy/>.

software. Both rooting and jailbreaking can make the user's device more susceptible to security vulnerabilities, viruses, and malware. This is more so the case if the device's primary user does not realize their phone has been compromised in such a way, and thus does not know that they need to respond to a heightened security risk, or if they do not know how to respond.

Other stalkerware applications that operate through the iCloud may require that the operator know only the targeted person's Apple ID and password to install the application. The operator may never need physical access to the targeted person's device. For example, companies such as mSpy advertise versions of their apps for iPhone that give the stalkerware operator access to the targeted individual's iCloud backups so long as the operator has the targeted individual's Apple ID and iCloud password.[17] However, if two-factor authentication is installed on the target's operating system, the operator would be required to have either physical (unlocked) access to the device, or another of the target's devices that would present the two-factor authentication prompt.

D. Methodology

This report analyzes the application of current Canadian law to the use, development, sale, and third-party distribution of consumer-level spyware for mobile devices (stalkerware apps). This includes apps advertised for intimate partner surveillance and spyware apps that are repurposed for intimate partner surveillance. Covert or overt stalking and abuse may occur through other forms of technologies, and on other types of personal electronic devices (such as laptops), but the focus of this report is the particular class of spyware technology that is designed to be installed on mobile devices.

The Citizen Lab research team focused on use with mobile devices because stalkerware apps are primarily designed for use in the mobile device environment, likely because most personal communications conducted through consumer-level Internet applications occur in this environment. Focusing on the spyware market for mobile devices also enabled more robust research outcomes by allowing for a comparative analysis of many of the numerous apps designed for mobile platforms without overextending the sample size to include other hardware or operating systems, which would dilute the available comparative inferences.

This report was completed by analyzing how existing Canadian laws would apply

17 mSpy, "Now you can monitor Non-Jailbroken iOS Devices!," <https://www.mspy.com/no-jail-break.html>.

to the types of stalkerware applications that are known to exist and focused on key functionalities as asserted by the stalkerware companies themselves. Since stalkerware technology has not yet been closely considered in the Canadian legal system, the analysis draws on analogous contexts involving the legal treatment of other forms of intimate partner harassment and abuse or alternative forms of malware. The analysis also analogizes from or extends relevant areas of technology law, such as digital privacy and intermediary liability. This analysis involved legal research methods, such as consulting legislation, case law (including judicial and regulatory decisions), legal scholarship, and policy documents. The analysis also builds on pre-existing literature and research associated with the study of intimate partner violence, abuse, and harassment and technology-facilitated gender-based violence, and pre-existing literature and research that is related to commercial spyware in other contexts, such as that of nation-state surveillance of civil society actors. Additionally, we conducted online searches to assess the current (at time of writing) availability of stalkerware apps on Google's and Apple's app stores.[18]

To a lesser extent, our report also incorporates other forms of research and analysis by the Citizen Lab, such as evaluating how spyware companies market and promote their products and services, and assessing such companies' public policy documents (such as privacy policies and Terms of Service).[19]

This report maps relevant Canadian laws onto the key actors and activities at each stage of stalkerware deployment. These stages encompass the following:

- Use of stalkerware by a private individual who has decided to target another by infecting the victim's device with this kind of malware;
- Initial creation and development by the app developer or stalkerware company;
- Sale of stalkerware by the developer itself; and
- Third-party distribution of stalkerware by intermediary platforms, such as online app stores.

18 The methodology that we used to search for stalkerware apps on the Google and Apple app stores was taken from Chatterjee et al, "The Spyware Used in Intimate Partner Violence," <https://www.ipvtechresearch.org/pubs/spyware.pdf>at 15. We discuss our findings from these searches in Part 4 of this report, "Legal Analysis of Third-Party Distribution of Stalkerware by Online Intermediaries."

19 For the full findings and analysis that resulted from the Citizen Lab's multidisciplinary research into stalkerware, including a technical analysis and evaluation of spyware companies' privacy policies, see the accompanying report published by the Citizen Lab, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry."

While situated in the Canadian legal context, the legal analysis in this report is both interdisciplinary and comparative. The report draws on adjacent fields such as science and technology studies (STS) and techno-sociology. It also references law and examples from foreign jurisdictions such as the United States of America and the European Union. While stalkerware and its harms have been an ongoing problem for many years, the legal system has yet to catch up and, in that sense, the report incorporates policy analysis and non-binding instruments that may inform the interpretation and application of existing laws to stalkerware.

Information Box 3: Report Terminology

- **Stalkerware:** Stalkerware is consumer-level technology that can be installed on a mobile device and that allows the operator of the app to remotely monitor the activities of the device's user or individuals routinely in the proximity of the user (such as parents and children). For the purpose of this report, stalkerware includes intimate partner spyware apps, repurposed spyware apps, and other repurposed technologies with stalkerware functionality, which are used for the purpose of intimate partner violence, abuse, and harassment, including intimate partner surveillance. We also use the terms **stalkerware app** and **stalkerware program**.
- **Spyware:** Spyware is software that enables a remote user to covertly obtain data about another individual's activities on an electronic device by surreptitiously transmitting data from the device to another computer system. Because this software is deployed in the context of targeting a specific individual or group for the purpose of surveillance, it does not include firmware updates, native operating system functions, or applications that collect large amounts of data from multiple users in the user-approved course of its normal functioning. We also use the terms **spyware app** and **spyware program**.
- **Intimate partner spyware apps:** Intimate partner spyware apps are apps that are intentionally designed and advertised for the purpose of facilitating surveillance of an intimate partner's mobile device.
- **Repurposed spyware apps:** Repurposed spyware apps are apps that are intentionally and primarily designed for the purpose of covertly surveilling another individual's activities on their mobile device, but which are not explicitly advertised for intimate partner surveillance. These applications could be marketed as programs advertised for covert monitoring of employees or children.
- **Other repurposed technologies with stalkerware functionality:** These are tracking and monitoring technologies available that are not generally intended to operate in a surreptitious manner or for surveillance purposes, but which can be repurposed to be used for surveillance of an individual through their mobile device. This category of software includes apps designed with tracking functions, such as Find My Friends or Find My iPhone.
- **Operator:** An operator is the person who installs or exploits stalkerware on another individual's mobile device and who uses that technology to remotely monitor and surveil the device user.

- **Target:** A target, **targeted person**, or **targeted individual** refers to the person who is subjected to surveillance through stalkerware technology that is installed on their mobile device.
- **Stalkerware developer:** A stalkerware developer is a company or person(s) that creates a spyware application by designing the program or creating the code required for a spyware app and its associated infrastructure (e.g., such as browser dashboards to view the collected data).
- **Stalkerware vendor:** A stalkerware vendor is an entity (1) that offers its own spyware application for sale directly to private individuals; (2) that owns the spyware software; or (3) whose business model primarily revolves around spyware. We also use the terms **stalkerware company** and **stalkerware business**.
- **Stalkerware intermediary:** A stalkerware intermediary is a third-party entity that did not develop or create the spyware and does not own the spyware, but distributes the spyware to users over its own infrastructure. Such distribution sometimes occurs in exchange for a fee or percentage of revenue (e.g., app stores).
- **Stalkerware distributor:** A stalkerware distributor is an entity that distributes stalkerware and that can be either a stalkerware business or an intermediary.
- **Dual-use technology:** Dual-use technology is technology that may be intended or used for legitimate or benevolent ends, but that is equally capable of or repurposed for illegal, harmful, or unethical practices. In contexts external to this report, the term can also mean technology that enjoys both military and civilian use, regardless of whether or not both uses were intended.

E. Stalkerware and Technology-Facilitated Gender-Based Abuse: Background and Literature Review

Numerous scholars, researchers, activists, journalists, and non-profit organizations working on issues relating to cybersecurity, human rights, online harassment, technology and gender equality, and intimate partner violence have recognized and examined technology-enabled forms of gender-based and intimate partner violence, abuse, and harassment. This work has resulted in a growing sphere of activity that includes civil society resources, non-profit training initiatives, and educational tools for victims and support workers. Academic research and scholarship across multiple intersecting disciplines has also contributed to this activity.[20]

20 **Appendix B** of this report includes a list of academic, policy, and investigative scholarship for those interested in exploring the scope of the work that has previously been done in this area. The appendix also provides a sample of key media coverage of stalkerware to demonstrate the nature of public discourse surrounding this issue, some of which is highlighted in this literature review.

With respect to civil society resources,[21] digital security training organizations, such as HACK*BLOSSOM and the Tactical Technology Collective ("Tactical Tech"), have created resources specifically to address technology-facilitated, gender-based abuse, including the former's DIY Cybersecurity for Domestic Violence and the latter's Gendersec Training Curricula. The National Network to End Domestic Violence (NNEDV) in the United States provides an online guide, "Technology-Facilitated Stalking: What You Need to Know." Take Back the Tech, which offers "feminist strategies against online gender-based violence," has done similarly with a Safety Toolkit and webpage on strategies against cyberstalking. In addition, individuals such as Eva Galperin, Director of Cybersecurity at the Electronic Frontier Foundation, have assisted targets of stalkerware and survivors and victims of domestic abuse in response to individual requests for help, by examining whether devices have been compromised by stalkerware and teaching targets how to regain control of their online accounts.[22]

The topic of stalkerware as a tool of intimate partner violence, abuse, and harassment has also garnered a high level of media attention in recent years. *Vice Motherboard* in particular has sustained in-depth coverage of the issue since February 2017 through their ongoing multi-part series, *When Spies Come Home*.[23] After law enforcement arrested infamous drug cartel leader Joaquin "El Chapo" Guzmán using, in part, evidence obtained from a stalkerware app, there was a flurry of public attention to this class of software.[24]

The remainder of this section provides a high-level review of the main findings of stalkerware-related scholarship, which have been integrated into the analysis provided in this report.

First, scholarship in this area has identified the vulnerability of data stored on personal electronic devices when devices (e.g., smartphones) are used in a trust-based environment like a home. For example, when regularly using devices in the close proximity of another individual (e.g., an intimate partner), many of the

21 **Appendix A** provides a list of links to the digital security and gender and technology guides and resources discussed in this section, in addition to other valuable contributions to this area of work.

22 Andy Greenberg, "Hacker Eva Galperin Has a Plan to Eradicate Stalkerware," *WIRED* (3 April 2019) <https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/>; Nicole Kobie, "Against a torrent of digital abuse, women are taking back control," *WIRED* (17 March 2018) <https://www.wired.co.uk/article/tech-abuse-digital-stalking-eva-galperin-prevent>.

23 "When Spies Come Home," *Vice Motherboard* <https://www.vice.com/en_us/topic/when-spies-come-home>.

24 Alan Feuer, "Drug Kingpin Used Spyware to Monitor His Wife and Mistress, Jurors Told," *The New York Times* (9 January 2019) <https://www.nytimes.com/2019/01/09/nyregion/el-chapo-trial.html>.

security measures native to the device are uniquely vulnerable to exploitation by intimate partners.[25] Specifically, many security options and much security software assumes an aggressor does not, and cannot, physically obtain access to a device or the passcode to unlock the device. These principles are significantly thwarted in cases of intimate partner violence, abuse, and harassment. As a result, cybersecurity measures on app platforms and electronic devices must be designed to combat both forms of threats.

Second, scholars have examined how digitally-enabled forms of control, stalking, and abuse manifest and replicate gender-based harm that occurs in non-technological environments.[26] Scholars also identified how technology-enabled abuse can amplify the scope and gravity of the harm itself.[27] As such, forms of abuse perpetrated through digital technology should be recognized as an inherently dangerous form of abuse that in its own right can cause emotional or psychological violence.[28] In one qualitative study in Australia, 83% of the participants identified technology-facilitated abuse as part of the pattern of domestic and family violence they experienced.[29] Survivors often go without legal protection and lack the resources to fully identify or cope with the abuse because of socio-technical gaps (e.g., where law enforcement, policy makers, legal services, and/or support services overlook or lack training about the role and implications of technology in intimate partner violence), and lacking technological proficiency among potential sources of protection, such as law enforcement and community support services.[30] Those gaps may exist to varying degrees among victims and survivors, law enforcement and other justice system participants, or community support workers.

25 See Diana Freed, et al, "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology," (2018) *CHI 18* 67; and Diogo Marques, et al, "Non-Stranger Danger: Examining the Effectiveness of Smartphone Locks in Preventing Intrusions by Socially-Close Adversaries," (2018) *USENIX Symposium on Usable Privacy and Security (SOUPS).*

26 Molly Dragiewicz, et al, "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms," (2018) 18(4) *Feminist Media Studies* 609.

27 *Ibid*.

28 Ioana Vasiu and Lucien Vasiu, "Light My Fire: A Roentgenogram of Cyberstalking Cases," (2016) 40 *American Journal of Trial Advocacy* 41.

29 The participants of the study were all women over 18 years old, who had experienced domestic family violence from their current or previous male intimate partner in the six months leading up to the first interview and engaged with the legal system in some way to respond to the violence: Heather Douglas, Bridget Harris and Molly Dragiewicz, "Technology-Facilitated Domestic and Family Violence: Women's Experiences," (2019) 59 *The British Journal of Criminology*.

30 See Diana Freed, et al, "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders," (2017) 1 *CSCW ACM on Human-Computer Interaction* 46 (where the authors present a qualitative study that analyzes the role of digital technologies in the intimate partner violence "ecosystem" in New York City).

Third, the academic literature in this area identifies a range of forms of technology-enabled abuse.[31] Such abusive behaviors include "harassment on social media, stalking using GPS data, clandestine and conspicuous audio and visual recording, threats via SMS, monitoring email, accessing accounts without permission, impersonating a partner, and publishing private information (doxxing) or sexualised content without consent."[32] In 2016, Vasiu and Vasiu examined the phenomenon of cyberstalking in the USA by studying approximately three hundred known court cases to examine the main perpetration and litigation aspects involved in cyberstalking.[33] The authors examine cyberstalking cases under the elements of US federal law and discuss the criminalization, research, and litigation implications of their study. The authors found that cyberstalkers' motivations "vary widely, from revenge and hate to erotic obsessions," and that a "significant number of cyberstalking cases involve former intimate partners."[34]

Regarding spyware in particular, in 2018, Chatterjee, et al, completed an in-depth study of the intimate partner, surveillance-spyware ecosystem. By designing a machine-learning tool that analyzed the Internet and app stores, they identified hundreds of apps that were relevant to intimate partner surveillance.[35] In 2019, Harkin, Molnar, and Vowles examined nine prominent spyware vendors to analyze how those companies attribute meaning to their products through marketing.[36] The authors identified a concerning trend in a growing consumer spyware market where companies tend to "valorize the desires of those seeking to engage in the use of spyware"[37] in terms of the *safety* or *care* of surveillance subjects. These attempts to align the companies' spyware products with benevolent ends stand in stark juxtaposition with the powerful capabilities of the spyware products sold and the documented association of spyware with gender-based abuse and illegal behaviour.[38]

---

31 See Delanie Woodlock, "The Abuse of Technology in Domestic Violence and Stalking," (2016) 23(5) Violence Against Women 584-602; Danielle Keats Citron & Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," (2019) forthcoming *California Law Review*.

32 Molly Dragiewicz, et al, "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms," (2018) 18(4) *Feminist Media Studies* 609 at 610.

33 Ioana Vasiu and Lucien Vasiu, "Light My Fire: A Roentgenogram of Cyberstalking Cases," (2016) 40 *American Journal of Trial Advocacy* 41.

34 Ioana Vasiu and Lucien Vasiu, "Light My Fire: A Roentgenogram of Cyberstalking Cases," (2016) 40 *American Journal of Trial Advocacy* 41 at 49.

35 Rahul Chatterjee, et al, "The Spyware Used in Intimate Partner Violence," (2018) *IEEE Symposium on Security and Privacy* 441.

36 Diarmaid Harkin, Adam Molnar and Erica Vowles, "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," (2019) *Crime Media Culture* 1-28.

37 *Ibid* at 21.

38 *Ibid*.

The fourth area of academic scholarship relating to stalkerware includes work that explores and critiques the normative and conceptual frameworks that are attached to existing or potential criminalization and/or regulation of technology-facilitated abuse. Scholars have identified areas where the normative underpinnings of the scope of current laws warrant reexamination. Citron, for example, has identified "sexual privacy" as a distinct privacy interest that requires recognition and protection.[39] Dragiewicz, et al, propose the term "technology facilitated coercive control" to encompass the technological and relational aspects of patterns of abuse against intimate partners.[40]

Finally, scholars have started to examine the need for law reform on the basis of responding to technological advancements that have created new or digitally-enabled forms of gender-based harm.[41] For example, both Citron and Clevenger have examined the legality of spyware under US law and the adequacy of existing laws in the USA to respond to the problem.[42]

Information Box 4: Accompanying Holistic Report: "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Applications Industry"

The Citizen Lab has published a holistic report examining stalkerware, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Applications Industry," which accompanies this report's legal analysis of stalkerware companies' practices, products, and services. "The Predator in Your Pocket" was collaboratively written by researchers from computer science, political science, criminology, law, and journalism studies. As befits their expertise, the report is divided into several parts, with each focusing on specific aspects of the consumer spyware ecosystem, which includes: technical elements associated with stalkerware applications, stalkerware companies' marketing activities and public policies, and these companies' compliance with Canadian federal consumer privacy legislation. The report provides a range of recommendations which, if adopted, may mitigate some of the most egregious practices engaged in or enabled by stalkerware apps and the companies which are involved in their production and sale. This report is available at https://citizenlab.ca/docs/stalkerware-holistic.pdf

39 Danielle Keats Citron, "Sexual Privacy," (2019) forthcoming in *Yale LJ*.

40 Molly Dragiewicz, et al, "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms," (2018) 18(4) *Feminist Media Studies* 609-625.

41 Heather Douglas and Mark Burdon, "Legal Responses to Non-Consensual Smartphone Recordings in the Context of Domestic and Family Violence," (2018) 41(1) *UNSW Law J* 157 (examining the legality of surreptitious audio recordings created in domestic and family violence cases in Australia).

42 Danielle Keats Citron, "Spying Inc.," (2015) 72 *Wash & Lee L Rev* 1243; Katherine Fisher Clevenger, "Spousal Abuse through Spyware: The Inadequacy of Legal Protection in the Modern Age," (2008) 21(1) *Journal of the American Academy of Matrimonial Lawyers* 653. See also Katherine Cooligan and Daniel Hohnstein, "'Intruding Upon the Seclusion of Personal Email' — What the Common Law Tort for the Invasion of Privacy Might Mean for Snooping Spouses and the Electronic Evidence that they Obtain," (2014) 34 *CFLQ* 135, examining the admissibility of evidence obtained through "snooping" in family law proceedings in Canada.

Part 1: Legal Analysis of Stalkerware Use

Part 1 considers the legality of using stalkerware under Canadian criminal and civil law. The criminal law analysis concludes that an operator's use of stalkerware technology could potentially violate numerous criminal laws; penalties for such offences could include significant jail time. Then, the civil law analysis of the use of stalkerware technology suggests that the operator of stalkerware technology may be liable to the victim under multiple potential torts for damages, including potential punitive and/or aggravated damages. It is entirely possible that an operator's activities might simultaneously open the operator to criminal and civil jeopardy.

A. Use of Stalkerware Technology and the Criminal Law

An operator's use of stalkerware applications against a targeted person may constitute one or more criminal offences under the *Criminal Code*. The use of stalkerware applications may be criminal per se, or the use of stalkerware technology may be one component of a series of acts or behaviour that cumulatively amounts to a criminal offence. Whether a particular offence is engaged will depend on the features and functionality of the particular technology. In some circumstances, monitoring or controlling an individual through technological means may be criminal, even when the target is aware that such behaviour is occurring.

Information Box 5: *Criminal Code* Offences Applicable to the Use of Stalkerware Technology

Invasions of digital privacy

- Interception of Private Communications, Section 184(1)
- Unauthorized Use of a Computer, Section 342.1
- Mischief in relation to Computer Data, Section 430(1.1)
- Possession of intercept devices and designated computer programs, Sections 191(1) and 342.2
- Identity Fraud, Section 403.1

Fear-based offences: Threatening behaviour that exploits access to the target's digital device

- Criminal Harassment, Section 264
- Extortion, Section 346
- Intimidation, Section 423

Breaches of sexual integrity and privacy

- Non-consensual Distribution of Intimate Images, Section 162.(1)
- Defamatory Libel, Section 300
- Voyeurism, Section 162(1)

As listed in **Information Box 5: Criminal Code Offences Applicable to the Use of Stalkerware Technology**, criminal laws that apply to stalkerware technology generally target three main forms of harm: serious invasions of privacy, the fear and psychological harm that is associated with harassment and threats, and serious breaches of an individual's sexual integrity. This section discusses each of these offences, and explains how they may apply in the context of stalkerware technology.

In considering the range of criminal offences under Canadian law, it is important to note that the context of the relationship between the operator and targeted person is an important factor for certain criminal offences that may be relevant to an operator's use of stalkerware technology. Where there are circumstances of trust in an intimate partner relationship and an ongoing pattern of threatening, controlling, or abusive conduct, the psychological consequences of being surveilled and controlled through technological means may be even more severe from the perspective of the targeted person. A breach of trust in an intimate relationship is also an aggravating factor in Canadian criminal sentencing law.

Information Box 6: What Happens After an Individual Makes a Complaint to the Police to Report a Crime?

Public legal education is one of the important ways to help complainants and victims of stalkerware abuse understand their legal rights and the legal options available to them. For many, the criminal justice system is an unfamiliar and intimidating place which can be a deterrent to seeking help. Many victims of criminal offences find it useful to understand what happens after an individual makes a complaint to the police and what they can expect to happen for the complainant and for the person who is the subject of the complaint. Some victims might fear that the police may not be able to adequately protect them if they seek help against a domestic abuser. Others might fear that if they make a complaint against somebody, the offender may get in more trouble than the complainant wants.

Complainants and victims often benefit from understanding that making a criminal complaint about the perpetrator of abuse does not automatically mean that the complainant will have to testify in an open court in a trial or that the perpetrator will automatically be jailed. In any case, one of the first priorities that the police will consider is the immediate, short-term safety of the complainant. There are a range of steps the police can and should take to protect an individual who is afraid for their safety.

After the short-term safety concerns are addressed, a complaint to the police might go down one of several paths. Criminal cases are often resolved in ways that do not require a trial or witness testimony in court. For instance, many cases are *diverted* when the offender has mental health issues and undergoes counselling to get help and treatment. While the police and the prosecution have the ultimate decision-making power over whether an individual is prosecuted, both the police and the

prosecution will seek input from a complainant in deciding how to proceed. The target of technology-facilitated abuse may choose to provide any input that they wish, such as a request that non-criminal preventative measures be considered, that the perpetrator of the abuse be cautioned or warned by police, that steps be taken to prevent offending behaviour, or that criminal charges be laid and a prosecution commenced if the officer has grounds to believe that an offence was committed. If the offender is found guilty, the victim also has an opportunity to provide input at the sentencing stage.

If a victim of stalkerware abuse or other forms of technology-facilitated abuse is fearful or concerned about making a complaint to the police, they may receive confidential help from a lawyer to help them understand and navigate the process or speak to a local community organization that provides support to persons experiencing intimate partner violence, abuse, and harassment.

For a range of potential reasons, the police may not always act upon and provide help if a criminal complaint or request for assistance is made. Community workers that work with victims and survivors of intimate partner violence, abuse, and harassment across Canada anecdotally report that complaints have not been acted upon by police in many cases involving technology-facilitated abuse. Complainants and victims of technology-facilitated harassment and stalking can contact legal counsel or a local community organization for shelter and help if a complaint is not investigated or acted upon by their local police service. Independent police oversight bodies such as, in Ontario, the Office of the Independent Police Review Director (OIPRD), may also receive complaints from the public with regard to the conduct of the police. Part 5 of this report provides a broader discussion regarding problems associated with a law enforcement gap.

i. Invasions of Privacy

This section analyzes criminal offences that fall under the category of invasions of privacy that are caused or facilitated by malware installed on a mobile device. Consider the following hypothetical case:

> Imani puts her cell phone down on her nightstand and leaves her room to have a shower and finish her nightly routine. Her partner, Misha, picks up the phone while she is gone. He has been upset and jealous of Imani's coworkers and thinks he needs answers about what's really going on in Imani's personal life. Misha punches in the password to unlock the screen. Imani didn't give him her phone password, but he learned it previously by peeking over her shoulder while she typed it in.
>
> In the moments he has alone with Imani's phone, Misha accesses the app store on Imani's phone and downloads and installs an application that he read about online. He gives himself administrative control over the app, so he can control it remotely from his own cell phone. Once installed, the app disappears from the main screens that Imani

is familiar with—it is turned on and working, but it hides in the background of the phone's operating system without any obvious visual clues that it has been installed.

Misha puts the phone back down on Imani's nightstand. In the weeks and months that follow, Imani and Misha continue to date and continue to text each other as usual. What Imani doesn't know is that Misha is now monitoring nearly every aspect of Imani's day-to-day life through her phone: reading all emails and text messages, looking at all the photos she takes on her phone, listening in on her phone calls as she makes them, and tracking her GPS location as she moves about the city.

The factual hypothetical case above engages several potential offences under the *Criminal Code*:

a) Technology that Intercepts Private Communications

Section 184(1) of the *Criminal Code* makes it a criminal offence for an individual (a "third-party operator") to wilfully intercept a private communication[43] without the consent of at least one of the direct participants ("first parties") to the communication.[44] An individual who commits this criminal offence may be liable to imprisonment for up to five years. The use of covert applications to listen in on a target's phone calls or read a target's private text-based messages in real-time as the communications occur would likely constitute a criminal offence.[45]

The offence of intercepting a private communication does not apply where one of the parties to the communication (the sender or recipient) consents to the interception.[46] Consent may be given expressly or implied.[47] Canadian courts have

43 Private communications may generally include telephone calls, text (SMS) messages, and other one-on-one electronic messages (e.g., Twitter direct messages, WhatsApp Messenger, Facebook Messenger). Under the *Criminal Code*, a "private communication" is one where either the originator or recipient of the message is located in Canada, and where the originator of the communication reasonably believes it will not be intercepted by anyone other than the intended recipient (s. 183 of the *Criminal Code*). In recent leading jurisprudence in this area, private communications include online text-based messages sent on a one-on-one basis (i.e., this would not generally include communications in a large, crowded chatroom): *R. v. Marakah*, 2017 SCC 59.

44 There are a number of exceptions carved out of this offence that apply to law enforcement authorities and telecommunications companies that would not be available to civilians who intercept private communications on a targeted person's electronic device.

45 To engage the offence, the "intercept" must have occurred through any "electromagnetic, acoustic, mechanical or other device," which is defined as "any device or apparatus that is used or is capable of being used to intercept a private communication" (*Criminal Code*, s.183).

46 It should be noted that this assumes non-state actors are parties to the communications. A separate set of rules apply where the consent comes from a state actor (a state agent, informant, or police officer, for example).

47 *Criminal Code*, s. 184(2)(a).

developed a meaningful and contextual interpretation of consent, which requires the following features for the consent to be valid:

1) Consent to intercept private communications must be voluntary (free from coercion).
2) Consent must be given knowingly (the consentor must be aware of what he or she is doing and aware of the significance of the act and the use that may be made of the consent).
3) To be valid and effective, the consent must be a conscious act of the consentor for reasons which the consentor considers sufficient.[48]

Certain types of stalkerware-facilitated and technology-facilitated abuse may engage the issue of consent in circumstances where intimate partners have shared access to a home network, computer, or a password to cloud-based storage. It cannot be assumed that sharing access to *some* electronic information is valid and effective consent to intercept any or all private communications that the operator can surreptitiously *gain* access to. The consequences of sharing access to a password or computer, for example, may be entirely unknown to an individual, who may not understand that their intimate partner could exploit that access to install malware on their electronic device or monitor their private communications from another computer. To be legally effective, consent must be made knowingly. In the context of an abusive, violent relationship, contextual circumstances should also be considered to determine whether coercion was used to secure the victim's 'consent'.

While the law is not entirely settled in this area, surreptitious access to another individual's stored, historic private communications may not fall within the definition of intercepting private communications. The leading interpretation of "intercept" currently requires that the intercepting party has technologically interfered with the transmission of the communication in real-time as the communication occurs.[49] Nevertheless, covertly or even overtly monitoring electronic information about an intimate partner (e.g., their location data, logs of telephone calls, or previously sent or received private communications) may fall within one or more of the additional criminal offences set out in this report.

48 *R. v. Goldman*, [1980] 1 S.C.R. 97 at p. 23-24; *R. v. J.P.G.*, [1996] O.J. No. 3550 (Ct. J.) at paras. 21-22.

49 *R. v. Jones*, [2017] 2 S.C.R. 696 at para. 72. The Supreme Court of Canada recently considered the definition of intercept in an appeal of *R. v. Mills,* 2017 NLCA 12 (hearing on May 25, 2018; judgment reserved).

b) Unauthorized Use of a Computer

Section 342.1 of the *Criminal Code* makes it a criminal offence to use a computer fraudulently (i.e. for purposes of a dishonest activity) and without colour of right (i.e. without an honest belief that the individual is legally authorized to do the act) for the purposes of engaging in the following actions:[50]

a) Obtaining, directly or indirectly, any computer service;

b) Intercepting or causing to be intercepted, directly or indirectly, any function of a computer system;[51]

c) Using or causing to be used, directly or indirectly, a computer system with intent to commit the offence of mischief to data; or

d) Using, possessing, trafficking in or permitting another person to have access to a computer password that would enable a person to commit any of the above three offences.

This offence has not previously been applied to stalkerware technology in any reported decision. However, the linkages between the offence of unauthorized use of a computer and stalkerware technology are obvious. By its very nature, stalkerware technology—which is designed to surreptitiously gain access to a target's device—is targeted by this law. Gaining surreptitious access to another individual's mobile device through stalkerware technology can run afoul of either s. 342.1(a) or (b). It should be noted that while the interpretation of subsections (a) and (b), listed above, have not yet been extensively considered in Canadian courts, it is significant that Parliament made it an offence to both *obtain* and *intercept* a computer service or function. These terms are not redundant and confirm that the scope of the offence is intended to be broad. It is likely, therefore, that gaining unauthorized access to another individual's smartphone through malware is itself criminalized under this offence.

Accessing a mobile device without authorization for the intended purpose of committing mischief to data (the next offence discussed in this section) would also run afoul of s. 342.1(c). Gaining unauthorized access to a device for the purpose of committing mischief to data could include the following examples:

50 *R. v. Livingston*, 2018 ONCJ 25 at para. 88.

51 This offence is satisfied if the interception occurs by means of "an electro-magnetic, acoustic, mechanical or other device," which means "any device or apparatus that is used or is capable of being used to intercept any function of a computer system": *Criminal Code*, s. 342.1(2).

- An operator who uses stalkerware technology that can restrict the mobile device's capabilities (e.g., block incoming calls from certain people or block access to certain websites) would be in violation of this offence because the technology is designed to interfere with the target's data and the functioning of the target's device.
- Similarly, stalkerware technology that has an SMS spoof function allows an operator to send outgoing SMS text messages through the targeted device and under its owners' identity. Such an activity constitutes an offence under this law because the use of that technology is intended to interfere with the target's communication data.

Surreptitious remote access to a coworker's email service led to a guilty verdict under this offence in *R. v. Charania* ([2012] O.J. No. 5113 (C.J.)). The offender was convicted for mischief in relation to computer data and unauthorized use of a computer for having remotely accessed (through his former employer's computer network) another employee's email account without authorization and forwarding e-mails to his own account.

c) Mischief in Relation to Computer Data

Under s. 430(1.1) of the *Criminal Code*, an individual commits the offence of mischief in relation to computer data if they do any of the following acts intentionally and without a colour of right (i.e., without an honest belief that the individual is legally authorized to do the act):[52]

a) Destroys or alters computer data;

b) Renders computer data meaningless, useless, or ineffective;

c) Obstructs, interrupts, or interferes with the lawful use of computer data; or

d) Obstructs, interrupts, or interferes with a person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it.

Computer data is defined very broadly under the *Criminal Code* and would undoubtedly include e-mails, text messages, and photographs or videos taken on a cell phone.

52 *R. v. Livingston*, 2018 ONCJ 25 at paras. 77-86.

Two situations arise where this offence will likely be committed through the use of stalkerware. First, an operator commits mischief in relation to computer data if the operator deprives the target of access to his or her own data (such as by blocking certain incoming communications). Second, an operator commits mischief in relation to computer data if the operator deletes or manipulates the target's data when using stalkerware technology.

d) Possession Offences: Possession of an Intercept Device or Device Designed to Commit an Offence under S. 430 or 342.1 of the *Criminal Code*

Each of the three aforementioned offences (intercepting private communications, unauthorized use of a computer system, or mischief in relation to computer data) are relevant to additional offences that pertain to the possession, making, or sale of certain electronic devices:

1) **Possession of an intercept device:** Section 191(1) makes it an offence to possess, sell, or purchase a device (or a component of a device) that is primarily useful for surreptitious interception of private communications (such as phone calls, text messages, or e-mails). This offence is discussed in further detail in Part 3, Section A, because it also applies to *selling* intercept devices. This offence would likely apply to a spyware program that is primarily useful for surreptitiously intercepting private communications, as many of the major consumer-level spyware apps do.
2) **Possession of a device for mischief in relation to computer data:** Section 342.2 makes it an offence to possess a device (which is expressly defined to include a computer program) that is "designed or adapted to primarily commit" the offence of mischief in relation to computer data, if the individual knows "that the device has been used or is intended to be used to commit such an offence."
3) **Possession of a device for unauthorized access to a computer:** Section 342.2 makes it an offence to possess a device (which is expressly defined to include a computer program) that is "designed or adapted to primarily commit" the offence of unauthorized use of a computer, if the individual knows "that the device has been used or is intended to be used to commit such an offence."

Covert spyware apps are inherently designed to enable the operator to gain unauthorized access to a third-party target's mobile device and, in some circumstances, to interfere with the integrity of the data on that device. As such,

even being in knowing possession of the program may constitute an offence under Canadian law, to the extent that the operator does not have a lawful excuse for possessing the program in question.

The significant impact of these offences in relation to the consumer-level spyware marketplace in Canada will be discussed in Part 3, Section A, as the offence under section 342.2 also applies to any individual or company that "makes, possesses, sells, offers for sale, imports, obtains for use, distributes or makes available" a computer program that is captured by the offence.

Information Box 7: Criminal Offences that Apply to Purchasing and Possessing Repurposed (Dual-Use) Spyware Apps

In this report, we discuss two types of spyware apps that may be installed on a mobile device: Intimate partner spyware apps (apps that are intentionally designed and/or advertised to facilitate surveillance of an intimate partner's mobile device); and Repurposed spyware apps (apps that are intentionally and primarily designed for the purpose of covertly surveilling another individual's activities on their mobile device, but which are not explicitly advertised for intimate partner surveillance).

Repurposed spyware apps include those that are marketed as programs designed to monitor employees or children. Repurposed spyware apps are forms of dual-use technology, meaning technology that may be intended or used for legitimate or benevolent ends, but that is equally capable of or repurposed for illegal, harmful, or unethical practices.

It should *not* be assumed that purchasing or possessing either intimate partner *or* repurposed spyware apps is legal in Canada. Of particular importance, the offence of possessing and purchasing an intercept device appears to prohibit the purchase and/or possession of *both* intimate partner spyware apps and repurposed spyware apps, so long as the individual knows that the app is "primarily useful" for surreptitiously intercepting private communications. In other words, the fact that the app is primarily useful to function in that manner is what makes purchasing and possessing the app illegal.

The application of criminal law to the sale of spyware apps in Canada (including dual-use spyware apps) is discussed in further detail in Part 3, Section A, "Criminal Liability of Vendors under the *Criminal Code*."

e) Identity Fraud

The offence of identity fraud under section 403(1) of the *Criminal Code* involves the illegal use of a targeted person's "identifying information." Identifying information

is broadly defined as referring to any information "commonly used alone or in combination with other information to identify or purport to identify an individual."[53] Of relevance in the context of stalkerware, "identifying information" includes user names, passwords, electronic signatures, digital signatures, name, address, and date of birth.

Although the term "identity fraud" is commonly associated with financial crimes, this offence is defined more broadly. Of relevance in the context of stalkerware, the offence of identity fraud reads:

> Everyone commits an offence who fraudulently personates another person, living or dead,
> (a) with intent to gain advantage for themselves or another person;
> …
> (c) with intent to cause disadvantage to the person being personated or another person. . .

The fraudulent personation of a target's identity for personal *advantage* or to *cause disadvantage* to another individual is captured by this offence. "Fraudulently" has been interpreted to mean an act of "bad faith."[54] "Advantage" is not restricted to a pecuniary or economic advantage.[55]

As a result, this offence is potentially engaged in the context of an intimate relationship where an operator uses technology to dishonestly or fraudulently use the target's identity information for an abusive purpose. For example:

- A stalkerware operator may use a keystroke logger to obtain account information of the target and uses those account usernames and passwords to gain access to additional personal information in furtherance of the operator's surveillance activities. To the extent that this malicious infiltration is intended to benefit the operator in some form or to cause a disadvantage to the target, the offence of identity fraud would be committed.

53 Section 402.1 of the *Criminal Code* states that identifying information is "any information — including biological or physiological information — of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver's licence number or password."

54 *R. v. Rozon* (1974), 28 C.R.N.S. 232 (Que. C.A.).

55 *R. v. Rozon* (1974), 28 C.R.N.S. 232 (Que. C.A.); *R. v. Marsh*, [1975] O.J. No. 1668 (Co. Ct.); *R. v. Boyle*, [2005] B.C.J. No. 2501 (C.A.).

- This offence would also be engaged when a stalkerware operator uses identifying information fraudulently obtained about a targeted individual to engage in doxxing: in this case, publishing the targeted person's account information online to intentionally leave the person vulnerable to other forms of identity fraud or theft.[56]
- A stalkerware operator may use technology that enables the operator to falsify text messages that appear to be written by the target (spoof SMS functions). To the extent that the operator engages in such conduct with the intent of either causing a disadvantage to the target or gaining some advance, the operator's conduct would likely fall within the offence of identity fraud.

ii. Fear-Based Offences

The criminal offences discussed in this subsection are perpetrated when individuals use stalkerware to harass, intimidate, threaten, or extort another person. The common thread across the offences is that the person targeted by the stalkerware app knows that they are being surveilled through their phone. It is the overt and brazen use of the stalkerware app that causes fear and interferes with the individual's dignity by depriving them of autonomy and control over their own life.

The following hypothetical case highlights some of the issues in fear-based situations:

> **Lane and Kendall have been in a romantic relationship for over three years. While they love one another, the relationship is fraught and conflict-prone. Over time, Lane began to realize that Kendall had difficulties with anger and jealousy, but she thought that as the relationship progressed, they would be able to work through Kendall's issues. That has not been the case. During verbal arguments, Kendall becomes out of control with rage, and Lane can see in Kendall's eyes that the situation could become physically aggressive if Lane doesn't diffuse it.**
>
> **Lane now walks on eggshells on a day-to-day basis to prevent explosive episodes. Over time, however, Lane has become more concerned. No matter what Lane does to prevent conflicts from arising, Kendall flies off the handle in unpredictable ways. Jealousy is a major problem for Kendall. Lane has stopped speaking to many friends and even some family members because it just causes too many problems with Kendall.**

56 For example, in *R. v. BLA*, 2015 BCPC 203, the offender was found guilty of numerous counts of harassment, extortion, public mischief, uttering threats, and breaching his recognizance. Included in a range of malicious behaviours involving online harassment, the offender threatened and disclosed the target's credit card information online.

Lane has also become increasingly concerned because Kendall seems to know a lot of information about what Lane does during the day, even when Kendall is at work. Lane thinks that Kendall somehow has access to Lane's text messages and locations. Lane knows that Kendall had access to Lane's phone once because Lane needed help with a work project. At that time, Lane allowed Kendall to use Lane's cell phone to help. Lane is afraid that Kendall did something with the phone during that time and that Kendall is now spying on Lane. Lane confronts Kendall, but Kendall responds angrily, accusing Lane of hiding things from Kendall. It causes one of their biggest fights yet and causes Lane to see that Kendall has gotten to the place where he appears to be completely out of control. Kendall eventually calms down but tells Lane that the only way Kendall can handle his fear that Lane is leaving their relationship is if Kendall can keep accessing Lane's location and text messages. Kendall tells Lane that this shouldn't be a big deal because Lane wouldn't have a problem with it if Lane has nothing to hide. Kendall has set up a 'geofence' that sends Kendall an alert if Lane leaves their apartment or Lane's office during the day.

Lane is afraid to the point of not knowing what to do. Lane realizes that Kendall is unstable and seems to be capable of anything when angry. Lane is too afraid to do anything about it because if Lane calls 911 or goes to the police station for help, Kendall will find out about it right away. Lane also doesn't know if the police will be able to do anything to help. Lane is afraid of how bad it could get with Kendall. Kendall has never assaulted Lane, but Lane has seen Kendall smash things in their apartment when angry. She also knows that Kendall had an issue with police involvement in a previous relationship, but Kendall didn't tell Lane all of the details.

a) Criminal Harassment

Criminal harassment is an offence under section 264 of the *Criminal Code*. The offence of criminal harassment would include the use of technology to stalk, control, and/or threaten a target, where the operator's behaviour causes the targeted person to be fearful for their safety or the safety of another person.

An act of criminal harassment is committed whenever the individual engaged in harassing conduct knows that the targeted person feels harassed (or was reckless or wilfully blind to the target's feeling of harassment) and where the person feels harassed and fearful for their safety or the safety of anyone known to them as a consequence of the actions of the offender.[57]

57 The Ontario Court of Appeal defines harassment broadly, as feeling harassed "in the sense of feeling tormented, troubled, worried continually or chronically plagued, bedeviled and badgered" (*R v. Kosikar* (1999), 138 C.C.C. (3d) 217 (Ont. C.A.)).

In determining whether the perpetrator's conduct caused the victim to "fear for their safety," safety is *not* limited to physical safety but may include substantial psychological harm or emotional distress.[58] Even a single event can constitute harassment.[59]

This offence could arise in circumstances where the target knows about, or later learns about, the technology-facilitated abuse and intrusions on privacy. The targeted person's awareness that their electronic device or information is being controlled or monitored does not render the offender's conduct lawful. Awareness, itself, is what may *cause* the harassment. Harassment may be caused by awareness of the operator's assertion of technological monitoring and control, which may be one part of an array of abusive conduct used by the offender to harass the targeted person.

In conducting an investigation into a case involving harassment, law enforcement authorities must assess all of the circumstances and the total effect of all related conduct over time. Conduct such as emotional abuse, physical abuse, financial control, and technological-control are all part of a matrix of abusive conduct that is designed to degrade and disempower the targeted person and to undermine and violate the victim's autonomy, dignity, and security of the person.[60] Perpetrators of such conduct often engage in a range of threatening and controlling behaviours that either quickly or over time cause a victim to be fearful. Fearfulness displaces any meaningful concept of consent to being watched or controlled electronically. Valid consent cannot be obtained by intimidation, threats, violence, or coercion.

Courts have recognized the uniquely disturbing effects of harassment in technologically-enabled environments, as the ubiquitous nature of electronic life means the operator's conduct can be that much harder to escape. In Alberta's Provincial Court, Justice Cioni sentenced a man who installed keylogging software on his ex-partner's computer, recorded her passwords, and illicitly obtained her phone records, e-mails, bank account access, and intimate images, which he used to criminally harass, cyberstalk, and impersonate her online. Justice Cioni described the resulting harm in the following manner:

58 *R. v. Szostak*, 2012 ONCA 503 at paras. 31, 45; *Coburn (Re)*, 2016 ONCA 536 at para. 17.

59 *R. v. Kosikar* (1999), 138 C.C.C. (3d) 217 (Ont. C.A.).

60 Police investigations into harassment cannot focus on specific events in isolation. The intimidating effects of an individual's conduct are compounded (or 'compound') over time. Where a particular type of harassing behaviour occurs in the context of other prior incidents or discreditable conduct, those other incidents serve as evidence and must be considered to assess the effect of a further incident on the complainant, and whether the perpetrator of the harassment knew that the conduct would cause the complainant to be fearful or that the accused was reckless as to whether the complainant would be fearful: *R. v. D (D.)* (2005), 203 C.C.C. (3d) 6 (C.A.).

> [This case] involves the use of electronics and with the capacity to strike to the heart of a person's well-being in our community. . . . [T]he trauma, the fear, the intimidation that goes with the course of harassment is harm itself.
>
> … it seems to me that where there is a more traditional form of harassment by phone calls, stalking, leaving things with full malice of forethought, that a person protects themselves by achieving safety, whether that is by changing address, phone number, even hiring security people, and while there is fear, a measure of some relief of the fear can be possible, although not much. But in a case like this where electronic means are used to attack a person, one wonders where the end of the road is in our society today. The accused's act of putting the [key]logger, as it is called, on the computer gave him complete access to codes and pass words [sic] and thereby the entire contents of the victim's computer and all of the plans that she had within that realm. He used it aggressively and badly. He disrupted her life with a specific plan of making her pay.[61]

b) Extortion

Personal information acquired vis-à-vis commercial spyware can be used to facilitate a range of criminal acts. In particular, efforts to control an individual by threatening to release private information about them may amount to extortion under section 346 of the *Criminal Code*. This section reads:

> Every one commits extortion who, without reasonable justification or excuse and with intent to obtain anything, by threats, accusations, menaces or violence induces or attempts to induce any person, whether or not he is the person threatened, accused or menaced or to whom violence is shown, to do anything or cause anything to be done.

Efforts to control an individual in an intimate partnership may be directed at causing the individual to do something specific or general. The essence of this offence is interference with an individual's freedom of choice, such as the freedom to continue in an intimate relationship or to choose to end that relationship, or the freedom to conduct one's personal affairs and life as one sees fit. Threats may be explicit or veiled. The offence transpires when the offender interferes with the targeted person's autonomy by causing the target person to avoid the threatened consequence which the target person fears or prefers to avoid.[62]

Threats coupled with demands interfere with the individual's *freedom of choice* because the individual may be coerced into doing something he or she would otherwise have chosen not to do.[63] The offence is not limited to economic or pecuniary demands and has been interpreted to apply to, for example, sexual demands.[64]

---

61 *R. v. Barnes*, [2006] A.J. No. 965 at para. 18; "Cyberstalker sentenced to one year," *CBC News* (16 March 2006) <https://www.cbc.ca/news/canada/cyberstalker-sentenced-to-one-year-1.583770>.

62 *R. v. Barros*, [2011] 3 S.C.R. 368.

63 *R. v. Davis*, [1999] 3 S.C.R. 759.

64 *R. v. Davis*, [1999] 3 S.C.R. 759.

Applied in the context of stalkerware, this offence is likely engaged when the offender threatens the targeted person with the release of private data, such as intimate images or private information, that was obtained through stalkerware in order to coerce the targeted person to comply with the offender's demand. Demands could include, for example, continuing in a relationship or abstaining from calling the police in relation to harassment or abuse.

c) Intimidation

Section 423 of the *Criminal Code* makes it an offence to engage in acts of intimidation. Such acts try to compel "another person to abstain from doing anything that he or she has a lawful right to do, or to do anything that he or she has a lawful right to abstain from doing." Acts of intimidation include "persistently following the person"[65] or "beset[ting] or watch[ing] the place where that person resides, works, carries on business or happens to be."[66] This offence is highly relevant in the context of stalkerware because these activities are purposefully enabled by the design and function of stalkerware apps.

In the context of stalkerware technology, an operator's use of the technology and knowledge of the surveillance by the targeted person engages the offence of intimidation. It is the awareness of the stalking and watching behaviour that gives rise to the harm. In the context of intimate-partner abuse, using stalkerware is intimidating and fear-inducing *because* the target knows they are being constantly watched and that the operator knows everything that the target does. If the targeted person knows that she is being watched by the operator through GPS location tracking she may be fearful, for example, to go to a lawyer's office, a police station, or a courthouse to seek help.

iii. Intimate Images: Invasions of Sexual Dignity and "Sexual Privacy"

A number of criminal offences pertain to the conduct of an intimate partner who exploits access to intimate photos and video recordings about their romantic partner (e.g., by either covertly recording them undressed or engaged in sexual activity, or through the non-consensual use or distribution of intimate photographs or videos that were consensually taken). These offences may include **Non-Consensual**

65 *Criminal Code*, s. 423(1)(c).

66 *Criminal Code*, s. 423(1)(f).

Distribution of Intimate Images,[67] **Voyeurism**,[68] and **Defamatory Libel**.[69] The offence of **Extortion** (discussed in Section A(ii)(b) of Part 1) is also relevant in the context of intimate images and sexual privacy because threatening behavior may be acutely harmful when an abusive partner threatens to disclose sexual recordings or images to intimidate or extort the victim.

Canadian criminal law is still developing ways to recognize the harm caused by invasions of sexual privacy or threats that interfere with an individual's sexual dignity. In *R. v. Jarvis*, the Supreme Court of Canada recently gave a privacy-enhancing interpretation to the scope of an individual's "reasonable expectation of privacy" from surreptitious visual recording for the sexual gratification of another person. Specifically, the Supreme Court considered the scope of the offence of **Voyeurism** (colloquially referred to as the "peeping tom" offence) in a case that involved a teacher who used a pen camera to surreptitiously film the cleavage area of one of his students while in a classroom. The Court held that privacy is not an all-or-nothing concept. Being in a public or semi-public space does not automatically negate all expectations of privacy with respect to observation or recording:

> One can think of other examples where a person would continue to expect some degree of privacy, as that concept is ordinarily understood, while knowing that she could be viewed or even recorded by others in a public place. For example, a person lying on a blanket in a public park would expect to be observed by other users of the park or to be captured incidentally in the background of other park-goers' photographs, but would retain an expectation that no one would use a telephoto lens to take photos up her skirt … The use of a cell phone to capture upskirt images of women on public transit, the use of a drone to take high-resolution photographs of unsuspecting sunbathers at a public swimming pool, and the surreptitious video recording of a woman breastfeeding in a quiet corner of a coffee shop would all raise similar privacy concerns.[70]

67 The offence of distributing intimate images (including images of an individual nude or engaged in explicit sexual activity) occurs when the offender knowingly distributes (or publishes, transmits, sells, makes available, or advertises) while knowing that the person depicted in the image has not consented to the distribution of the image. The visual recording must have been made in circumstances where the person depicted had a reasonable expectation of privacy both at the time the image was made and at the time the offence was committed: *Criminal Code*, Section 162.1(1).

68 Voyeurism is a criminal offence that may arise in the context of intimate partner violence when an individual abuses their access to intimate visual images of their romantic partner. Voyeurism refers to the surreptitious observation or visual recording of a person when they have a reasonable expectation of privacy. Such surreptitious conduct becomes criminal when it is done for a sexual purpose, or where the person being watched or visually recorded is nude or engaged in sexual activity (or is in a place where they are reasonably expected to be nude or engaged in sexual activity, such as a bedroom): See *Criminal Code*, Section 162(1)(a)(b) and (c).

69 Section 300 of the *Criminal Code* makes it an offence to knowingly publish defamatory libel. Defamatory libel is defined as "matter published, without lawful justification or excuse, that is likely to injure the reputation of any person by exposing him to hatred, contempt or ridicule, or that is designed to insult the person of or concerning whom it is published."

70 *R. v. Jarvis*, 2019 SCC 10 at para. 40.

The court's interpretation of the offence of voyeurism in *Jarvis* is a significant development in Canadian privacy jurisprudence and criminal law, insofar as it recognized a nuanced, autonomy-enhancing form of privacy. The Court's analysis steered away from imputing consent and acceptance of sexual surveillance simply because an individual is in circumstances that they cannot control (e.g, being in a public place). The decision in *Jarvis* will likely influence how many of the offences and laws considered in this report are interpreted and applied when applied to technology-enabled environments or to stalkerware. The offence of voyeurism is also directly applicable to stalkerware that enables the operator to remotely activate a camera on the target's device.

The offence of **Defamatory Libel** applies where an individual intentionally creates and publishes fake information about another individual. This offence is relevant to stalkerware because access to a target's private communications platforms, photos, and location can be egregiously abused by the operator in circumstances that give rise to Defamatory Libel. This offence may become increasingly relevant to ways that stalkerware technology can facilitate abuse. The technology can enable perpetrators to interfere with the victim's sexual autonomy and dignity by exploiting access to personal information about the victim. The following cases demonstrate the associated risks with that access:

- In *R. v. Simoes*,[71] the Court of Appeal for Ontario upheld a criminal conviction for Defamatory Libel where the offender sent e-mails to the victim's employer that invited the employer to engage in sexual activity with the employee. The e-mails were sent from fake e-mail accounts that were set up in the victim's name. The same sexually explicit message was posted on an adult online dating website. That posting also included the victim's photo. The communications were traced back to the offender's IP address.
- In *R. v. J.T.B.*,[72] an offender pled guilty to offences of publishing intimate images without consent (s. 162.1), assault (s. 266), sexual assault (s. 271), and obstruction of justice (s. 139(2)). The victim and offender ended a "troubled" romantic relationship due to the offender's previous violence and abuse. The following events, which occurred after their breakup, are only part of the subject matter of the offender's guilty pleas:

71 [2014] O.J. No. 856 (C.A.).

72 2018 ONSC 2422.

> [M]atters nevertheless took a very dark turn when Mr B. embarked on covert and sustained measures, (of which Ms B. was completely ignorant), to orchestrate a violent sexual attack on Ms B. by a stranger or strangers. Mr B. alone knows the true and complete motives underlying that perverse and horrid scheme. According to him, however, his motives included some form of twisted notion that, after the violent sexual attack was underway, Mr B. would intervene at some point to play the role of "rescuer" and end Ms B.'s torment, with the expectation that Ms B. then would show him more affection, in turn leading to a renewed romantic relationship.
>
> Execution of that horrid scheme by Mr B. repeatedly would employ images and knowledge of Ms B. and her [specified] residence, as well as ongoing familiarity with her employment, habits and movements which Mr B. had acquired through his intimate and spousal relationship with Ms B., and/or which Mr B. still was able to access and acquire through his ongoing trusted interactions with Ms B., who had no idea of Mr B.'s sinister plans for her.
>
> In late December of 2016, Mr B. took the first steps to implement those plans by creating an artificial profile on a social-media website which facilitates the meeting of consenting adults for sexual activity.
>
> . . .In an effort to confirm and emphasize the nature of what Ms B. supposedly wanted done to her during the course of the contemplated attack and sexual assault, Mr B. . . .sent Mr Y. numerous photos of unknown women being physically restrained and sexually assaulted in various ways…. To facilitate execution of his plans from a logistical perspective, Mr B., posing as Ms B., also provided Mr Y. with detailed instructions as to where, when and how the contemplated attack and prolonged sexual assault would take place….Mr B. went to considerable lengths to convince Mr Y. that the text messages really were coming from Ms B., and to address Mr Y.'s repeatedly indicated desire for confirmation that the contemplated attack and ensuing sexual assault would be mutually agreed and consensual.[73]

While the latter case of *R. v. J.T.B*. did not include a charge of Defamatory Libel, the factual circumstances of the case suggest that the investigating officers may have had grounds to lay that additional charge against the offender. Regardless, what the circumstances of these offences demonstrate is the extent to which access to a target's private communications platforms, photos, and location can be egregiously abused by the operator. As the Court described in *R. v. J.T.D.*:

> . . .Mr B.'s criminal scheme made elaborate use of the anonymity and lack of identity confirmation the internet facilitates, coupled with his ability to circulate and share information and images obtained through his past interaction with Ms B., who was his primary focus and obsession.[74]

73 *Ibid*.

74 *Ibid*.

B. Preventative Orders and Additional Remedies under Criminal and Family Law

i. Preventative Orders: Peace Bonds and Restraining Orders

Where an individual is afraid that they are being watched through a stalkerware app or stalkerware technology is being used as a means of intimidating and harassing behaviour that is done with the intention of causing the targeted person to fear for their safety, the target of such behaviour has multiple legal options available to obtain help and to prevent that behaviour from continuing. In addition to or as an alternative to making a criminal complaint to the police, an individual ("complainant") who is fearful of another individual ("defendant") may seek a court restraining order under s. 810 of the *Criminal Code*. This section of the *Criminal Code* lets the court impose an order with conditions that restrain the defendant from having contact or communication with the complainant or other conditions deemed appropriate in the circumstances. The court may impose such an order if there are reasonable grounds to believe the complainant is fearful that the defendant "will cause personal injury to him or her or to his or her spouse or common-law partner or child or will damage his or her property."

A 2015 amendment to the *Criminal Code* allows the issuance of a preventative order when a complainant fears that they will become the victim of a potential offence of non-consensual distribution of images, under section 810(1)(b).

If an individual wants to apply for such a preventive order, he or she may take any of the following steps:

1) Contact the police.
2) Go to the Justice of the Peace office at a criminal courthouse.
3) Contact a lawyer who practices criminal law for help with obtaining access to those orders.

Restraining orders are also available through provincial family court processes across Canada. Family law litigation in Canada has revealed multiple known cases involving technology-facilitated abuse and surveillance through spyware. Accusations of "covert surveillance, including physical surveillance through investigators and electronic surveillance, are … frequent."[75] In one reported case,

75 Ron Foster and Lianne Cihlar, "Technology and Family Law Hearings," (2014) 5 *Western Journal of Legal Studies* 1 at 3.

a family law court in Ontario granted a restraining order to a mother who was afraid of her daughter's father. In addition to other sources of concern, the mother discovered that her former spouse had installed spyware on their daughter's computer and was obtaining personal information about the mother through that computer. The spyware enabled him to access information such as her privileged e-mail communications with her own lawyer, the mother's contact information (as she had been hiding from him at the time for safety concerns), and other social information.[76]

ii. Admissibility of Illegally Obtained Evidence in Family Law Proceedings

The focus of this report is stalkerware in the context of gender-based abuse and violence against women. However, such technology may also be used in the context of family disputes, where the operator may not necessarily intend to harass or abuse their former partner, *per se*, but has installed spyware on their former partner's device near or after the point of conjugal breakdown, in hopes of obtaining evidence to their advantage in litigation. Recent precedents from family law proceedings in Alberta suggest that illegally-obtained evidence should be presumptively inadmissible in family law proceedings, so as not to encourage litigants to engage in such illegal or unethical conduct.[77]

C. Civil Law Claims

An individual who is targeted by an operator of stalkerware technology may seek relief in the civil justice system. However, it is important to note that a single wrongful act can be both a criminal offence and a wrongful act under civil law, which is known as a tort. For this reason, an individual who is targeted through stalkerware technology may choose whether to make a complaint to the police about the matter, to sue the operator in civil law, or to pursue a combination of the two courses of redress.

76 *Shoshi v. Vuksani*, 2013 ONCJ 459.

77 *AJU v. GSU*, 2015 ABQB 6 (concerning materials that "Mr. U" obtained as a result of installing spyware on "Ms. U's" personal computer without her knowledge; Mr. U obtained information regarding Ms. U's online activities and dropped off a package of information at her parent's home, before later trying to use the same information in family court proceedings); *St. Croix v. St. Croix*, 2017 ABQB 490 (concerning surreptitiously recorded voice communications); *TT v. JT*, 2012 ABQB 668 (concerning a case where one of the parties had hacked into the e-mail account of the other and tried to adduce evidence obtained; the court found it to be irrelevant, but would have excluded the evidence in any event).

Information Box 8: The Difference between Criminal Law and Civil Law

Violations of criminal law are prosecuted by the government. The legal process is started by a police officer who collects evidence that is then used by the prosecutor. The victim of a crime has a right to provide input to the process, but the victim doesn't have a right to make decisions about what happens with the case.

Civil law concerns legal disputes between private parties. A case under civil law is started by an individual (plaintiff or claimant) who brings a lawsuit to sue another individual for financial compensation for an injury. A claimant must show the court evidence that the defendant is responsible for causing a legal injury to the claimant (this doesn't mean a physical injury, but rather a violation of the claimant's legal right). The plaintiff (often with the assistance of a lawyer) decides what claim to make and is responsible for gathering evidence and bringing it to court.

The key question that determines whether a claimant can sue someone for financial compensation is whether the claimant has a cause of action. This means they have a basis in law and fact to launch a case and bring the matter before a court. The analysis in the present section (Part 1, Section C) describes causes of action that are relevant in the context of stalkerware.

The following section provides information about tort claims under civil law that are relevant to stalkerware. While the analysis in the criminal law section, in Section A of Part 1, applies throughout Canada,[78] the analysis of the civil law draws distinctions between the provinces because civil laws vary between provinces. Four main categories of torts are considered: invasions of privacy, public disclosure of private facts, breach of confidence, and intentional infliction of mental suffering. The final section will discuss recent litigation about novel claims under the 'tort of harassment'.

i. Invasion of Privacy

No consistent approach to invasions of privacy exists under civil law in Canada. Four provinces—British Columbia, Manitoba, Newfoundland, and Saskatchewan—have privacy legislation that has created a statutory tort that is actionable in court.[79] In Quebec, the right to privacy is protected by articles 3 and 35-37 of the *Civil Code of Quebec* and by section 5 of the *Quebec Charter of Human Rights and Freedoms*. In 2012, the top court in Ontario created a common law

78 For clarity, as a federal regime, there is only one criminal law system across Canada.

79 *Privacy Act*, R.S.B.C. 1996, c. 373, s. 1 (British Columbia); *The Privacy Act*, C.C.S.M. c. P125 (Manitoba); Privacy Act, R.S.N. 1990, c. P-22, ss. 3 and 4 (Newfoundland); *The Privacy Act*, R.S.S. 1978, c. P-24, ss.2-3 (Saskatchewan).

invasion of privacy tort called "intrusion upon seclusion."[80] The other provinces and territories in Canada have not yet recognized a tort of invasion of privacy.

Statutory Right of Privacy: There are similar statutory torts of invasion of privacy in British Columbia, Manitoba, Newfoundland and Saskatchewan. These provinces' respective privacy acts establish a cause of action for an invasion of privacy but have left the courts to define the contours of that right. If the *defendant acts wilfully (not a requirement in Manitoba) and without a claim of right* (in other words, the defendant didn't believe they had a right to intrude upon the plaintiff's privacy in the manner alleged), they will be liable to the plaintiff. The claim is actionable without proof of damage. Conduct that, in the absence of consent, is *prima facie* evidence of a violation of privacy includes surveillance of others, listening to or recording private conversations, or making use of personal documents such as diaries or letters. The tort clearly pertains to cases involving stalkerware, given the offensive conduct is exactly the type that this class of software facilitates. Remedies may include the award of damages, injunction, and return to the plaintiff of documents obtained by the defendant as a result of the violation.

Intrusion Upon Seclusion: In *Jones v Tsige*,[81] the Ontario Court of Appeal recognized a tort of intrusion upon seclusion. This tort allows a right of action for damages as a result of a significant and deliberate invasion of personal privacy. The three elements of the cause of action are: (1) the defendant's conduct must be intentional (which includes recklessness); (2) the defendant must have invaded the plaintiff's private affairs or concerns without lawful justification; and (3) a reasonable person would regard the invasion as highly offensive—causing distress, humiliation, or anguish. Intrusions into intimate aspects of one's life, such as financial or health records, sexual practices and orientation, employment, diary or private correspondence, qualify as "highly offensive" for the purpose of the test. The Court of Appeal's rationale for recognizing a common law right rested heavily on technological developments in the 21st century:

> The Internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information. As the facts of this case indicate, routinely kept electronic databases render our most personal financial information vulnerable. Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled and the nature of our communications by cellphone, e-mail or text message.
>
> It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily

80 *Jones v. Tsige*, 2012 ONCA 32.

81 2012 ONCA 32.

> accessible in electronic form. Technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the *Charter*, has been recognized as a right that is integral to our social and political order.[82]

The Court of Appeal held at that time that damages for this tort can be awarded in amounts up to $20,000. Awards of aggravated and punitive damages may also be appropriate in particularly serious cases. The recognition of this tort has clear implications for stalkerware technology given its ability to collect intensely personal information to the effect of causing distress, humiliation, or anguish to the targeted person.[83]

ii. Public Disclosure of Private Facts

A nascent common law tort of public disclosure of private facts may be developing in Ontario.[84] This tort would be engaged where an operator uses stalkerware to harvest highly private data about the target (such as sexual images) and discloses them publicly. This would include "revenge porn" scenarios and other serious forms of doxxing.[85] Doxxing (broadcasting private authentic information about a person against their will) essentially turns private data into a weapon against the target.

The case *Jane Doe 464533 v N.D.*[86] concerned non-consensual publication of intimate images. On a summary judgment motion, the judge found the defendant liable for three alternative causes of action: public disclosure of private facts, breach of confidence, and intentional infliction of mental suffering (the latter two are considered below). Regarding public disclosure of private facts, the court held:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[87]

82 *Ibid*.

83 Katherine Cooligan & Daniel Hohnstein, "'Intruding Upon the Seclusion of Personal Email' — What the Common Law Tort for the Invasion of Privacy Might Mean for Snooping Spouses and the Electronic Evidence that they Obtain," (2014) 34 *CFLQ* 135.

84 See for example, *S.D. v. Royal Winnipeg Ballet* (*c.o.b. The Royal Winnipeg Ballet School*), [2018] O.J. No. 1700 (S.C.J.), where this tort was recognized as a common issue in certified class proceedings relating to allegations regarding intimate images of students of the Royal Winnipeg Ballet that were distributed and/or sold.

85 For a recent case in the criminal context involving repeated instances of doxxing by an offender, see *R. v. B.L.A.*, 2015 BCPC 203.

86 2016 ONSC 541 .

87 *Ibid*.

The summary judgment motion was subsequently set aside for unrelated reasons, leaving the state of the law regarding the development of common law torts for disclosure of private facts uncertain. However, in 2018, the Ontario Superior Court of Justice again awarded general damages of $50,000, aggravated damages in the amount of $25,000, and another $25,000 in punitive damages in a civil judgment in another case that involved non-consensual publication of intimate images in an abusive domestic relationship. The Court recognized the existence of a tort of public disclosure of private facts after applying a common law analysis.[88] We expect that the law in this area will continue to develop.

iii. Breach of Confidence

The tort of breach of confidence typically applies in commercial contexts; however, the tort can also be applicable in cases of personal breaches of confidence. Three elements must be proven to establish a cause of action for breach of confidence: (1) the information has the necessary quality of confidence; (2) the information was imparted in circumstances importing an obligation of confidence; and (3) there was an unauthorized use of that information to the detriment of the party that shared the information in confidence. Detriment to the communicating party is ordinarily considered in commercial circumstances where the recipient has misused the confidential information for commercial advantage. However, in *Doe 464533 v N.D. (supra)*, Stinson J stated "I see no rational basis to distinguish between economic harm and psychological, emotional and physical harm."

Applying the analysis adopted by the court in *Jane Doe 464533 v. N.D.* (which concerned non-consensual distribution of intimate images), if a target provides an operator with confidential information on the understanding that the operator will hold that information in confidence, and the operator then uses the confidential information to the detriment of the target (e.g., using a cell phone password to install stalkerware on the target's phone), the operator could be found liable for breach of confidence.

iv. Intentional Infliction of Mental Suffering (IIMS)

This tort lets a claimant recover damages based on severe emotional distress that another individual causes. For a claimant to successfully bring an action for intentional infliction of mental suffering (IIMS), they must demonstrate that the

88 *Jane Doe 72511 v. Morgan*, 2018 ONSC 6607; see Omar Ha-Redeye, "Public Disclosure of Private Facts - Redux," *Slaw* (11 November 2018) <http://www.slaw.ca/2018/11/11/public-disclosure-of-private-facts-redux/>.

perpetrator has engaged in very offensive and outrageous conduct.[89] A defendant will be liable for their conduct where the plaintiff establishes that the defendant's conduct was (1) flagrant and outrageous, (2) calculated to harm the plaintiff, and (3) caused the plaintiff to suffer a visible and provable illness (e.g., severe mental suffering; depression; post-traumatic stress disorder).[90]

The nexus between IIMS and stalkerware technology is particularly stark where stalking and controlling behaviour through technological means becomes known to the target through any combination of physical threats, coercion, harassment, or threats to disclose private data, such as sensitive personal information or sexual images or videos. Such experiences are profoundly disturbing, humiliating, and degrading, and they can cause serious and long-term psychological harm for the victims of this form of abuse. In cases where such harms arise, this tort should be applicable.

v. Non-Intentional Torts, the Tort of Harassment, and Developing Adequate Legal Responses to Stalkerware Technology in the Civil Justice System

The causes of action described thus far in this section fall under the category of intentional torts. They apply where a defendant's *intentional* action caused a legally recognized harm to the plaintiff.

An operator's use of stalkerware technology is likely to engage causes of actions under the umbrella of intentional torts because of the deliberate nature of the actions required to covertly install malware on the target's mobile device and the deeply invasive features of the technology. However, in some circumstances, other torts, such as the Tort of Negligence, may apply to a given situation. This tort might be applicable to situations where the stalkerware operator owes a duty of care to the target. Unlike intentional torts, non-intentional or negligence-based torts are causes of action that arise when the defendant's conduct was sufficiently *careless or reckless* that it caused legally-recognized harm to the plaintiff.

It is an open question in Canada whether there is (or will become) a **Tort of Harassment** at common law. Common law is developed by judges in court, as opposed to law created by governments in the form of legislation. Harassment and

89 *Merrifield v. Canada (Attorney General)*, 2019 ONCA 205.

90 *Merrifield v. Canada (Attorney General)*, 2019 ONCA 205 at para. 54.

stalking are prohibited under s. 264(1) of the *Criminal Code* (Criminal Harassment) where the activities cause the victim to fear for their safety. However, it is not clear at the time of writing whether there is a corollary common law tort of harassment that is available to victims of criminal harassment.

Generally, subjects of harassment or stalking resort to traditional intentional torts, such as assault, battery, intentional infliction of mental distress, trespass, nuisance, or defamation. In provinces where the causes of action are available, cases involving harassment or stalking may best be remedied by torts related to invasion of privacy or IIMS. The disadvantage of relying on such traditional intentional torts is that these torts may not capture the full extent of the wrongful conduct. Specifically, numerous discrete acts may be cumulatively far more damaging than one would expect when examining the operator's behaviour in isolation.

Manitoba is distinct from the rest of Canada on this issue. In 1999, the provincial government passed the *Domestic Violence and Stalking Act*, which provides an array of civil remedies for stalking and domestic violence. Included in the Act is a tort of stalking that is actionable without proof of damage. In 2016, Manitoba also passed the *Intimate Image Protection Act* to provide civil remedies in cases involving non-consensual distribution of sexual imagery. Manitoba has also recognized a tort of sexual harassment in *Lajoie v. Kelly (c.o.b. Swayzees Restaurant)*.[91]

While some lower courts in Canada have recognized a common law tort of harassment,[92] a recent decision of the Court of Appeal of Ontario in *Merrifield v. Canada (Attorney General)* challenges this tort's existence. After reviewing a number of lower court decisions that—as the Court of Appeal put it—"assume rather than establish the existence of the tort," the Court of Appeal declined to recognize a common law tort of harassment in Ontario.

Part of the Court of Appeal's rationale was that the tort of IIMS is already available.[93] However, the Court also recognized that the two torts are not the same. The Court

91 [1997] M.J. No. 52 (Q.B.). Note that in Ontario, the Superior Court of Justice rejected the existence of a common law cause of action for a tort of sexual harassment. However, that may be influenced by the fact that cases have been litigated in the employment context, which means the *Human Rights Code* (R.S.O. 1990, c. H.19) has exclusive jurisdiction over matters relating to harassment and discrimination on the basis of sex. Complainants of sexual harassment can commence an action under the *Human Rights Code*, and are therefore arguably not deprived of any remedy. See: *K.L. v. 1163957799 Quebec Inc.*, 2015 ONSC 2417.

92 *Mainland Sawmills Ltd. et al v. IWA-Canada et al*, 2006 BCSC 1195; *Savino v. Shelestowsky*, 2013 ONSC 4394; *McHale v. Ontario*, 2014 ONSC 5179; and *P.M. v. Evangelista*, 2015 ONSC 1419.

93 *Merrifield v. Canada (Attorney General)*, 2019 ONCA 205 at para. 42.

of Appeal described the difference between IIMS and the nascent tort of harassment as follows:

> Whereas IIMS requires flagrant and outrageous conduct, the proposed harassment tort would require only outrageous conduct. More significant, IIMS is an intentional tort, requiring an intention to cause the kind of harm that occurred or knowledge that it was almost certain to occur. This is a purely subjective test. . ., whereas the proposed tort of harassment would require either intention or objectively-defined reckless disregard. Finally, IIMS requires conduct that is the proximate cause of a visible and provable illness, whereas causing severe or extreme emotional distress is sufficient for the proposed tort of harassment.

The Court of Appeal ultimately concluded, "while we do not foreclose the development of a properly conceived tort of harassment that might apply in appropriate contexts, we conclude that Merrifield has presented no compelling reason to recognize a new tort of harassment in this case."[94]

It should be noted that the Court of Appeal's analysis in *Merrifield* does not engage any analysis of the offence of harassment under *criminal* law or the development of civil law in the technological age.[95] The absence of any discussion about the offence of criminal harassment is surprising. One of the key differences between IIMS and the proposed tort of harassment is that the latter includes intentional ***or reckless*** conduct on the part of the defendant. Under criminal law, the offence of criminal harassment may already be proven by proof of either mental state (intentionally or recklessly harassing the victim). In other words, the knowledge (*mens rea*) requirement can be satisfied by recklessness or willful blindness that the defendant's act caused the victim to be harassed. It would not, therefore, be a dramatic development in Canadian common law to likewise recognize a tort that is premised on proof of the same mental state.

The Court of Appeal in *Merrifield* may well have been concerned about overextending the reach of the law. However, an alternative option to rejecting the tort could have been used to limit the reach of the tort. The court could have adopted the same limiting factor under a civil law tort of harassment as already exists under the criminal offence of harassment: criminal harassment is made out only where there is proof that the defendant's conduct *caused the complainant to fear for their safety or the safety of anyone known to them*, and the complainant's fear was,

94 *Merrifield v. Canada (Attorney General)*, 2019 ONCA 205 at para. 53.

95 The facts in *Merrifield* did not have a technological component. The allegations in *Merrifield* related to relations between an employer and employee in a disciplinary setting.

in all the circumstances, reasonable. As described above, "safety" is *not* limited to physical safety but may include substantial psychological harm or emotional distress. This definition of safety is arguably a more appropriate delimiting criterion than requiring victims of harassment to prove the higher evidentiary thresholds under the tort of IIMS.

Nevertheless, the analysis from the Court of Appeal in *Merrifield* is helpful because the Court provides guidance from paragraphs 19-26 about the circumstances where it will be appropriate for a court to incrementally recognize the existence of novel cause of action. There is no tort in Canada that specifically addresses the use of stalkerware by an operator against a targeted person. However, civil law is an ever-evolving area of law, which means there is the potential for the law to develop new torts when losses arise in novel ways. To the extent that the existing causes of action (IIMS, public disclosure of private facts, or intrusion upon seclusion/breach of privacy) do not yield an adequate remedy in cases where a targeted individual has been victimized by surveillance through stalkerware, careful consideration should be made as to whether a novel tort must be recognized.

Cases involving the use of stalkerware technology—particularly in the context of intimate partner or gender-based abuse—are "facts that cry out for a remedy."[96] The need for a remedy was also influential in the Court of Appeal's analysis in *Jones v. Tsige*.[97] Unlike the factual circumstances in *Merrifield*, perpetrators of intimate partner abuse who use stalkerware to facilitate their abuse exhibit highly-concerning behaviours that need intervention by courts. Domestic abuse and gender-based violence are widely recognized as aggravating factors under both criminal and civil law. With respect to all of the causes of action, it would be appropriate for persons victimized by stalkerware operators to want to seek punitive damages to deter individuals from engaging in such reprehensible conduct in the future. Courts have recognized that while the principal forum for punishment remains the criminal law, punitive damages may also be awarded as a form of additional deterrence in the face of reprehensible behavior. And, unlike in the factual circumstances in *Merrifield*, the use of stalkerware applications constitutes a novel form of conduct that is the result of a number of technological advancements in the digital age.[98]

96 *Jones v. Tsige*, 2012 ONCA 32 at para. 69.

97 *Ibid*.

98 Technological development was also an important factor in the Court of Appeal's analysis in *Jones v. Tsige* that led to the recognition of the novel tort of intrusion upon seclusion.

Notwithstanding the policy and legal reasons that support developing the common law in response to cases involving stalkerware technology, legislative responses (such as those adopted in Manitoba) would be the most straightforward path toward sending a clear message that the operation of stalkerware is unlawful.

Part 2: Legal Analysis of Creating and Developing Stalkerware

While significant responsibility for stalkerware-facilitated abuse lies with those who operate stalkerware to abusive ends, responsibility also falls to the parties involved in the surrounding commercial and technological ecosystem that supports the widespread availability and sale of stalkerware. In Parts 2 through 4 of this report, we examine the legal and policy issues that are implicated by those who create, develop, and directly or indirectly sell stalkerware in the consumer market.

Assessing the legal ramifications of creating, developing, and selling stalkerware can be challenging because it is a dual-use technology. As defined in **Information Box 3: Report Terminology**, "dual use" generally means technology that may be intended or used for legitimate or benevolent ends, but which is equally capable of or repurposed for illegal, harmful, or unethical practices.

Stalkerware is considered dual-use technology because it encompasses multiple categories of apps that each lend themselves to both beneficial and harmful ends.[99] Referring to the classifications in **Information Box 2: Classification of Stalkerware Technology**, repurposed spyware apps (e.g., child monitoring apps) and other repurposed technologies (e.g., GPS tracking apps or built-in phone GPS) give stalkerware its dual-use nature. These apps have ostensibly "legitimate" aims, but they are then used by operators against targeted individuals, turning the apps into stalkerware whether the developers intended such or not. It is also worth noting that even objectives often considered "legitimate," such as surveilling children or employees, raise legal and ethical questions, which complicate the dual-use nature of the technology.[100]

In the context of criminal and tort law, attributing and determining liability for stalkerware abuse focuses predominantly on the operator's actions, rather than

---

99 The dual nature of many technologies is also why some consider technology in general to be "neutral," thus placing all responsibility for any negative consequences of its use or misuse on users alone. However, a longstanding and formidable body of academic literature, law and technology scholarship, and science and technology studies has thoroughly interrogated and brought this view into question. See, e.g., Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006); Langdon Winner, "Do Artifacts Have Politics?," (1980) 109(1) *Daedalus* 121 <https://www.cc.gatech.edu/~beki/cs4001/Winner.pdf>; and Anupam Chander & Vivek Krishnamurthy, "The Myth of Platform Neutrality" (2018) 2 Geo L Tech Rev 400 <https://georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Chander-Krishnamurthy-pp-400-16.pdf>.

100 For a discussion of these legal and ethical questions, see Part 5, Section A: "Challenges of Dual-Use Nature of Stalkerware: How Legitimate Are "Legitimate" Spyware Apps?."

on the technology itself. Where the technology can be used for either good or ill, however, the law can be more hesitant in holding its creators or vendors accountable for acts that a third party has committed with the technology in question. Additional complexity in attributing or determining liability beyond the operator does not mean, however, that other actors who are involved in developing and distributing stalkerware do not, or ought not to, have legal obligations.

Legal obligations could involve preventative measures, such as designing apps in a way that mitigates or prevents harm on a technical level. Such obligations might remove or constrain an operator's ability to misuse the technology. For example, the simple act of removing a spyware app's concealment feature (i.e., where the app becomes "invisible" and does not appear anywhere on the target's device) would mitigate the possibility of covert surveillance in most cases, as would implementing features such as just-in-time notifications and persistent notifications during recording or logging activities. However, this design change would not remedy situations where a targeted individual is coerced or manipulated by an abusive partner into installing stalkerware onto their phone. Refusals to remove the concealment feature or provide clear notifications are just two examples of how actors involved in the stalkerware industry could be implicated in harms visited upon targeted individuals, to an extent that may justify legal liability.

Writing about commercial spyware in the context of repressive governments that target human rights activists, journalists, and political dissidents, McKune and Deibert suggest:

> [T]here is no single mechanism best suited to addressing the problems associated with the spyware trade; instead, we are better served by engaging a constellation of practices. When combined, these other practices can be thought of as a "web of constraints" around the commercial spyware market. While abuses of commercial spyware will likely never be eliminated entirely, this web of constraints can help build a community of practice, and legal and normative progress, that mitigate against them moving forward.[101]

The approach described by McKune and Deibert would apply to the stalkerware market as well. This report highlights as many threads as possible in building an effective legal and normative "web of constraints" around stalkerware. In addition, it contributes to a "constellation of practices" among support workers, victims' advocates, lawyers, police officers, gender equality NGOs, and civil society more

101 Sarah McKune and Ronald Deibert, "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking," *The Citizen Lab* (2 March 2017) <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf> at p. 4.

generally to support and assist those targeted by stalkerware operators, while preventing further abuse, harassment, and violence to targeted individuals and potential future targets.

The remainder of this section of the report, Part 2, focuses on legal and policy issues that apply to creators and developers of stalkerware apps. Section A discusses the human rights obligations that apply to stalkerware developers (provided they are also vendors) and Canada's human rights obligations with respect to businesses operating or based in the country, under the United Nations *Guiding Principles on Business and Human Rights* and the *Canadian Charter of Rights and Freedoms*. Section B reviews industry efforts at self-regulation, such as professional codes of ethics and grassroots worker protests, and assesses their likelihood of efficacy with respect to stalkerware. Section C provides a legal analysis of how Canadian laws address or fail to address "harmful innovations," including through criminal liability, product liability and class action proceedings, and intellectual property law including copyright, trademark, and patents.

A. Human Rights Obligations Apply to Spyware Companies

Canada is a signatory to numerous international human rights treaties and has long professed its ongoing commitment to human rights.[102] Based on these commitments, Canada has a responsibility to meet these obligations by providing mechanisms in domestic law for remedy and enforcement against abuses of stalkerware. While this report elsewhere details potential legal strategies to pursue against stalkerware-facilitated abuse in Canadian tort law, criminal law, privacy law, and intermediary liability law—with a focus on businesses specifically in the latter two areas—Canadian human rights law and governance also has a role to play, domestically and as informed by Canada's international human rights obligations. Businesses have a standalone obligation to respect human rights.[103] The UN Human Rights Council endorsed the *Guiding Principles on Business and Human Rights* in

102 See, e.g., Government of Canada, "Canada's approach to advancing human rights," <https://international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/advancing_rights-promouvoir_droits.aspx?lang=eng>; and Janice Dickson, "Freeland: Canada will always defend human rights," *CTV News* (6 August 2018) <https://www.ctvnews.ca/politics/freeland-canada-will-always-defend-human-rights-1.4042604>.

103 United Nations Human Rights Office of the High Commissioner, "*Guiding Principles on Business and Human Rights*: Implementing the United Nations 75 'Protect, Respect and Remedy' Framework," A/ HRC/17/31 (New York and Geneva, 2011) <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> at p. 13. The UN Guiding Principles have also been incorporated into the OECD Guidelines for Multinational Enterprises: "OECD Guidelines for Multinational Enterprises: 2011 Edition," OECD (2011) <https://www.oecd.org/daf/inv/mne/48004323.pdf>.

June 2011, and the document serves to "clarify and elaborate on the implications of relevant provisions of existing international human rights standards" and their implementation.[104] These existing international human rights standards are rooted in binding international instruments such as the *International Covenant on Civil and Political Rights* (ICCPR) and the *International Covenant on Economic, Social and Cultural Rights* (ICESCR). Canada has ratified both instruments.[105] The ICCPR and ICESCR arose from the *Universal Declaration of Human Rights* (UDHR);[106] the Declaration is an international normative moral force that "represents the universal recognition that basic rights and fundamental freedoms are inherent to all human beings, inalienable and equally applicable to everyone, and that every one of us is born free and equal in dignity and rights."[107]

Human rights obligations apply to all businesses around the world regardless of size or location. These obligations are, in part, rooted in businesses' role as "specialized organs of society performing specialized functions" and which are "required to comply with all applicable laws and to respect human rights."[108] Such requirements exist independent of countries' human rights obligations and stand apart from, and on top of, any domestic or international human rights laws and regulations that apply to a given business.[109]

The business model of many stalkerware companies involves enabling a private individual to track, monitor, and collect the intimate details of another private individual's daily digital activities, including where they are, whom they speak with, what they say, what they hear, and what they see (through photos and videos). All

104 United Nations Human Rights Office of the High Commissioner, "Frequently Asked Questions about the *Guiding Principles on Business and Human Rights*," United Nations Human Rights Office of the High Commissioner, HR/PUB/14/3 (2014) at p. 1 and 8.

105 Government of Canada, "Reports on United Nations human rights treaties," Department of Canadian Heritage (30 October 2017) <https://www.canada.ca/en/canadian-heritage/services/canada-united-nations-system/reports-united-nations-treaties.html>.

106 United Nations, "Human Rights Law," <https://www.un.org/en/sections/universal-declaration/human-rights-law/index.html>.

107 *Ibid*.

108 *United Nations Human Rights Office of the High Commissioner*, "*Guiding Principles on Business and Human Rights*: Implementing the United Nations 75 'Protect, Respect and Remedy' Framework," A/ HRC/17/31 (New York and Geneva, 2011) <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> at p. 13.

109 *Ibid* at p. 13. See also the discussion on corporate social responsibility and businesses' human right obligations with respect to commercial spyware sold to governments of repressive regimes: Jakub Dalek, et al, "Planet Netsweeper: Section 3 - Discussion & Conclusions," *The Citizen Lab* (25 April 2018),<https://citizenlab.ca/2018/04/planet-netsweeper-section-3-discussion-conclusions/>.

these activities may occur without the operator informing the targeted person of the surveillance or obtaining their meaningful consent. Such surveillance may occur in the context of legal disputes between former partners;[110] however, operators also use stalkerware in ongoing relationships to assert power and control over targeted persons, and to instill fear, intimidation, and isolation in the targeted individual.[111] These uses of stalkerware therefore constitute a form of intimate partner violence, abuse, and harassment that occurs in the context of gender inequality and technology-facilitated gender-based violence.[112]

Because stalkerware is used to perpetuate gender-based and intimate partner violence, abuse, and harassment, stalkerware app developers and vendors are implicated in fundamental human rights violations under instruments such as the UDHR and ICCPR.[113] These violations include a targeted individual's right to be free from "arbitrary interference with [their] privacy, family, home or correspondence" and protection of the law against such;[114] the right to freedom of opinion and expression,"[115] including the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers . . . through any other media of [their] choice;"[116] the right to freedom of association;[117] the right to life, liberty, and security of the person;[118] and the right to protection against discrimination.[119]

110 See, e.g., *U (AJ) v. U (GS)*, 2015 ABQB 6, a custody case in which the father illegally obtained evidence through installing spyware on the mother's computer, and included it in a "Divorce Defence Book."

111 Danielle Keats Citron, "Spying Inc." (2015) 72:3 *Washington and Lee L Rev* 1243 <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=4464&context=wlulr> at p. 1257-58; "Technology-Facilitated Stalking: What You Need to Know," National Network to End Domestic Violence (22 May 2017) <https://nnedv.org/latest_update/technology-facilitated-stalking/>; Heather Douglas, Bridget Harris & Molly Dragiewicz, "Technology-Facilitated Domestic and Family Violence: Women's Experiences," (2019) 59 *The British Journal of Criminology* <https://academic.oup.com/bjc/advance-article-abstract/doi/10.1093/bjc/azy068/5281174?redirectedFrom=fulltext> at p. 2-3.

112 Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto), Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović (November 2017) <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf>.

113 United Nations General Assembly (1948), "*Universal Declaration of Human Rights*," United Nations (10 December 1948) <http://www.un.org/en/universal-declaration-39human-rights/> [UDHR]; United Nations General Assembly (1976), "*International Covenant on Civil and Political Rights*," United Nations (16 December 1966) <http://www.ohchr.org/en/40professionalinterest/pages/ccpr.aspx> [ICCPR].

114 UDHR, Art. 12; ICCPR, Art. 17.

115 UDHR, Art. 19; ICCPR, Art. 19.

116 ICCPR, Art. 19(2).

117 UDHR, Art. 20; ICCPR, Art. 22.

118 UDHR Art. 3; ICCPR, Art. 9.

119 UDHR, Art. 7, ICCPR, Art. 26.

Depending on the circumstances and individuals involved, operators' use of stalkerware in cases of intimate partner abuse may also implicate the targeted individual's right of ethnic, religious, or linguistic minorities to engage in their own community, culture, religion, and language.[120] Additionally, stalkerware-facilitated abuse may violate an individual's ability to exercise their right to "freedom of thought, conscience and religion," including manifesting such "alone or in community with others and in public or private."[121] If technology-facilitated abuse takes place within a conjugal relationship or former relationship, that would further violate the "equality of rights and responsibilities of spouses as to marriage, during marriage and at its dissolution."[122]

The abusive uses and dissemination of stalkerware, where allowed to continue, may also engage the UN *Convention on the Elimination of All Forms of Discrimination Against Women* (CEDAW),[123] another binding international treaty that Canada has ratified.[124] In particular, Article 3 requires signatories to "ensure the full development and advancement of women, for the purpose of guaranteeing them the exercise and enjoyment of human rights and fundamental freedoms on a basis of equality with men."[125] Other articles address specific aspects of ensuring "the maximum participation of women on equal terms with men in all fields,"[126] such as in political and public life, education, employment, health, and economic and social benefits.[127] The type of dynamic that operators' usage of stalkerware introduces or exacerbates in intimate partner violence, abuse, and harassment prevents the targeted persons, most often women, from fully accessing and benefiting from maximum participation in society as CEDAW requires.[128] Specifically, when being targeted by stalkerware, some may retreat from public life or private activities to the detriment of their ability to engage in politics, pursue education, retain or obtain employment, seek health services, or otherwise participate in social, political, or economic pursuits and deriving the associated benefits of such pursuits.

120 ICCPR, Art. 27.

121 UDHR, Art. 18; ICCPR Art. 18.

122 ICCPR, Art. 23(4).

123 United Nations Entity for Gender Equality and the Empowerment of Women, "Convention on the Elimination of All Forms of Discrimination against Women" <https://www.un.org/womenwatch/daw/cedaw/text/econvention.htm> [CEDAW].

124 Government of Canada, "Reports on United Nations human rights treaties," *Department of Canadian Heritage* (30 October 2017) <https://www.canada.ca/en/canadian-heritage/services/canada-united-nations-system/reports-united-nations-treaties.html>.

125 CEDAW, Art 3.

126 CEDAW, Preamble.

127 CEDAW, Arts 7, 10, 11, and 12.

128 See generally Heather Douglas, Bridget Harris & Molly Dragiewicz, "Technology-Facilitated Domestic and Family Violence: Women's Experiences," (2019) 59 *The British Journal of Criminology*.

Businesses are responsible, under the *Guiding Principles on Business and Human Rights* (GPBHR), for adverse human rights impacts their activities cause The GPBHR imposes responsibilities on businesses to avoid causing or contributing to adverse human rights impacts, to address such adverse impacts where they occur, and to prevent or mitigate adverse human rights impacts "that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."[129] These duties include conducting human rights due diligence, assessing the impacts of activities on human rights, acting on findings, ceasing or preventing any known contribution to adverse human rights impacts, and providing remediation.[130]

Notably, businesses must verify whether they have adequately addressed their adverse human rights impacts by tracking "the effectiveness of their response" based, in part, on feedback from those impacted.[131] This requirement means that stalkerware businesses are obligated, at minimum, to consult affected groups and individuals such as women who are negatively impacted by stalkerware, and to assess whether their business is adequately addressing the human rights violations that result from their business activities or business relationships. That is to say, stalkerware companies must consult women and other individuals who have been harmed by the creation, sale, and ultimate use of stalkerware, which has been deployed to stalk, intimidate, coerce, extort, or control targeted persons, including in the furtherance of gender-based or intimate partner violence, abuse, and harassment.

Particularly relevant in the stalkerware context is that the GPBHR requires businesses to demonstrate heightened sensitivity and greater consideration towards "individuals belonging to specific groups or populations that require particular attention, where they may have adverse human rights impacts on them." The GPBHR expressly indicates, as groups requiring heightened human rights sensitivity: "indigenous peoples; women; national or ethnic, religious and linguistic minorities; children; persons with disabilities; and migrant workers and their families."[132]

129 United Nations Human Rights Office of the High Commissioner, "Guiding Principles on Business and Human Rights: Implementing the United Nations 75 'Protect, Respect and Remedy' Framework," A/ HRC/17/31 (New York and Geneva, 2011) <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> at p. 15.

130 *Ibid* at p. 17, 21, and 24.

131 *Ibid* at p. 22 (Guiding Principle 20).

132 *Ibid* at p. 14.

Based on our review of businesses' human rights obligations under the GPBHR, we conclude that such obligations are squarely engaged where companies are involved in the development of stalkerware, given the increasingly well-known and documented association of stalkerware with gender-based and intimate partner violence, abuse, and harassment.

Information Box 9: The Wassenaar Arrangement and Challenges of Regulating Dual-Use Technology

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA) is a non-binding export control agreement between 42 countries, including Canada.[133] Members are expected to implement the agreement through domestic legislation. The WA regulates commercial spyware that is sold to governments. Such regulation is required due to the harms that arise where spyware is sold to repressive regimes with poor human rights track records, and where the technology is used to spy on and persecute human rights defenders, political dissidents, and journalists.[134] In regulating exports of commercial spyware, the WA has faced challenges that may similarly arise with attempted regulation or prevention of consumer sales of stalkerware.

In 2013, the WA faced significant backlash from security researchers, the cybersecurity industry, privacy and digital security advocates, and related experts. The backlash was in response to what was otherwise a laudable amendment to control the distribution of "intrusion software" and "IP network communications surveillance systems," in an attempt to more strictly control the dissemination of spyware. However, the WA's broad definitions would have potentially imposed onerous export licensing obligations on many of the everyday cybersecurity research tools, security research activities, and cross-border information-sharing and vulnerability-disclosure practices, that cybersecurity professionals relied on.[135] A late 2017 update revised the new provisions to refine relevant definitions and add explicit exceptions to address these concerns. However, the WA remains limited in that each member country must interpret and implement the agreement's provisions through domestic regulations. [136]

133 *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, Founding Documents, WA-DOC (17) PUB 001 (February 2017) <https://www.wassenaar.org/>.

134 See, e.g.: The Citizen Lab's series on the abuse NSO Group's spyware in Mexico, including John Scott-Railton, et al, "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware," *The Citizen Lab* (20 March 2019) <https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/>; Bill Marczak, et al, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* (18 September 2018) <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>; Bill Marczak, et al, "NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident," *The Citizen Lab* (31 July 2018) <https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/>.

135 Kim Zetter, "Why an Arms Control Pact has Security Experts up in Arms," *WIRED* (24 June 2015) <https://www.wired.com/2015/06/arms-control-pact-security-experts-arms/>; Sergey Bratus, "Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It," (Public comment, 9 October 2014) <https://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf>.

136 Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnera-

The regulatory process and controversy surrounding the "intrusion software" amendments in the WA may serve as guidance for how to more effectively regulate stalkerware. Specifically, lawmakers and regulators must consult knowledgeable technical experts early on when drafting any legislative or regulatory reforms. They should also consult those who are most impacted by stalkerware, i.e., individuals who have been targeted by stalkerware or are vulnerable to being targeted by stalkerware, and representatives from communities that would be most affected by legal reform in this area, such as support workers, victims' and survivors' advocates, and non-profit organizations that work on the issue of gender-based abuse and violence against women, both technology-facilitated and otherwise.

Additionally, in critiquing the limitations of WA as a licensing regime, McKune and Deibert point out, "[p]erhaps most importantly, [export controls] subject regulatory efforts to the artificial constraint of designating an item for control, as opposed to focusing on the questionable practices of this industry."[137] Any legal or regulatory reforms proposed to address the harms of stalkerware should focus on the business practices of those who develop and sell this type of technology, as the UN Guiding Principles on Business and Human Rights also recommends. This would ensure that legislation and policy is precisely targeted at the core harms involved, while avoiding either overreach capturing unrelated and beneficial activities such as security research, or under-inclusion of relevant stalkerware business practices.

i.Canada's Business and Human Rights Obligations

As a signatory of multiple international human rights instruments,[138] Canada has a responsibility to implement its international human rights commitments by providing mechanisms in domestic law for remedy and enforcement against abuses that arise from the creation, sale, and use of stalkerware. The UN *Guiding Principles on Business and Human Rights*, on its own, does not constitute a legal mechanism that provides redress to victims of abusive business practices. Instead, these Principles explicitly set out businesses' human rights obligations and the obligations that states must enforce in the course of governing and regulating

bility Research," *Lawfare Blog* (5 January 2018) <https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research>; Tom Cross, "New Changes To Wassenaar Arrangement Export Controls Will Benefit Cybersecurity," *Forbes* (16 January 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/01/16/new-changes-to-wassenaar-arrangement-export-controls-will-benefit-cybersecurity/#2256df7d5ed6>.

137 Sarah McKune & Ronald Deibert, "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking," *The Citizen Lab* (2 March 2017) <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf> at p. 7 (emphasis in original).

138 See, e.g., Government of Canada, "Canada's approach to advancing human rights", <https://international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/advancing_rights-promouvoir_droits.aspx?lang=eng>; and Janice Dickson, "Freeland: Canada will always defend human rights", *CTV News* (6 August 2018) <https://www.ctvnews.ca/politics/freeland-canada-will-always-defend-human-rights-1.4042604>.

business activities, in accordance with pre-existing international human rights law and standards.

The Government of Canada and the judiciary must adhere to the *Canadian Charter of Rights and Freedoms*. The *Charter*, like the UDHR and ICCPR, protects the right to "freedom of thought, belief, opinion and expression" (section 2(b)); freedom of association (section 2(d)); the "right to life, liberty and security of the person and the right not to be deprived thereof" (section 7); the right "to be secure against unreasonable search or seizure" (section 8); and the right to "equal protection and equal benefit of the law without discrimination," particularly "discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability" (section 15(1)).[139] Section 8, in particular, has undergirded constitutional privacy rights with respect to electronic communications.

Where the Charter does not directly apply (e.g., in the case of private actors), the Canadian executive[140] and administrative[141] branches of government must still apply *Charter* values and relevant human rights principles in their discretionary decisions concerning businesses that operate or are based in Canada. Adhering to these values and principles might involve decisions about whether to provide funding to certain businesses or organizations, or otherwise lend them political support or social license (perceived or otherwise). For example, the Citizen Lab has previously called on the Canadian government to cease supporting and promoting an Internet filtering company known as Netsweeper, whose activities have raised human rights concerns abroad.[142] In the context of stalkerware, the Canadian government should ensure it does not provide funding support or otherwise to stalkerware businesses, and instead establish measures to prevent or mitigate human rights abuses that result from the unethical use of technology created by Canadian companies.

B. Professional Ethics and Industry Initiatives

There are no laws or regulations that apply to all technology sector workers and computer programmers as a category of professionals, in a manner akin to

139 *Constitutional Act, 1982,* Part 1, "Canadian Charter of Rights and Freedoms."

140 *Operation Dismantle Inc. v. R.,* (1985), [1985] 1 S.C.R. 441; *Khadr v. Canada (Prime Minister)*, 2010 SCC 3.

141 *Doré v. Quebec*, 2012 SCC 12 at paras. 55-58.

142 Letter from Ronald J Deibert (Professor, Department of Political Science, University of Toronto and Director, Citizen Lab, Munk School of Global Affairs and Public Policy) to The Honourable Chrystia Freeland, Minister of Foreign Affairs, His Excellency Roberto Ampuero Espinoza, Minister of Foreign Affairs (Ministry of Foreign Affairs of Chile), and Randy Boissonnault, Special Advisor to the Prime Minister of Canada on LGBTQ2 Issues and Member of Parliament for Edmonton Centre (31 July 2018), <https://citizenlab.ca/wp-content/uploads/2018/07/citizen_lab_open_letter_erc_sm.pdf>.

medical malpractice law in the context of doctors or licensing regimes as applied to lawyers. However, calls to integrate mandatory ethics and accountability into the technology and software engineering sectors have been magnified as Internet and technology companies have amassed escalating political power, technological capabilities, and societal influence, alongside numerous scandals resulting from revealed abuses of power, unethical business practices, or insufficient attention to user privacy and safety.[143] These calls have likely grown in tenor for many reasons, including the public's rising awareness of privacy and data protection implications linked to popular online services;[144] concerns about the long-term impact of online platforms and algorithms on human society, psychology, and well-being;[145] and the uneven distribution of advanced technology's benefits and harms across groups of people and between citizen and state.[146] Many reform proposals and policy recommendations have emerged from this public concern. Among these proposals are suggestions to impose a fiduciary duty on certain kinds of Internet companies;[147]

143 See, e.g., Lizzie O'Shea, "Tech has no moral code. It is everyone's job now to fight for one," *The Guardian* (25 April 2018) <https://www.theguardian.com/commentisfree/2018/apr/25/tech-no-moral-code-racist-ads-cambridge-analytica-technology-ethical-deficit>; Mae Capozzi, "Should Software Engineers Care About Ethics?," *Digital Culturist* (20 April 2018) <https://digitalculturist.com/should-software-engineers-care-about-ethics-8b1d98a62b66>; Kathy Pham, "Honouring All Expertise: Social Responsibility and Ethics in Tech," Berkman Klein Luncheon Series (17 April 2018) <https://cyber.harvard.edu/events/2018/luncheon/04/ethicaltech>; Chris Wysopal, "The ethics of creating secure software," *CSO* (7 September 2018) <https://www.csoonline.com/article/3304300/application-development/the-ethics-of-creating-secure-software.html> ("Software development has shifted from simply a technical process to an exercise of social morality"); B. Cameron Gain, "DevOps Ethics: The Danger of Unethical Code," DevOps.com Blog (11 September 2018) <https://devops.com/devops-ethics-the-danger-of-unethical-code/>; Sharon Florentine, "Should software developers have a code of ethics?," *CIO* (30 March 2018) <https://www.cio.com/article/3156565/developer/should-software-developers-have-a-code-of-ethics.html>.

144 Phoenix Strategic Perspectives Inc., "2016 Survey on Privacy: Final Report," Officer of the Privacy Commissioner of Canada (December 2016) <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/#toc1-3> at s. 3.

145 Dominic Rushe, "Facebook sorry – almost – for secret psychological experiment on users," *The Guardian* (2 October 2014) <https://www.theguardian.com/technology/2014/oct/02/facebook-sorry-secret-psychological-experiment-users>; Holly Shakya and Nicholas Christakis, "A New, More Rigorous Study Confirms: The More You Use Facebook, the Worse You Feel," *Harvard Business Review* (10 April 2017) <https://hbr.org/2017/04/a-new-more-rigorous-study-confirms-the-more-you-use-facebook-the-worse-you-feel>; Alice Warton, "New Studies Show Just How Bad Social Media Is For Mental Health," *Forbes* (16 November 2018) <https://www.forbes.com/sites/alicegwalton/2018/11/16/new-research-shows-just-how-bad-social-media-can-be-for-mental-health/#463293f67af4>; Robbie Gonzalez, "Your Facebook Posts Can Reveal if You're Depressed," *WIRED* (16 October 2018) <https://www.wired.com/story/your-facebook-posts-can-reveal-if-youre-depressed/>.

146 See, e.g., Kate Crawford, "Artificial Intelligence's White Guy Problem," *The New York Times* (26 February 2016) <https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html>.

147 Jack M Balkin, "Information Fiduciaries and the First Amendment", (April 2016) 49:4 *UC Davis L Rev* 1185.

to pass new transparency legislation;[148] and to establish mandatory ethics courses in software coding programs, computer science degrees, and similar education paths to careers in coding.[149]

In addition to these developments, there have been some efforts at self-regulation from within the technology sector itself.[150] While such initiatives are voluntary and do not constitute, nor are they equivalent to, law or formal regulations, they nonetheless serve as an important normative signalling force to the rest of the industry. For example, the Association for Computing Machinery (ACM) updated its Code of Ethics and Professional Conduct in July 2018 in recognition of present-day concerns.[151] This update was the first since 1992, when the ACM and Institute of Electrical and Electronics Engineers (IEEE) Computer Society jointly developed and adopted the previous version of the Code. In announcing the new Code, the ACM stated that it would apply to its approximately 100,000 members[152] across 190 countries. Specifically, the Code recognizes that "[b]ecause computing is now inextricably linked into almost every aspect of society, the actions of computing professionals have more impact than ever before. It is imperative that everyone in our field act responsibly."[153]

Several key principles in the ACM Code of Ethics and Professional Conduct seem to bar software and computer professionals from knowingly creating, developing, maintaining, or otherwise contributing to the proliferation of stalkerware. In

148 Bill S. 1989, *Honest Ads Act*, 115th Congress (2017-2018).

149 As written by Dave West, "[a]cademically, this movement is already in the works. Harvard University and the Massachusetts Institute of Technology (MIT) are jointly offering a new course on the ethics and regulation of artificial intelligence, the University of Texas at Austin recently introduced its Ethical Foundations of Computer Science course and Stanford University is developing a computer science ethics course for next year:" "Why Tech Companies Need a Code of Ethics for Software Development", *Entrepreneur* (19 April 2018) <https://www.entrepreneur.com/article/311410>.

150 Lorenzo Franceschi-Bicchierai, "Kaspersky Lab Will Now Alert Users to 'Stalkerware' Used In Domestic Abuse," *Motherboard* (3 April 2019) <https://motherboard.vice.com/en_us/article/vbw9g8/kaspersky-lab-alert-stalkerware-domestic-abuse>.

151 Association for Computing Machinery, "World's Largest Computing Association Affirms Obligation of Computing Professionals to Use Skills for Benefit of Society," (17 July 2018)<https://www.acm.org/media-center/2018/july/acm-updates-code-of-ethics>.

152 The ACM is a non-profit organization, and membership is obtained voluntarily, through paying an annual membership fee and nominally agreeing to adhere to the organization's Code of Ethics and Policy Against Harassment. Many join for access to new research, published scholarship, and an extensive digital library, in addition to discounted conference registration fees.

153 Association for Computing Machinery, "World's Largest Computing Association Affirms Obligation of Computing Professionals to Use Skills for Benefit of Society," (17 July 2018)<https://www.acm.org/media-center/2018/july/acm-updates-code-of-ethics>.

particular, commentary for Principle 1.1, "Contribute to society and to human well-being," states:

> This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority.[154]

Similarly, the Code requires software professionals to "[a]void harm," which includes "unjustified physical or mental injury, unjustified destruction or disclosure of information;" to engage in "careful consideration of potential impacts;" and to mitigate any unintended harm as much as possible, or "ensure that [intended] harm is ethically justified."[155] Principle 1.4, "Be fair and take action not to discriminate," sets out that "[t]he use of information and technology may cause new, or enhance existing, inequities."[156]

Of particular importance is Principle 1.6, "Respect privacy:"

> The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. … Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups.[157]

The Code also calls on software professionals to recognize that "[p]rofessional competence starts with technical knowledge and with awareness of the social context in which their work may be deployed."[158] Principle 3.1 mandates: "Ensure that the public good is the central concern during all professional computing work. People—including users, customers, colleagues, and others affected directly or indirectly— should always be the central concern in computing."[159]

It is worth noting that the joint IEEE CS/ACM Code of Ethics that had been in place since 1992 includes largely similar principles, such as:

154 ACM Code of Ethics and Professional Conduct, Principle 1.1, commentary <https://www.acm.org/code-of-ethics>.

155 *Ibid*, Principle 1.2.

156 *Ibid*, Principle 1.4.

157 *Ibid*, Principle 1.6.

158 *Ibid*, Principle 2.2, commentary.

159 *Ibid*, Principle 3.1.

> Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate: […] 1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. […] 1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools." [160]

Developing and selling software in a way that facilitates the abusive and harmful ends that stalkerware often serves, without genuine attempts to bar such uses through technological design and initial coding, should run counter to software industry associations' standards of ethics and professional conduct. For instance, the human rights violations and infringement on targeted persons' autonomy that arise when operators employ stalkerware would contravene Principle 1.1 ("human well-being"), while invasive monitoring of all of someone's mobile communications and device activities would contravene Principle 1.6's edict to "respect privacy."

Violations of the Code of Ethics may be reported to the ACM Committee on Professional Ethics or to ACM leadership. Complaints trigger an enforcement process that may encompass any of the following escalating stages: initial review, potential remediation, a preliminary inquiry, convening of a 3-member panel from the ACM Council, a Council hearing, determination of remedies, and appeal.[161] Consequences of confirmed violations of the Code may include a "letter of admonishment," temporary conference or volunteering bans, community service, bans from publishing in ACM publications, or expulsion.[162] This process applies only to members of the ACM and its Special Interest Groups; membership in the ACM is entirely voluntary and the chair has sole discretion to decide whether or not the committee will pursue a given complaint. Moreover, complainants must report violations within 180 days and final decisions require a three-fourths majority of Council members to take effect.[163] All of these factors, together, may limit the effect of the Code in the industry overall. Even if other industry organizations apply similar codes of ethics to their own members, such as the IEEE,[164] their voluntary and discretionary nature, and inability to apply to the sector as a whole, raise questions about their effectiveness. There is arguably a need to look beyond self-regulatory initiatives when protecting the public interest and mitigating the harms of poor or hostile software design.

160 Don Gotterbarn, Keith Miller & Simon Rogerson, "Software Engineering Code of Ethics," (1997) 40:11 Communications of the *ACM* 110.

161 Association for Computing Machinery, "ACM Code of Ethics Enforcement Procedures,"<https://www.acm.org/code-of-ethics/enforcement-procedures>.

162 *Ibid*.

163 *Ibid*.

164 IEEE, "IEEE Code of Conduct," (June 2014) <https://www.ieee.org/about/compliance.html>.

Both individuals and organizations in the mobile app industry (as with most other industries) have "essential roles to play as guardians of business ethics."[165] In implicit recognition of this principle, a spate of public protests arose among employees who objected to controversial projects at Google ("Project Maven"), Microsoft, and Amazon ("Rekognition")[166] in 2018. Technology workers at each company pressured their respective employers to cancel or reconsider contracts with the U.S. military and law enforcement agencies.[167] While it is positive to see some employees protest on human rights grounds, the technology sector as a whole is unlikely to adequately and reliably safeguard the public interest and human rights without the reinforcement of legal mechanisms; to our knowledge, there have been no equivalent protests from the employees of stalkerware companies, as an example. Thus, meaningful structural, institutional, and cultural shifts that recognize the potential human rights impacts of certain technologies or design choices, in addition to legal requirements and obligations, are needed amongst developers and engineers,[168] particularly with respect to women and intersecting socio-political identities.

C. Regulating Harmful Innovation

There are several areas of Canadian law that may limit or regulate stalkerware creators: criminal law, product liability law, and intellectual property law. These laws relate to consumer protection or legal protection for innovation. Criminal and product liability law may be applied when goods and services are suspected of being disproportionately harmful, while intellectual property law could potentially provide an indirect way to impede the development or dissemination of stalkerware apps.

i. Criminal Law and Product Liability

Criminal law and product liability law in Canada regulate manufacturers who produce unreasonably dangerous products. These areas of the law are likely to be

165 Jonathon Penney, et al, "Advancing Human Rights-by-Design in the Dual-Use Technology Industry", forthcoming in *Colum J of Int'l Aff* (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3218975> at p. 9.

166 Ali Breland, "Amazon employees protest sale of facial recognition tech to law enforcement," *The Hill* (21 June 2018) <https://thehill.com/business-a-lobbying/393583-amazon-employees-protest-sale-of-facial-recognition-tech-to-law>.

167 Nitasha Tiku, "Why Tech Worker Dissent is Going Viral," *WIRED* (29 June 2018) <https://www.wired.com/story/why-tech-worker-dissent-is-going-viral/>.

168 See, e.g., Cade, "On Weaponised Design," *Our Data Ourselves* <https://ourdataourselves.tacticaltech.org/posts/30-on-weaponised-design/>.

engaged in the context of stalkerware technology. Due to the significant overlap under these areas of the law with respect to both *creating* and *selling* stalkerware apps, this area of liability is discussed in Part 3(A) and 3(B) of this report.

ii. Intellectual Property Law

Intellectual property law regulates and protects intangible assets that people or entities create, whether through authorship, invention, building goodwill and branding, or other form of creation that falls under one or more relevant areas of law. Three major areas of intellectual property law may apply to stalkerware apps depending on the app's specific design or technical mechanisms. These areas include copyright, trademark, and patent law.

a) Copyright and Trademark Law

Copyright law is not intended and should not be relied on to address the core harms that arise from the widespread availability and use of stalkerware.[169] However, we include it here to demonstrate the full breadth of ways in which stalkerware apps may be legally questionable. The Canadian *Copyright Act* defines the protected category of "literary work" to include "computer programs," and defines "computer program" as "a set of instructions or statements, expressed, fixed, embodied or stored in any manner, that is to be used directly or indirectly in a computer in order to bring about a specific result."[170] If a spyware company or app developer can demonstrate that another company or developer copied their software as the basis of the latter's stalkerware app or is selling an app with copied code, and provided that the copying did not fall under "fair dealing" exceptions,[171] the stalkerware company could be liable for copyright infringement (for reproduction)[172] or secondary infringement (for selling or possessing in order to sell).[173] Stalkerware vendors could also be subject to criminal liability for selling software that infringes copyright.[174] If found to have infringed on another party's copyright, a stalkerware company would have to discontinue using the copied code and/or pay damages to

169 For example, if the initial app developer agreed to license their code to the stalkerware app company, this would satisfy copyright law and simply redistribute revenues earned from sales of the abusive technology.

170 *Copyright Act*, R.S.C. 1985, c. C-42, s. 2.

171 Fair dealing applies when the law permits the reproduction or otherwise use of someone's copyrighted work without their authorization. Examples of fair dealing include using someone's work for research or private study, education, criticism or review, news reporting, non-commercial user-generated content, parody, or satire: *Copyright Act*, R.S.C. 1985, c. C-42, s. 29-30.

172 *Copyright Act*, R.S.C. 1985, c. C-42, s. 27(1).

173 *Copyright Act*, R.S.C. 1985, c. C-42, s. 27(2).

174 *Copyright Act*, R.S.C. 1985, c. C-42, s. 42.

the initial developer.[175] Where the initial developer opposed the use of their code for stalkerware purposes on moral grounds, they could sue the stalkerware developer or company on grounds of having infringed their moral rights and their copyright. The aggrieved party could seek the same remedies of an injunction and/or damages in such a legal proceeding.[176]

Trademark law is not intended to and would not provide a remedy to the core harms of stalkerware in a way that protects or provides redress for targeted individuals. The applicability of trademark law is limited to potentially reducing the public availability of stalkerware apps where the app developers have engaged in trademark infringement. For example, some forms of malware have been designed to look identical to, and been mistaken for, legitimate apps such as Telegram and Instagram:

> "Once installed, some of these Telegram 'clones' have access to mobile devices' full contact lists and messages, even if the users are also using the legitimate Telegram app. In the case of phony Instagram apps, the malicious software sends full session data back to back-end servers, which allows the attacker to take full control of the account in use," Cisco explained.[177]

If a company has a valid trademark, such as their name and logo, they have the "exclusive right to the use throughout Canada" of that logo, with respect to their goods or services.[178] A legitimate app company whose app has been imitated by a stalkerware app, to an extent that would cause consumers to confuse the two,[179] could thus pursue the stalkerware vendor for engaging in trademark infringement. Such legal action on the part of the legitimate app company would preserve the trust and security of its own users, while also potentially reducing the availability of stalkerware on the consumer market and protecting potential targeted persons.

b) Patent Law

Stalkerware companies could seek to patent their computer code under Canada's patent laws if that code were designed in a way that meets the criteria for novelty, utility, obviousness and patentable subject matter.[180] Software code (or a "computer

175 *Copyright Act*, R.S.C. 1985, c. C-42, s. 34.

176 *Copyright Act*, R.S.C. 1985, c. C-42, s. 28.1 and 34(2).

177 Phil Muncaster, "Fake Telegram Apps Used to Spy on Iranian Users," *Info Security Group* (6 November 2018) <https://www.infosecurity-magazine.com/news/fake-telegram-apps-used-spy/>.

178 *Trade-marks Act*, R.S.C., 1985, c. T-13, s. 19.

179 *Trade-marks Act*, R.S.C., 1985, c. T-13, s. 20.

180 *Re Amazon.com Inc.*, 2011 FCA 328 at para. 34.

program") alone is not patentable subject matter,[181] but a computer program may be patentable as part of a larger invented system involving a computer or device. What specifically such a patent may cover—which is often determined based on technical mechanisms and specific configurations or interactions—has been the source of significant and long-running legal turmoil and confusion.[182] Resulting from this uncertainty, the possibility thus remains that stalkerware developers could be eligible for patents depending on the specific design of their software and how it interacts with particular devices. A stalkerware business might also seek a patent if they move beyond designing apps and produce novel mobile devices that integrate stalkerware functionalities.[183]

These possibilities raise the question of whether such inventions could be refused patents on grounds of public interest or likelihood of harmful consequences. Current Canadian patent law does not prohibit awarding patents to inventions that may be considered to have immoral, unethical, public-interest-violating, or harmful design or uses. Such a prohibition did exist in the Canadian *Patent Act* but was repealed in 1993, which "made it clear that granting a patent is not an expression of approval or disapproval […] Parliament thereby signaled, however passively, that these important aspects of public policy would continue to be dealt with by regulatory regimes outside the *Patent Act.*"[184]

181 Canadian Intellectual Property Office, "A guide to patents", Government of Canada (26 September 2018) <https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr03652.html>.

182 See, e.g., Canadian Intellectual Property Office, "A guide to patents", Government of Canada (26 September 2018) <https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr03652.html> ("You cannot patent a scientific principle, an abstract theorem, an idea, some methods of doing business or a computer program."); *contra* Cameron Gale, "Canadian Software Businesses Should Consider Patents Despite CIPO's Misleading Messages", Bereskin & Parr (22 February 2019) <https://www.bereskinparr.com/doc/canadian-software-businesses-should-consider-patents-despite-cipo-s-misleading-messages>; and Government of Canada, "Chapter 16: Computer-Implemented Inventions," in *Manual of Patent Office Practice* (MOPOP) <https://manuels-manuals.opic-cipo.gc.ca/w/ic/MOPOP-en#!fragment/zoupio-_Toc520378339/BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoAvbRABwEtsBaAfX2zgFYAmABgGYA7AA4+fAJwBKADTJspQhACKiQrgCe0AOSapEOLmwAbQwGEkaaAEJkuwmFwJlqjdtv2EAZTykAQhoBKAKIAMoEAagCCAHImgVKkYABG0KTsEhJAA>.

183 For instance, FlexiSPY already offers popular mobile devices (from other manufacturers) pre-installed with their stalkerware: <https://www.flexispy.com/en/express.htm>. This is not quite the same as a mobile device that includes built-in native functionalities intended to be used as stalkerware, but demonstrates how stalkerware businesses do not necessarily limit their products and services to selling only the stalkerware apps themselves.

184 *Harvard College v. Canada*, 2002 SCC 76 at para. 14. The Court proceeded to discuss Bill C-13 (as it was called at the time), the *Assisted Human Reproduction Act*, would have banned activities such as cloning human beings or modifying human germ lines, but would not prevent inventions towards those aims from being patented, concluding, "[t]his illustrates, again, the fundamental distinction made by Parliament between patentability of an invention and regulation of activity associated with an invention" (at para. 15).

This hands-off approach with respect to assessing the public interest, ethical value, or implications of a particular innovation at the patent stage is in contrast to the approach taken in Europe and international treaties that Canada has signed and ratified. For instance, the World Trade Organization *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS) states that "[m]embers may exclude from patentability inventions, the prevention within their territory of the commercial exploitation of which is necessary to protect *ordre public* or morality, including to protect human, animal or plant life or health or to avoid serious prejudice to the environment, provided that such exclusion is not made merely because the exploitation is prohibited by their law." Similarly, the UN Committee on Economic, Social and Cultural Rights has stated, "States [sic] parties should prevent the use of scientific and technical progress for purposes contrary to human rights and dignity, including the rights to life, health and privacy, e.g., by excluding inventions from patentability whenever their commercialization would jeopardize the full realization of these rights."

At this point, it does not appear that Canadian patent law would be of any use in addressing the problems that arise from stalkerware. Moreover, Canadian patent law is traditionally agnostic about the value judgments that would be involved in refusing a patent on public interest grounds. However, a reversal of this policy could give greater meaning to patent law's underlying implicit bargain between the monopoly rights given to creators and the public interest in their inventions.[185]

185 Benjamin J. Kormos, "Giving Frankenstein a Soul: Imposing Patentee Obligations," (2009) 21 *IPJ* 309. However, under the current patent system, there is also the remote possibility that a public interest-minded individual may engage in "offensive patenting" of a stalkerware program or stalkerware device specifically to aggressively assert the patents against would-be stalkerware developers, while not using their own patent to develop such software or devices, and thus impeding the creation and deployment of such technology.

Part 3: Legal Analysis of Selling Stalkerware

In this Part of the report we examine the potential legal liability of stalkerware businesses, companies, and vendors. Stalkerware developers may also be considered vendors if they are selling the apps they have created. This Part proceeds as follows: Section A analyzes stalkerware vendors' criminal liability under the Canadian *Criminal Code*. Section B subjects stalkerware vendors and developers to an analysis under product liability law and class action proceedings. Section C conducts a consumer privacy law analysis of stalkerware issues under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and compares Canadian privacy obligations and enforcement measures to those established by the European Union's General Data Protection Regulation (GDPR). Section D discusses the applicability of *Canada's Anti-Spam Legislation* (CASL) to stalkerware.

A. Criminal Liability of Vendors under the *Criminal Code*

Creating and selling stalkerware technology potentially engages multiple criminal offences under the *Criminal Code* in Canada. Under the *Code*, individual developers, vendors, and stalkerware companies, may be subject to criminal prosecution.

i. Sale of Intercept Devices

It is an offense under the *Criminal Code* to possess, sell, or purchase a device (or a component of a device) that is primarily useful for surreptitious interception of private communications.[186] Section 191(1) of the *Criminal Code* states:

> Every one who possesses, sells or purchases any electro-magnetic, acoustic, mechanical or other device or any component thereof knowing that the design thereof renders it primarily useful for surreptitious interception of private communications is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

The definition of "any electro-magnetic, acoustic, mechanical or other device," is provided in the *Criminal Code* as follows: "any device or apparatus that is used or is capable of being used to intercept a private communication. . . ." This definition has since been interpreted purposively and broadly.[187] In *Lyons v. The Queen*, the

186 This offence carves out exceptions for the use of such devices by law enforcement authorities.

187 *Lyons v. The Queen*, [1984] 2 S.C.R. 633 at 664.

Supreme Court of Canada held that an intercept device refers to "any equipment or procedure relating to the electromagnetic spectrum. . . ."[188] The Court further held that Part VI[189] "is broad legislation embracing in these extensive provisions the use of a wide range of radio, telephone, optical and acoustical devices for listening to and recording private communications as broadly defined."[190]

In 2017, the Supreme Court again used broad language to describe the definition of intercept. The Court stated that "interception relates to actions by which a third party interjects itself into the communication process in real-time through technological means."[191] These provisions were applied in relation to the use of a computer to intercept private communications in *R. v. TELUS Communications Co*.[192] This application confirmed that Part VI of the *Criminal Code* is not limited to more traditional intercept devices *per se*, such as audio recorders or wiretap devices and, indeed, extends to contemporary modes and methods of interception. Further support for this interpretation comes from the fact that the offence under s. 191 of the *Criminal Code* applies to "any component thereof" of a device which facilitates interception, in addition to the possession or sale of a "device."

As a result, an app or computer program that is designed to intercept private communications by allowing another individual to surreptitiously listen to or read the private communications of a target in real-time will likely fall within the definition of an intercept device under this offence. Consequently, stalkerware developers and companies that possess and sell spyware programs that intercept private communications such as emails, SMS, phone calls, and other voice- or text-based messaging platforms (as many of the major stalkerware apps do) would likely run afoul of the offence under section 191 of the *Criminal Code*. The criminal intent of selling intercept devices is satisfied where it is proven that the individual *knows* that the design of the device or a component of a device, is "primarily useful for surreptitious interception of private communications."[193] The criminal consequences of committing this offence may include up to two years in custody.

188 *Ibid*.

189 Part VI of the *Criminal Code* regulates invasions of privacy occasioned by the interception of private communications. It regulates when it is lawful or illegal under criminal law to intercept private communications.

190 *Lyons v. The Queen*, [1984] 2 S.C.R. 633 at 664.

191 *R. v. Jones*, [2017] 2 S.C.R. 696 at para. 72.

192 [2013] 2 S.C.R. 3 at para. 32.

193 *Criminal Code*, s. 191.

This offence would not apply to smart devices that may be reconfigured to enable surreptitious interception and/or recording of private communications.[194] The sale offence is limited to an individual who possesses or sells "any electro-magnetic, acoustic, mechanical or other device or any component thereof *knowing that the design thereof renders it primarily useful* for surreptitious interception of private communications." This limiting characteristic rules out criminalizing the sale of smartphones with native features that can be configured to intercept private communications because the intercept function is not the primary function of the phone. This is not to say that an individual who *uses* a smartphone to intercept private communications would not be committing an offence. As discussed in Part I of this report, it is an offence to intercept private communications in the absence of lawful authority.

ii. Illegal Commercial Activity in Relation to Computer Programs Designed to Commit Offences of Mischief in Relation to Computer Data or Unauthorized Use of a Computer System

Section 342.2 of the *Criminal Code* has not been closely considered by Canadian courts. Nevertheless, this section has potential implications for the (il)legality of commercial activity in relation to covert spyware programs in Canada. Section 342.2 makes it an offence for an individual or company to carry out a range of activities in relation to computer programs where those activities are "designed or adapted to primarily commit" the offences of mischief in relation to computer data or unauthorized use of a computer system. The offence criminalizes any individual or company that "makes, possesses, sells, offers for sale, imports, obtains for use, distributes or makes available" a computer program that falls within the scope of the offence. The extensive range of prohibited activities captured by this offence demonstrates Parliament's intention to construct a decisive criminal ban on profit-related activities in relation to illegal spyware programs.

To be found guilty of this offence, the government must prove that the individual or company knew that the device "has been used or is intended to be used to commit such an offence."[195] The criminal penalty for this offence is imprisonment for up to two years.

194 For example, some online reports describe how the "live listen" function on an iPhone can be repurposed for remote eavesdropping when used with wireless Airpods.

195 *Criminal Code*, s. 342.2(1).

As described in Part 1, Section A(i), the invasive functions of stalkerware applications may cause the company or individual selling them to fall within the scope of this offence. Regardless of whether the app is programmed by default to operate covertly or provides an operator with the clear opportunity to operate the program covertly, by their very nature, the defining characteristics of spyware apps are to surreptitiously gain unauthorized access to a target person's mobile device in order to access data held on (or transmitted from) that device. Further, many of the available apps also provide added features that enable the operator to interfere with data on the targeted person's mobile device in a number of ways, engaging the further offence of mischief in relation to computer data.

However, a limiting factor may mean this offence cannot provide a clear criminal prohibition against the consumer-level commercial trade in spyware for repurposed spyware apps in the absence of law reform. This is due to the "colour of right" defence that is available in respect of the offence of unauthorized use of a computer (section 342.1(1)) or mischief in relation to computer data (section 430(1.1)); in either of these cases, the stalkerware operator might possess what is termed a *colour of right*. Colour of right "refers to a defendant's honest belief, even if mistaken or unreasonable, that he or she was legally permitted or authorized to do the act in question."[196] This defence is relevant in the context of dual-use spyware programs because some individuals may use the spyware program on the basis that they believe they are allowed to do so. For example, a parent who surreptitiously monitors their child through a spyware app may have an honest belief that they are justified in doing so.

The colour of right defence in the underlying offences may mean that the *selling* offence under section 342.2 of the *Criminal Code* will not prevent the sale of spyware apps if the spyware program is being used in a manner that is not illegal. To be found guilty of the *selling* offence under section 342.2, the Crown must prove two elements of the offence:

1) That the spyware program being sold is "designed or adapted primarily to commit an offence under section 342.1 or 430;"
2) That the vendor selling the spyware app also knew "that the device has been used or is intended to be used to commit such an offence."[197]

196 *R. v. Livingston*, 2018 ONCJ 25 at para. 82

197 *Criminal Code*, s. 342.2

These elements of the selling offence create a catch-22 that may undermine the purpose of the offence. If the company that sells the spyware program is advertising the product in a manner that causes the purchasers to believe that the product is legal and useful for benevolent purposes (e.g., child safety), the vendor could therefore cause many users to have a colour of right in the use of the app. In doing so, the app being sold would no longer be designed or adapted "primarily" for the purpose of the computer-based offences under sections 342.1 or 430, and the vendor would therefore not be in violation of the selling offence. The outcome of this interaction would be absurd, as it would essentially enable spyware vendors to shrink the scope of offences by advertising products in order to profit from activities that would otherwise be illegal.

Since this offence has not yet been closely analyzed in Canadian courts, it is unclear how these issues will play out in a criminal prosecution. As the selling offence is currently framed under the *Criminal Code*, the question of whether a particular vendors' sale of spyware is an offence will come down to a factual question of whether the prosecution has evidence that the app is primarily intended or designed to be used for the computer-based offences in section 342.1 and 430, and whether the prosecution can prove that the vendor knew that the app had been used illegally. The latter would be not be onerous, if there is evidence that the vendor knew that the spyware app was being used for surreptitious intimate partner surveillance in at least *some* contexts. But it is much more difficult to quantify whether dual-use apps are "primarily" designed for illegal use, given the colour of right defence could arguably justify a range of surreptitious surveillance (e.g., child monitoring) that would otherwise contravene the offences under sections 342.1 and 430.

Federal lawmakers should re-examine whether the colour of right defence is the right fit for the offences under sections 342.1 and 430(1.1) in the circumstances of intrusive commercially-available spyware programs that enable covert surveillance and interference with another individuals computer data. It is unusual to use the language of colour of right in a context where the federal lawmakers are seeking to change behaviour. For example, there is a colour of right defence to the offence of theft. This makes sense because, generally speaking, it is readily understood that the crime of theft is in fact a crime. However, given the power that spyware vendors have in framing what people believe through advertising practices, it is arguably inappropriate to enable vendors to essentially undermine the scope and purpose of the offences for the purpose of profiting off of intrusive spyware programs.

Two options could clarify this element of the law. First, the offences under section 342.1 and 430(1.1) could be amended to provide a defence of a "lawful excuse" instead of the colour of right defence. Lawful excuse is another commonly used term that provides a defence to numerous offences under the *Criminal Code*. While there is no standard definition of excuse in the *Criminal Code*, the *Code* does make clear that ignorance of the law is not an excuse.[198] Second, the selling offence under section 342.2 could instead be amended to make it clearer that the surreptitious capabilities of the spyware program are what render the sale of the program illegal, even if it were theoretically possible that the program could be used in a manner that provides the individual user with a defence. This amendment would better enable the law to cut off the supply of covert spyware apps in the consumer marketplace at the source.

iii. Risk-Based Offences: Criminal Negligence, Common Nuisance, and Dangerous Products

Individuals or corporations that sell stalkerware applications that facilitate gender-based abuse may face criminal investigation and potential prosecution for offences relating to endangerment of the public, namely **Criminal Negligence** and **Common Nuisance**. Criminal negligence involves engaging in conduct that shows a wanton or reckless disregard for the life or safety of others.[199] Common Nuisance, in contrast, occurs where an individual or corporation "does an unlawful act or fails to discharge a legal duty and thereby. . .endangers the lives, safety, health, property or comfort of the public[.]"[200] Safety has been interpreted by courts to include safety from physical harm and from substantial psychological harm or emotional distress. Given the increasingly recognized association between stalkerware and intimate partner surveillance and abuse, these two offences are engaged by the commercial sale of stalkerware due to the harm caused for the targets of harassment, stalking, and abuse.

In addition to *Criminal Code* offences, the *Canada Consumer Product Safety Act* generally prohibits individuals and companies from manufacturing, importing, advertising, or selling a consumer product that is a danger to human health or safety. Furthermore, this *Act* prohibits any person from advertising or selling a

198 *Criminal Code*, s. 19. An example of the lawful excuse defence in the context of surveillance activities is the offence of trespassing at night, which was interpreted by the Ontario Court of Appeal in *R. v. Priestap*, [2006] O.J. No. 1511 (C.A.).

199 *Criminal Code*, s. 219.

200 *Criminal Code*, s. 181.

consumer product that they know is a danger to human health or safety.[201] Health Canada (which administers the *Act*) can resort to the courts and seek criminal charges against a person or company that has contravened the *Act*.[202] Given that stalkerware can pose a harm or danger to persons targeted with the software, a legal argument might assert that stalkerware cannot be manufactured, advertised, or sold.

Information Box 10: Criminal Offences that Apply to Selling Repurposed (Dual-Use) Spyware Apps

In this report, we discuss two categories of spyware apps for mobile devices: intimate partner spyware apps (i.e., apps that are intentionally designed or advertised to facilitate surveillance of an intimate partner's mobile device) and repurposed spyware apps (i.e., apps that are intentionally and primarily designed for the purpose of covertly surveilling another individual's activities on their mobile device, but which are not explicitly advertised for intimate partner surveillance). Repurposed spyware apps include those that are marketed as programs designed to monitor employees or children. Repurposed spyware apps are forms of dual-use technology. Dual-use technologies may purportedly be intended for legitimate or benevolent ends are equally capable of or repurposed for illegal, harmful, or unethical practices.

It should not be assumed that selling either intimate partner or repurposed (i.e., dual-use) spyware apps is legal in Canada. The offence of selling an intercept device likely prohibits the sale of both intimate partner spyware apps and repurposed spyware apps, so long as the vendor knows that the app is "primarily useful" for surreptitiously intercepting private communications. In other words, the fact that the app is primarily useful to function in that manner is what makes selling the app illegal. As most spyware apps appear to enable the surreptitious interception of private communications, the implications of this offence for the commercial spyware market in Canada are far-reaching.

Other criminal laws could likewise make the sale of dual-use spyware apps illegal. However, the analysis is more contextual in respect of these potential offences. As a result, it is difficult to reach a general conclusion that would apply to every spyware app vendor. The following factors will generally apply:

- **How does the spyware app function? Does it allow for surreptitious surveillance?**
- **How does the vendor advertise its product? Would some or most of the advertised uses of the apps be illegal?**
- **What does the vendor know about the specific uses of its app? Note, however, that knowledge is not determinative where the offence criminalizes recklessness.**

201 *Canada Consumer Product Safety Act*, S.C. 2010, c. 21 at s. 7-10.

202 *Ibid* at s. 41 and 42.

- **What does the vendor know about the prevalence of harmful and/or illegal uses of its app?**
- **What has the vendor done (or not done) to prevent harmful or illegal uses of its app?**

Risk-based offences (e.g., criminal negligence or common nuisance discussed in Part 5, Section A(iii)) may apply to intimate partner surveillance apps and repurposed spyware apps. This holds due to the offences' focus on the danger and harm caused by the sale and subsequent abuse of the spyware app as opposed to upon whether there are also other benign uses of the app.

The offence under section 342.2(1) of selling a spyware program that is "designed or adapted to primarily commit" other computer-based offences (i.e., mischief in relation to computer data and unauthorized use of a computer), at first glance, appears to be directly applicable for both intimate partner spyware apps and repurposed spyware apps, depending on all the circumstances. However, compared to the offence of possessing an intercept device, it is less likely that this offence would clearly apply in the context of selling repurposed spyware apps. The key question that the offence looks at is what proportion of the intended or designed uses of the app are uses that are offences under sections 342.1 and 430(1.1) of the *Criminal Code*. This is not as obvious in the context of repurposed spyware apps. The reason for this is due to the fact that neither of the offences of mischief in relation to computer data (section 430(1.1) and unauthorized use of a computer system (section 342.1) apply where the individual engaging in the surreptitious act has a "colour of right." Colour of right means a good faith belief that one is entitled to do the act that is otherwise criminal. This is described in more detail in Part 3, Section A(ii).

B. Product Liability and Class Proceedings

Manufacturers and vendors of stalkerware apps could face claims on multiple grounds relating to dangerous or defective product design under Canada's product liability law. Several variables would affect what causes of action may be available against a stalkerware developer or vendor. Specifically, these variables are associated with the functionality of the spyware, the terms of use between the spyware company and the purchaser, and the legal or statutory framework in place in the particular province.

Generally speaking, product liability law includes contract law[203] and tort law principles. Even where there is a contractual relationship between a manufacturer or vendor and a consumer, tort law liability may sometimes operate concurrently.[204] In the absence of a contractual relationship between the claimant and the company, tort liability likely governs the legal claim. Legal claims pursuant to product liability

203 Contract law is also referred to in the consumer context as warranty law that is often comprised of both common law and statutory law depending on the province.

204 *Central and Eastern Trust Co. v. Rafuse et al*., [1986] 2 S.C.R. 147.

tend to focus on misrepresentations, failures to warn, negligent or defective design, or negligent or defective manufacture of a product.

Multiple claims associated with product liability and class proceedings may pertain in the case of stalkerware applications. Claims will depend on the functionality of the program and the conduct or due diligence of the spyware company. For example, if a spyware developer or vendor fails to warn consumers of the dangers inherent in the use of its product and where it knows or has reason to know of these harms, the company might be liable under these sets of laws.[205] A duty to warn applies in respect of the ultimate consumer. Given stalkerware apps are installed on the target's device, it could be argued that the duty is owed to the target (as opposed to the operator who actually purchases the app). Even the (in)sufficiency of an attempt to warn may lead to a cause of action:

> Once a duty to warn is recognized, it is manifest that the warning must be adequate. It should be communicated clearly and understandably in a manner calculated to inform the user of the nature of the risk and the extent of the danger; it should be in terms commensurate with the gravity of the potential hazard, and it should not be neutralized or negated by collateral efforts on the part of the manufacturer. The nature and extent of any given warning will depend on what is reasonable having regard to all the facts and circumstances relevant to the product in question.[206]

Even robust warning labels may be insufficient in the context of powerful, consumer-level, covert spyware programs. The manufacture and sale of such programs is inherently dangerous for targets of stalkerware technology. An action against a company could arise for negligence or gross negligence on the basis of negligent design. In determining whether a product contains a design defect, the legal question is whether the design of the product poses an unreasonable risk of harm to either the user or third parties who would be foreseeably affected by the product.[207] That would arguably not be a contentious question when it comes to spyware apps: where the product itself is illegal (such as a spyware program that is primarily useful for surreptitiously intercepting private communications), the actual sale of the program to a stalkerware operator would not simply be negligent, it would be a criminal offence under Canadian law. The criminalization of the sale is indicative of the product's dangerousness. Even apart from any criminal prohibition, Canadian courts have repeatedly recognized the harm and damages occasioned by invasions

205 *Buchan v. Ortho Pharmaceutical (Canada) Ltd.* (1986), 54 O.R. (2d) 92 at para. 16 (C.A.); *More v. Bauer Nike Hockey Inc*., 2011 BCCA 419.

206 *Ibid* at para. 18.

207 Douglas Harrison, Yves Martineau & Samaneh Hosseini, "Canada," in Harvey Kaplan, Gregory Fowler and Simon Castley, eds, *Product Liability 2013* (London, UK: Law Business Research Ltd, 2013) at p. 28;

of privacy, harassment, and technology-facilitated gender-based violence.[208] These issues are relevant to both intimate partner spyware apps and repurposed spyware apps.

Furthermore, the *Canada Consumer Product Safety Act (CCPSA)* generally prohibits individuals and companies from manufacturing, importing, advertising, or selling a consumer product that is a danger to human health or safety, and prohibits any person from advertising or selling a consumer product that they know is a danger to human health or safety.[209] Manufacturers and vendors who violate those prohibitions may be subject to administrative penalties levied by Health Canada, or Health Canada can resort to the courts by seeking criminal charges against a person who has contravened the Act or regulations.[210] While the *Criminal Code* and *CCPSA* do not directly grant a private remedies for litigants, they are useful in shedding light on the scope of a spyware vendor's duty of care.

One question that arises in the stalkerware context is the nature of the relationship between a spyware company and the surveillance targets who was not involved or responsible for the purchase of the spyware program. In the absence of a contractual relationship between those parties, contract or warranty law principles may not apply. Instead, an action founded upon tort law principles is more likely to apply in a claim by a targeted person against a spyware developer or company. Generally speaking, the duty of care owed by manufacturers and distributors extends beyond the consumer to those that "might reasonably be foreseen to suffer injury or damage if the manufacturer or vendor fails to exercise reasonable care."[211] In the stalkerware context, the foreseeable danger of harm caused by a spyware program to a targeted person is not remote. A covert spyware program will be used to target third parties who are not party to the purchase of the program: this is the premise of the purported utility of the program. The same is also foreseeable where the vendor provides an operator-enabled option to use the program covertly in stealth mode. For consumer-level surveillance programs, their inherent purpose and design is to surveil third parties. Moreover, the dangerousness of consumer-level spyware programs in the context of intimate partner violence, abuse, and harassment has arguably now become notorious.[212]

208 See Part 1 of this Report.

209 *Canada Consumer Product Safety Act* (S.C. 2010, c. 21), s. 7-10.

210 *Ibid* at s. 41 and 42.

211 Dean F. Edgell, *Product Liability Law in Canada* (Markham, ON: Butterworths, 2000) at 1.

212 See the academic, research, and media resources listed in Appendix B of this report.

Many stalkerware companies hold out terms of use, disclaimers, or liability waivers in respect of illegal uses of the spyware program. However, it is an open question whether such disclaimers are legally effective in an action brought by a third-party surveillance target who has been harmed by the spyware program. Given the consumer context, the absence of 'sophistication'[213] of the purchasers and targets of stalkerware, and the inherent vulnerability of surveillance targets who are not notified of any waiver of liability regarding an operator's use of the spyware, a court may conclude that a waiver of third-party liability may be ineffective. Even where the spyware app has a user-enabled setting that activates a stealth mode or hidden mode (i.e., to conceal its operation from the targeted person), the immediately foreseeable consequences of providing operators with that *option* may make it difficult for a spyware company to shift liability to the stalkerware operator who turns the 'stealth mode' option on in a given case.

Other causes of action may arise concerning data leaks and breaches that are associated with spyware companies that sell stalkerware apps. Depending on the particular province, deemed warranties[214] with respect to consumer goods and services[215] generally apply as a matter of law that will override any attempt to limit the stalkerware company's own liability for their failure to maintain the security of personal data obtained through the stalkerware app. These deemed warranties establish an implied warranty on the part of the vendor that the goods or services are of reasonably acceptable quality. Reporting by *Motherboard* suggests that stalkerware spyware companies may be vulnerable to liability on the basis that they often secure personal information poorly.[216] In some coverage, *Motherboard* reports that a spyware company left an entire database of personal images, recordings, and other data exposed in a publicly available online location. The company did nothing to remedy the vulnerability when it was contacted to fix the data breach.[217] According to *Motherboard*, there have "been 12 stalkerware companies that have either been breached or left data exposed online" in the last two years.[218]

213 In legal parlance, "sophistication" denotes the amount of knowledge, resources, power, and legal experience that a party to a contract has.

214 A warranty means a legal promise that is made regarding the quality of a good or service by a vendor to consumer. A deemed warranty means the promise is imposed on the vendor by law.

215 See for example, in Ontario: *Consumer Protection Act*, 2002, S.O. 2002, c. 30, Sched. A at s. 9

216 Lorenzo Franceschi-Bicchierai, "This Spyware Data Leak is So Bad We Can't Even Tell You About It," *Motherboard* (22 March 2019) <https://motherboard.vice.com/en_us/article/j573k3/spyware-data-leak-pictures-audio-recordings>.

217 *Ibid*.

218 *Ibid*.

Class action proceedings may be a useful vehicle for access to justice for groups of persons targeted by spyware programs and who may be unaware that they have been victimized. Class action proceedings would likely also serve as an important tool for deterring companies from making spyware programs available in the Canadian marketplace. In class action proceedings, the class plaintiff may seek compensatory damages for class members who have personally suffered damages as a result of a stalkerware developer's or vendor's conduct and non-compensatory damages, such as punitive or aggravated damages, that are intended to have a deterrent effect. One of the purposes of class proceedings is to facilitate behaviour modification in the commercial sector incentivizing companies to come into compliance with Canadian law. Given their potential to encourage behaviour modification, class action suits may be able to modify the business practices of stalkerware companies, especially those offering dual-purpose applications.

C. Consumer Privacy and Data Protection Law

Individuals in Canada have a quasi-constitutional right to privacy, recognized by the Supreme Court of Canada:

> Privacy legislation has been accorded quasi-constitutional status… This Court has emphasized the importance of privacy — and its role in protecting one's physical and moral autonomy — on multiple occasions… [T]he growth of the Internet, virtually timeless with pervasive reach, has exacerbated the potential harm that may flow from incursions to a person's privacy interests. In this context, it is especially important that such harms do not go without remedy.[219]

Privacy rights extend across a wide variety of online contexts, including contexts associated with mobile devices, the personal data such devices contain, and the software that is installed on them, such as mobile applications ("apps"). In fact, as Adrian Fong writes, "the data privacy implications associated with apps are heightened beyond traditional data collection means because of apps' ability to collect data instantaneously, continuously, and often without knowledge of the user, at an extremely granular level. . . This micro-level collection of data … creates more pressing data privacy implications for individuals."[220]

The privacy concerns described arise where an individual has knowingly and willingly installed the app onto their own device, as a function of the app itself and its interrelations with the broader data-driven digital economy (see **Information**

219 *Douez v. Facebook, Inc.*, 2017 SCC 33 at para. 59.

220 Adrian Fong, "The role of app intermediaries in protecting data privacy," (2017) 25(2) *International Journal of Law and Information Technology* 85 at 90 (footnotes omitted).

Box 11: Privacy, Consent, and Mobile Apps in the Digital Economy). These concerns are amplified several-fold in the case of stalkerware apps, where a targeted individual did not knowingly or willingly install the app onto their device. Instead, the targeted person either is unaware the spyware app was installed and is tracking them, or was coerced into installing the software by an abusive operator. In addition, many spyware apps market themselves as being undetectable once set up on a target's phone, suggesting that consent is neither contemplated nor afforded in at least some use cases. As such, stalkerware raises even more severe and significant privacy concerns compared to the already heightened privacy concerns that mobile apps as a class implicate generally.

Consumer privacy rights and data protection in the context of private companies falls under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA),[221] or under "substantially similar" provincial legislation.[222] PIPEDA applies to private sector use and management of individuals' personal information, and the Office of the Privacy Commissioner of Canada (OPC) is responsible for upholding and enforcing PIPEDA.

This section of the report conducts a privacy law analysis of stalkerware vendors, including stalkerware developers who sell their products or services, under PIPEDA. Readers who reside in provinces with substantially similar legislation—which replaces PIPEDA in each of those provinces—are encouraged to refer to their respective provinces' privacy and data protection laws to determine how they would apply to the activities of stalkerware vendors and developers, and to consult a local lawyer if necessary.

Section i expounds why stalkerware companies and developers who are also stalkerware vendors are likely accountable, under PIPEDA, for their activities.[223] Section ii discusses potential exceptions that may make it difficult to hold

221 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

222 See e.g., British Columbia's *Personal Information Protection Act*, S.B.C. 2003, c. 63 [BC PIPA]; Alberta's Personal Information Protection Act, S.A. 2003, c. P-6.5 [AB PIPA]; and Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*, C.Q.L.R. c. P-39.1; Office of the Privacy Commissioner of Canada, "Provincial legislation deemed substantially similar to PIPEDA," (2017) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/>. In contrast, privacy rights as protected against the State are governed by section 8 of the *Canadian Charter of Rights and Freedoms*.

223 As this section of the report focuses on stalkerware companies alone, it does not include an analysis of PIPEDA's application to third-party intermediary platforms, such as mobile app stores, that facilitate the sale of stalkerware. However, Part 4 focuses entirely on these third-party intermediaries and thus includes a PIPEDA analysis therein.

a stalkerware company accountable under PIPEDA, where an operator uses stalkerware in the context of intimate partner abuse or gender-based violence. Section iii sets out a number of data protection rights that PIPEDA guarantees to individuals and that stalkerware companies likely violate. Section iv provides a brief parallel analysis of stalkerware companies under the European Union's General Data Protection Regulation (GDPR). This analysis highlights ways in which Canadian legislation could better protect targets' privacy rights in the context of stalkerware-facilitated abuse.

Based on our analysis, we conclude that stalkerware businesses ought to be accountable under PIPEDA, particularly given the Act's emphasis on meaningful consent and on collecting, using, or disclosing data only for "appropriate purposes." However, potential loopholes in current law may result in determinations that consider stalkerware companies to fall outside the Act's purview. The OPC should issue an interpretation bulletin or similar statement to confirm that PIPEDA obligations apply to stalkerware companies. Moreover, the OPC should make clear that stalkerware apps contravene the *Guidelines for obtaining meaningful consent* and the *Guidance on inappropriate data practices*. We further consider that, compared to data protection authorities' powers to enforce the GDPR in Europe, the OPC requires effective enforcement powers to meaningfully uphold PIPEDA in Canada. Such powers include the ability to impose administrative monetary penalties (AMPs), the ability to issue orders rather than recommendations, and the ability to compel companies to adhere to such orders. The absence of powers to enforce PIPEDA means that while privacy law may technically apply to stalkerware companies, the regulator is functionally challenged in actually preventing or mitigating these companies' harmful business practices or bringing them into compliance with the law.

Information Box 11: Privacy, Consent, and Mobile Apps in the Digital Economy

When it comes to discussing privacy and data protection in the context of stalkerware apps, there are two spheres of concern, each of which may undergo a slightly different analysis. The first sphere is the primary focus of this report: personal information and data that the stalkerware or repurposed spyware app collects from the target's device and makes available to the stalkerware operator. The second sphere of concern considers how stalkerware apps may simultaneously collect, use, or disclose data in the way that many mobile apps do regardless of their purpose, in the sense of tracking users' activities and behaviours for potential monetization or advertising. The consent that users give in this second context—often obtained by imputing consent in the app's Terms of Service or Terms of Use—may also be questionable or invalid, particularly if a user has not read or understood the Terms before installing and using the app. The result is that stalkerware may violate a target's consent on multiple levels: first, with respect to being monitored and tracked by the stalkerware operator, and second, with respect to having the app

itself collecting data from the target's device, regardless of whether that data is passed on to the operator.

At times, the impugned activities of stalkerware apps, when described, seem identical to the activities of a wide range of other apps, websites, Internet companies, and data brokers that constitute the "digital information economy" or "big data economy." However, there is a distinction in that such companies ostensibly must obtain consent from users in every case, and the user is the individual whose data is being collected. In the context of stalkerware-facilitated abuse, the application may not even nominally obtain consent from the individual whose data is being collected, where it has been surreptitiously installed onto a target's phone by the "user"/operator. Having said that, some may consider this distinction to be a thin one, particularly in the context of a much larger discussion and body of literature outside the scope of this report, including the concept of surveillance capitalism.[224]

Indeed, the Office of the Privacy Commissioner of Canada has issued a guidance specifically setting out best practices for mobile app developers, in conjunction with the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia.[225] These guidelines should inform interpretation and application of consumer privacy law to stalkerware vendors and developers. The guidance sets out principles and best practices such as developer accountability,[226] transparency,[227] and minimal, secure collection.[228]

Most pertinent to the stalkerware context, the guidance emphasizes that timing of consent is critical: apps should notify and obtain consent from individuals in real-time, such as activating a notification or symbol at the moment the app activates collection of data such as the user's location, or records a video or accesses photos.[229] This would mean that a stalkerware app should notify the targeted individual, through their device, each time the app actively accesses that individual's personal information. If the app is persistently monitoring and tracking the individual's activity and ongoingly exfiltrating their data, then a persistent indicator should appear and remain visible so long as the app is collecting the user's personal data.

224 See e.g., Shoshana Zuboff, "Big other: surveillance capitalism and the prospects of an information civilization" (March 2015) *J of Info Tech* 30:1 at 75-89.

225 "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps" (24 October 2012), online (pdf): Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/media/1979/gd_app_201210_e.pdf>. See also Tamir Israel, "Regulatory Guidance: Mobile Privacy, Tracking & Advertising" (31 October 2012), online: *CIPPIC* <https://cippic.ca/en/mobile_privacy_guidelines>.

226 "You should also ensure that all of your business arrangements and contracts are compliant with privacy laws because you are ultimately accountable." *Ibid* at p. 4.

227 While your app's privacy policy tells the user about your practices, you should also provide specific, targeted notifications to users when they need to make a decision about whether to consent to the collection of their personal information." *Ibid* at p. 5.

228 "[I]f your app transmits personal information, you should not log it unless it is necessary. If you have to log it, secure it and delete it as soon as possible.Avoid collecting information about a user's movements and activities through the use of location and movement sensors unless it relates directly to the app and you have the user's informed consent. Never collect sound or activate the device camera without the specific permission of the user." *Ibid* at p. 6.

229 *Ibid* at p. 8.

i. Stalkerware Vendor or Developer Accountability under PIPEDA

PIPEDA applies to every organization that "collects, uses, or discloses personal information in the course of commercial activities."[230] In the stalkerware context, PIPEDA would apply to a vendor or developer if the targeted person's data is considered "personal information" and if the data collection, use, or disclosure is considered to occur as part of "commercial activities." Canadian law and jurisprudence has defined both of these terms; the following subsections review and apply them to the stalkerware context.

PIPEDA also applies extraterritorially and thus to stalkerware companies so long as they have a "real and substantial" connection to Canada.[231] This connection is likely established where the following conditions are met: a stalkerware company is selling to, and supporting their applications' use by, operators in Canada; a stalkerware company is collecting, using, or disclosing the personal information of targeted individuals in Canada; and/or a stalkerware company is doing business in Canada.[232]

a) Do Stalkerware Companies Collect "Personal Information?"

PIPEDA defines "personal information" as "information about an identifiable individual."[233] Both the OPC and the courts have applied this definition broadly and found that various types of data constitute personal information, i.e., information that can be linked to an identifiable individual.[234] Personal information has been found to include biometric information, photographs, videos, Global Positioning System (GPS) data, and Internet Protocol (IP) addresses.[235] Data may also become personal information if there is a "serious possibility" that someone could combine it with other data to identify an individual, even if the initial piece of data itself would not lead to an identifiable individual.[236]

230 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 4(1)(a).

231 *Lawson v. Accusearch*, 2007 FC 125; Office of the Privacy Commissioner of Canada, "Canadian adware developer Wajam Internet Technologies Inc. breaches multiple provisions of PIPEDA," PIPEDA Report of Findings #2017-002 (17 August 2017) at para. 200; Office of the Privacy Commissioner of Canada, "After a significant Adobe data breach, customer questions company's security safeguards and the response it provided about impacts on his personal information," PIPEDA Report of Findings #2014-015 (3 September 2014).

232 *Ibid*.

233 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 2(1).

234 Office of the Privacy Commissioner of Canada, "Personal Information." (11 October 2013), online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/>.

235 *Ibid*.

236 *Ibid*.

Stalkerware applications generally collect and disclose to the operator any to all of the following information: SMS text messages, call logs and call histories, location and GPS data, contacts, web-browsing history and bookmarks, the contents of social media accounts (including direct messages on Twitter, matches on Tinder, and messages on Instagram), chat logs and histories from online messaging apps (e.g., WhatsApp, Snapchat, Facebook Messenger, WeChat, LINE, or Telegram), all keystrokes that the target makes while using the device, and photos and videos that are stored on the device. Much of this information would reveal or be easily linked to an identifiable individual, the target, and thus would be considered "personal information" under PIPEDA.

Information Box 12: Friends and Family: Stalkerware Collection of Third-Party Personal Information

The analysis carried out in this report is primarily concerned with the personal information and privacy rights of a targeted individual whose device was infected with stalkerware. However, it is important to realize that collection or disclosure of certain kinds of information also involves data that may constitute personal information (as defined by PIPEDA) of third-party individuals, such as friends, family, colleagues, or support workers, with whom the victim communicates. Such data includes, for instance, SMS text conversations, call logs, and private chat or messaging histories. The privacy rights of those in contact with the target are also engaged, and their consent and data protection rights may also be violated by a stalkerware app on the target's device.[237] See section ii(b) for discussion on how the OPC may consider third parties' consent to be implied in this context.

b) Do Stalkerware Businesses Engage in "Commercial Activity?"

PIPEDA defines "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character. . ."[238] For example, in one case, an "organization that republished Canadian court and tribunal decisions on its own website was found [by the OPC] to be engaged in commercial activity where: the primary purpose of the website was to use personal information . . .

237 See, for instance, Office of the Privacy Commissioner of Canada, "Mother and daughter were videotaped during covert surveillance of another individual," PIPEDA Case Summary #2009-007 (8 June 2009) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-007/>. In this case, an insurance company engaged in covert video surveillance of a woman due to a legal dispute and, in the process, also conducted surveillance of her sister and niece. Neither of these people were involved in the dispute and the data was collected without their knowledge or consent. This act of collection was found to violate PIPEDA, for lack of consent and failing to limit collection of data.

238 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 2(1).

for the purpose of generating revenue through its paid removal service,"[239] among other factors. Applying this reasoning to the stalkerware context, such apps may also be considered to be using personal information for the purpose of generating revenue, by charging operators for ongoing access to the personal information of a targeted individual.

The definition of commercial activities excludes the actions of private individuals from the scope of PIPEDA. The *Act* thus would not apply to the individual operators who buy and use stalkerware (i.e., the customers of stalkerware companies), but the *Act* would apply to the companies themselves. Stalkerware developers and vendors derive revenue from trafficking in the personal information of targeted persons, by enabling operators to monitor and track targeted individuals through their personal devices. The operators have paid stalkerware companies for software that collects identifying personal data and discloses such data to the operators. Payment for digital spying and cyberstalking capabilities is these organizations' business model. This brings the sale of stalkerware products and services within the scope of commercial activity under PIPEDA.

c) Do Stalkerware Companies "Collect, Use, or Disclose" Targeted Persons' Data?

Having established that targets' data would likely be considered personal information, and that stalkerware companies engage in commercial activities, only one element remains in determining whether PIPEDA applies to stalkerware companies: do the companies in fact collect, use, or disclose targets' data, or is it only the operator who does so, using the respective companies' spyware?

Primary findings from Citizen Lab researchers indicate that the companies collect targeted persons' data on an ongoing basis and subsequently disclose it to stalkerware operators (i.e., their customers). Of the list of stalkerware applications investigated (set out in the Introduction), each company routed data from targeted devices through its own servers before making the data available to the operator. For clarity, the companies collect targets' data on a technological level; they do not just provide the operator with a way of exfiltrating data from the target's device without relying on a stalkerware company's infrastructure. Additionally, the stalkerware companies studied in this report typically disclose the collected data to an operator

239 PIPEDA Interpretation Bulletin, "Commercial Activity," <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/ >.

through purpose-built dashboards or portals, which are maintained and provided by each company as a way for their customers to access the personal information, data, and logs collected from the targeted individuals' devices.

Furthermore, many stalkerware companies, including those that the Citizen Lab researched, run their respective business models on a monthly or annual subscription fee basis.[240] Stalkerware is functionally a service that the company provides for as long as the operator pays the monthly fee. The company's direct and ongoing involvement in collecting targets' personal information and disclosing that data to operators through platforms they control or develop constitutes an integral aspect of the stalkerware service and business model.

d) Are Stalkerware Companies Accountable under PIPEDA?

According to section 4.1.3 of Schedule 1 of PIPEDA, "[a]n organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing." The summation of stalkerware applications' functionalities, as described in Section B of the Introduction to this report, suggests that targets' personal information comes into and remains in the "possession or custody" of these app companies. As such, these businesses are responsible for this data, which is exfiltrated from targeted individuals' devices, and for their own customers' (i.e., the stalkerware operators') personal information.

What appears to be the situation in many cases of stalkerware, including the apps that Citizen Lab studied, is that data is routed through the app developer's servers. Given this finding, the app developer may be considered accountable as the data remains in their "possession and custody" by virtue of this routing through the company's infrastructure.

Alternatively, suppose that a stalkerware developer designed their app so that an operator could use it to monitor and exfiltrate data from the targeted individual's device, but the developer could not access any of the target's data. In this scenario, the application would exfiltrate data from the targeted person's device directly to the operator's device without going through the app company's servers or other infrastructure. In this case, it may be more challenging to consider the stalkerware developer or vendor accountable under PIPEDA, due to the lack of direct involvement in collecting and processing the targeted person's data.

240 See, e.g., FlexiSPY, "FlexiSPY is available for mobiles, computers, and tablets," (accessed online April 2019): <https://www.flexispy.com/en/buy-flexispy.htm>; Mobistealth, Pricing options (accessed online April 2019): <https://www.mobistealth.com/products.php>; Hoverwatch, Pricing options (accessed online): <https://www.hoverwatch.com/pricing>; and TheTruthSpy, "Packages & Prices" (accessed online April 2019): <http://thetruthspy.com/the-best-free-spyware/>.

If a privacy commissioner or a court finds that a greater nexus is required between app developers and vendors and the collection and disclosure activities of their stalkerware apps, then a situation where spyware discloses the targeted person's information to an operator without involving the spyware company or its infrastructure after point of sale may constitute a significant loophole in PIPEDA, so far as remedying privacy harms from stalkerware is concerned. Should such a loophole exist, then a stalkerware company would not be responsible for complying with the *Act*, with respect to the targeted person's personal information.

We argue, however, that the app developer still controls the design of the stalkerware app and its functions, and thus bears responsibility for those who use the app the way it is designed to be used. This accountability rests on developers, in particular, because they may alter the functions and features of the application at any time, including by pushing new updates to devices that have had their software installed. However, it is unclear whether this form of the developer's control and choice over their own app's design and technical features necessarily suffices to meet the criteria for accountability under PIPEDA. Thus, further guidance concerning spyware app companies' accountability for facilitating the surreptitious or otherwise illicit collection and processing of personal information may be required.

Establishing liability may also depend on the type of stalkerware involved. For example, spyware designed and expressly advertised for activities associated with intimate partner violence, abuse, and harassment (what we termed "intimate partner spyware" in **Information Box 2: Classification of Stalkerware Technology**) would have a high likelihood of violating PIPEDA on its face, by virtue of lacking an "appropriate purpose" under section 5(3) of the *Act*.

By contrast, ostensibly "legitimate" child and employee monitoring spyware (dual-use spyware) is purportedly designed and can be used for the purpose of either open monitoring for reasonable parental or employer purposes, or covert or coerced surveillance of individuals such as intimate partners, by the operator. The degree of sensitivity in the personal information collected in tandem with the potentially surreptitious nature of surveillance overtly engages data protection law, including the principle that collecting, using, or disclosing more sensitive personal data warrants a higher degree of scrutiny. Dual-use spyware vendors and developers, even in the context of child and employee monitoring, thus require a higher standard of scrutiny be applied to them, relative to those who engage in commercial activities that do not involve collecting, using, or disclosing intimate personal information. Given that these kinds of spyware can also be repurposed to

constitute stalkerware, we argue that dual-use spyware applications are particularly in need of intense scrutiny.

The final category of stalkerware, as we defined in the Introduction, includes other, narrower technologies, such as find-my-phone apps that have been repurposed for illicit surveillance. Such technologies are subject to the same obligations and same degree of accountability for user privacy and data protection as spyware apps. However, as such technologies are not clearly designed to monitor and track other people in the manner of spyware, more connecting factors may be required in a given case to establish a nexus between the app developer or vendor and an operator's abusive practices, to an extent giving rise to legal responsibility. For instance, one such required factor might entail demonstrating that the app developer failed to take remediating action while also having specific knowledge that an operator was using their spyware app to engage in ongoing abuse with respect to a specific individual.

Much of the analysis in this part of the report contemplates stalkerware as spyware that is designed and deployed to monitor, covertly or without consent, intimate or former partners or to surveil children or employees. The analysis is thus less focused on repurposed phone features or repurposed non-spyware apps such as GPS, anti-theft, or find-my-phone types of applications.

ii. Exceptions that May Remove Stalkerware Companies from PIPEDA's Ambit

There are at least three possible lines of reasoning by which PIPEDA may be found not to apply to a stalkerware business in cases where a private individual deploys the developer's or vendor's spyware on another individual. This subsection discusses each argument and the challenges it poses to holding stalkerware companies accountable under PIPEDA. It also sets out why PIPEDA ought to apply and provides recommendations to close these potential regulatory gaps.

a) "Personal or Domestic Purpose"

The first reason that PIPEDA may not apply to a stalkerware business is based on an analysis of section 4(2)(b) of PIPEDA. Section 4(2)(b) excludes from the *Act* "any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose."[241] This provision prevents PIPEDA from being applied to

241 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 4(2)(b); equivalent provisions appear in the *Personal Information Protection Act*, S.B.C. 2003, c. 63, s. 3(2)(a),

individual persons acting in a private capacity, as opposed to organizations or, for instance, sole proprietors.[242] Thus, pursuing legal action against a stalkerware operator who is acting in the capacity of a private individual would likely require civil litigation or criminal prosecution, as set out in Part 1.

Some case law around the scope of PIPEDA's application, however, suggests that stalkerware companies might also fall outside PIPEDA's purview if their services are used by an individual "for personal or domestic purposes;" this case law and its deriving legal theory rests on the principle of agency.[243] According to this theory, the stalkerware company is acting as the *agent* of the stalkerware operator when the stalkerware app collects and discloses the target's data. Following this reasoning, it is the stalkerware operator who is engaged in monitoring and tracking the targeted person, and they are doing so for a "personal or domestic" purpose—i.e., using the technology to intimidate, harass, or abuse an individual for non-commercial purposes and outside the course of commercial activities.

Several factors suggest that the agency argument may be an inappropriate argument to apply in the stalkerware context. First, all of the cases that have relied on this principle involved third-party investigative companies that had been hired by one party in a formal legal dispute to uncover information about the other party, for the purpose of marshalling evidence for the lawsuit. In each of these cases, the court considered this kind of legal dispute to be a "personal" purpose, which extended to cover the third-party investigators who were considered to be acting on behalf of the individual plaintiff or defendant. PIPEDA thus did not apply to the investigative companies' activities with respect to the targeted person whose personal information was collected, used, or disclosed without consent. However, PIPEDA accounts for some kinds of legal dispute-related investigations under section 7(1)(b),[244] which suggests that allowing section 4(2)(b) to cover organizations would

and *Personal Information Protection Act*, S.A., 2003, c. P-6.5, s. 4(3)(a).

242 For clarity, 'individual person' in this case does not refer to organizations or individuals who are operating as businesses (such as sole proprietors or freelancers), but individuals operating in their capacity as private figures.

243 *Ferenczy v. MCI Medical Clinics*, [2004] O.J. No. 1775 at para. 30 (S.C.J.); *State Farm Mutual Automobile Insurance Co. v. Canada (Privacy Commissioner)*, 2010 FC 736 at para. 106; Financial Services Commission of Ontario (Arbitration Decision), *Borowski v. Aviva Canada Inc.*, FSCO A07-002593 at paras. 38-41. See also Office of the Privacy Commissioner of Canada, "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act* by Elizabeth Denham Assistant Privacy Commissioner of Canada," PIPEDA Report of Findings #2009-008 (16 July 2009) at paras. 310-11.

244 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 7(1)(b): "For the

be redundant and—particularly in the case of organizations handling personal data while engaged in commercial activities—would misconstrue what Parliament intended when it included this subsection in the *Act*.

The Alberta Information and Privacy Commissioner has suggested that PIPEDA's section 4(2)(b) may be superfluous in legal investigation contexts, basing this reasoning on equivalent provisions in the Alberta *Personal Information Protection Act* (PIPA, or AB PIPA).[245] An organization that collects personal information without knowledge or consent, if "reasonable for the purposes of an investigation or a legal proceeding" (AB PIPA), or "reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province" (PIPEDA), already does not require consent to carry out their activities. PIPEDA specifically articulates, in section 7, all exemptions under which an organization can collect or disclose personal information in the course of commercial activities without first obtaining knowledge or consent. The implication is that organizations that commercially collect, use, or disclose personal information without consent and under circumstances *not* specifically exempted remaining accountable under PIPEDA, even if the organizations collected, used, or disclosed the data "on behalf of" an individual who hired the organization for their own personal purpose. For clarity: there are no express exemptions in PIPEDA that specifically exclude stalkerware vendors from being obligated to comply with the *Act*.

Important public policy considerations and PIPEDA's overarching objective militate toward interpreting section 4(2)(b) to apply only to individuals who act for a "personal or domestic" purpose and not to organizations acting commercially in circumstances where they are retained as a business to help achieve a client's personal or domestic purpose. The Alberta Information and Privacy Commissioner

purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if … it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province[.]"

245 Alberta Office of the Information and Privacy Commissioner, "Re Engel Brubaker," Order P2008-010 (30 September 2010) at para. 104 ("While it is true that, in Alberta, a similar conclusion can be achieved if section 4(3)(a) [AB PIPA's equivalent of PIPEDSA's section 4(2)(b)] is read as though it embraces organizations acting on behalf of individuals for personal or domestic capacities, it is not necessary to take this view to achieve the desirable result in policy because the legislation deals specifically with the handling of information for legal proceedings. Indeed, it is arguable that by including the provisions relating to investigations and legal proceedings [AB PIPA section 14(c.3)(d), with equivalent in PIPEDA section 7(1)(b)], by implication, the legislature did not regard law firms or investigators acting on behalf of individuals in civil or criminal proceedings as acting outside the scope of the Act.").

noted in *Re Engel Brubaker*, while applying section 4(3)(a) of Alberta's PIPA (the equivalent to PIPEDA's section 4(2)(b)):

> [R]eading section 4(3)(a) in this way [to exempt commercial activity conducted "on behalf of" paying individuals pursuing a "personal or domestic" purpose] would result in the position that not only organizations that act for the purpose of legal proceedings and related investigations would have no responsibilities under the legislation; the same would be true of any organizations that act on behalf of an individual for a personal or domestic purpose, This would be a significant result and one which, had the legislature intended it, might have been expressed specifically, rather than by way of the somewhat ambiguously-worded section 4(3)(a).[246]

Moreover, interpreting section 4(2)(b) to exempt the commercial activities of organizations retained by private individuals for their own personal purposes would exculpate entire businesses and sectors that set themselves up specifically, or ostensibly, to serve private individuals for a variety of personal purposes. For example, consumer-market DNA analysis businesses, such as 23andMe, collect and store potentially sensitive health data. Their use and management of this personal information is not, or ought not to be, exempt from PIPEDA simply because customers pay the company for DNA tests only for the personal or domestic purpose of discovering more about their own genetic information.

The specific wording in the term "personal or domestic purposes" makes it especially troubling to apply section 4(2)(b) of PIPEDA to exempt stalkerware companies from accountability where their services are used to perpetrate intimate partner abuse or gender-based violence. In the context of family law and gender equality issues more broadly, in both Canada and other jurisdictions, intimate partner violence has historically been hidden or downplayed as a "family matter" or merely constituting "domestic" problems within the private home, in contrast to being recognized as a serious and important public policy issue. Balos writes:

> One of the most powerful societal values that has reinforced the vulnerability of women to domestic violence has been the concept of the private, domestic sphere. Physical abuse of a wife by her husband was deemed a private matter and therefore not appropriate for state intervention. The privileging of privacy connected with the home resulted in a history of judicial decisions that refused to recognize the harm suffered by a victim of domestic violence and therefore a refusal to recognize a legal remedy.[247]

246 *Ibid* at para. 105.

247 Beverly Balos, "A Man's Home Is His Castle: How the Law Shelters Domestic Violence and Sexual Harassment," (2004) 23 *St Louis U Pub L Rev* 77 at p. 87. See also, in the Australian context, Bridget A Harris and Delanie Woodlock, "Digital Coercive Control: Insights From Two Landmark Domestic Violence Studies" (2019) 59:3 *British J of Criminology* 530 at 535 ("Undoubtedly, the constructs of privacy 'permit, encourage, and reinforce violence against women'. Legislation and policy was, traditionally, limited or lacking, which signalled government reluctance to intervene

Should section 4(2)(b) be interpreted to shield the commercial activities of stalkerware companies because they are harnessed in pursuit of a "personal or domestic" purpose by an abusive operator, the law would, in these instances, be returning intimate partner violence and gender-based abuse to the "personal or domestic" sphere. Such a shift would be contrary to decades of legal and societal progress, research, and advocacy pulling this issue into the open and to hard-won recognition of intimate partner violence and gender-based abuse as a systemic socio-political problem that requires collective and systemic responses.

b) Implied Consent of Third Parties

An operator's use of stalkerware implicates third parties' privacy rights and personal information, in addition to those of the targeted person. The target person's friends, family, colleagues, and others are subjected to similar monitoring and tracking—albeit to a lesser extent—by the stalkerware operator, insofar as their information is captured in the targeted persons' message histories and other exfiltrated logs. In some cases, however, the OPC has determined that a company is not responsible for obtaining direct consent from third parties prior to collecting, using, or disclosing their information, if such information is obtained by the company in question as a result of a private individual using the company's services.

For example, in 2009, the OPC determined that Facebook was not responsible for obtaining consent from non-Facebook users before allowing Facebook users to tag these non-users in photos on the website. In this decision, the OPC stated:

> For situations where one party collects from a second party the personal information of a third, our Office has determined in previous cases that, depending on the circumstances, it may be deemed incumbent on the second party (in this case, the Facebook user) to directly obtain the consent from the third (in this case, the non-user). We have also determined in such cases that the first party (in this case, Facebook), though not responsible for directly obtaining consent, must nevertheless take reasonable measures to ensure that consent is obtained by the second party. In other words, the first party must exercise due diligence to ensure that the requirement for consent is met.[248]

in 'domestic' matters. … The 'veil of privacy' that shrouded 'the domestic' sphere was, Fineman asserts, lifted by second-wave feminist reviews of the family and family law. The tireless work of activists, advocates and academics has contributed to greater recognition of associated harm and risk and the framing of DV [domestic violence] as a 'public' problem") (internal citations omitted).

248 Office of the Privacy Commissioner of Canada, "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act* by Elizabeth Denham Assistant Privacy Commissioner of Canada," PIPEDA Report of Findings #2009-008 (16 July 2009) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-business-es/2009/pipeda-2009-008/> at para. 312.

However, this application of PIPEDA would be unworkable in the stalkerware context, because the second party (the targeted person) cannot realistically obtain consent from their contacts to share their personal information with the operator and the stalkerware company—nor should the targeted person be expected to be able to. The targeted person may be unaware that the spying is occurring or they may be prevented from revealing the operator's activities to their friends and family, either due to explicit coercion or because they are ashamed or afraid of harm or retribution if they disclose the abuse. Even if the targeted person did attempt to obtain consent, the consent or its refusal would be meaningless because the targeted person lacks control over the stalkerware and its operations. Moreover, it is also possible that disclosing the monitoring could cause others in the targeted person's life to withdraw from interacting with them electronically, thus leading to further isolation and vulnerability.

Given the realities of stalkerware, the targeted person is not the second party as the Facebook user is; the targeted person is the third party. Their friends and family are fourth parties, and it is the operator who is the second party. According to the argument of implied consent of third parties, the onus would thus lie upon the operator to obtain consent from the targeted individual and their contacts. In this case, the stalkerware company would still be obligated to ensure that the operator was in compliance with the law.

In fact, a joint investigation by the OPC and Office of the Information and Privacy Commissioner for British Columbia (OIPC BC) determined in April 2019 that Facebook had violated PIPEDA by not obtaining adequate consent from the "friends" of users who had installed a certain app. This app, used by Cambridge Analytica to conduct psychographic modelling on users for political strategizing, collected those friends' personal information despite the friends not having themselves installed the app.[249] Specifically, the OPC and OIPC BC stated (referring to friends of installing users as "Affected Users"):

> *The onus was on Facebook to ensure that adequate information was made available to support knowledge and consent for its disclosures* [of Affected Users' personal information to the app]. In our view, they did not do so with respect to disclosure of Affected Users' information to the TYDL App, or more generally, to the apps installed by their friends.
>
> Furthermore, where personal information is sensitive and collected, used, or

249 See generally Office of the Privacy Commissioner of Canada, "Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia," PIPEDA Report of Findings #2019-002 (25 April 2019) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/>.

> disclosed *in a way that is outside the user's expectations, express consent is required.* [. . .] In this context, we are of the view that *Facebook should have obtained express consent on an app-by-app basis* before disclosure of any personal information that an Affected User had restricted to "friends" only.
>
> Facebook also claims it had consent to disclose Affected Users' personal information to the TYDL App by virtue of the Installing User's decision to install the app. In our view, *it is unreasonable for Facebook to rely on consent from the Installing User in this context.* In particular, we note that each Installing User could have hundreds of friends, none of whom would have had any knowledge of the disclosure of their personal information to the TYDL App, let alone the purposes for that disclosure.[250]

This OPC and OIPC BC decision would seem to close to the door on a stalkerware company's ability to rely on their customer, the stalkerware operator, to obtain meaningful consent from the targeted person. Even if there are not "hundreds of friends" or dozens of apps involved, where stalkerware is deployed in the context of intimate violence, abuse, and harassment, the targeted individual similarly has "no way of truly knowing what personal information would be disclosed to which app and for what purposes,"[251] or even the fact that personal information is being disclosed. Based on the analysis in the OPC and OIPC BC joint investigation, PIPEDA should require stalkerware companies to obtain direct and express consent from targeted individuals, and the companies cannot redirect this duty to their customers.

In the event that implied consent of third parties were found to apply to the stalkerware context, the stalkerware company must in all cases "nevertheless take reasonable measures to ensure that consent is obtained by the second party"[252]—in this case, the operator. The stalkerware company thus remains accountable to the extent that it must ensure its customers have obtained meaningful consent from targeted persons, even if the company does not bear legal responsibility for directly obtaining consent from those targeted persons before collecting, using, or disclosing their personal information. For absolute clarity, however, the OPC and its provincial counterparts should consider issuing an Interpretation Bulletin or statement that affirms that stalkerware companies *may not* rely on operators to obtain meaningful consent from targeted persons, to fulfill the meaningful consent requirement of PIPEDA.

c) Delegating PIPEDA Compliance through Terms of Use and License Agreements

The OPC permits businesses to meet their PIPEDA obligations associated with transferring data to other parties by including compliance and safeguard provisions

250 *Ibid*. at paras. 108-111 (emphasis added).

251 *Ibid*. at para. 102.

252 *Ibid*.

in contract agreements with those other parties.[253] As such, a stalkerware company might assert that they have complied with PIPEDA by including clauses regarding legal use and demanding operators obtain targeted persons' consent, in their privacy policies, terms of service (ToS), end user license agreements (EULAs), or other public-facing policy documents that customers purportedly agree to adhere to in purchasing a stalkerware app.[254]

To demonstrate how this argument might apply to stalkerware, consider an OPC decision that involved a daycare centre that had set up a live webcam feed, which let parents watch their children at the daycare after inputting unique passwords they were assigned to access the feed. One parent launched a complaint upon learning that the daycare was recording and storing the webcam feed, and doing so without appropriate safeguards. Responding to the OPC investigation, the daycare "required parents using the webcam service to sign a contract agreeing to not record the webcam feed" and to promise they would "keep the assigned password confidential." In resolving the complaint, the OPC permitted the daycare to continue its webcam monitoring service despite lacking "technological safeguards to prevent a parent from recording the video viewed on the webcam and sharing it." The OPC allowed the continuation of the webcam monitoring service even though the daycare stated that it was "not aware of any mechanism by which it can determine on a timely basis whether the contract has been breached, and in particular, whether the live stream has been recorded in violation of the contract."[255] Analogously, a stalkerware business could claim that requiring their customers to adhere to the company's ToS or EULA—"promising" not to install the software onto another individual's phone without explicit consent or to otherwise use the app

253 See, e.g., in the context of using cloud providers, "[i]n short, SMEs must use contractual or other means to ensure that personal information is appropriately handled and protected by the cloud provider:" Office of the Privacy Commissioner of Canada, "Cloud Computing for Small and Medium-sized Enterprises," (14 June 2012) <https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/gd_cc_201206/>; see also Office of the Privacy Commissioner of Canada, "PIPEDA Interpretation Bulletin: Accountability," PIPEDA Information Bulletin (17 April 2012) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02_acc/>.

254 See, e.g., FlexiSPY, "Legal Disclaimer," (2015) <https://www.flexispy.com/en/legal-disclaimer.htm> (accessed 1 March 2019); TheTruthSpy, "Terms of Use / Legal," (9 January 2015) <thetruthspy.com/terms-of-use/> (Accessed 1 March 2019); mSpy, "MSPY END USER LICENSE AGREEMENT," (25 May 2018) <https://www.mspy.com/legal-info.html> (Accessed 1 March 2019); Hoverwatch, "Terms of Service," (21 May 2013) <https://www.hoverwatch.com/terms-of-service> (Accessed 1 March 2019); and Highster Mobile, "Terms & Conditions" (17 May 2018) <https://highstermobile.com/terms/>.

255 Office of the Privacy Commissioner of Canada, "Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection," PIPEDA Report of Findings #2011-008 (5 June 2012) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-008/> at paras. 15-16.

for illegal activities—suffices to fulfil the developer's and/or vendor's obligations under PIPEDA.

However, several factors distinguish the situation where an operator uses spyware abusively from that of the daycare's webcam feed. In the case of the webcam feed, the OPC required the daycare to implement several recommendations to bring it into compliance with its PIPEDA obligations.[256] At the least, it would seem that stalkerware developers and vendors would also have to implement measures to ensure their compliance with PIPEDA. Such measures for stalkerware businesses would include, at a minimum:

- ensuring encrypted connections between the site of data collection and the site of accessing and viewing the data;
- regularly reviewing system logs for abusive uses of their spyware technology;
- ensuring that all monitored individuals are fully informed of the monitoring activity and associated risks; and
- terminating the accounts of customers (operators) found to be using the companies' surveillance apps abusively.

Most importantly, the OPC noted as part of its decision that the daycare required consent to engage in webcam monitoring as a condition of enrollment in the centre. Further, "[b]ecause individuals would appear to have alternative child care options available that do not utilize live video streaming, there is no evidence that parental consent is not freely and voluntarily provided."[257] The daycare required informed consent from the parents whose children would be monitored; by definition, the daycare could only monitor children whose parents or guardians had freely and voluntarily given meaningful, informed consent beforehand;[258] without that

256 Office of the Privacy Commissioner of Canada, "Accountability," PIPEDA Interpretation Bulletin (17 April 2012) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02_acc/>.

257 Office of the Privacy Commissioner of Canada, "Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection," PIPEDA Report of Findings #2011-008 (5 June 2012) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-008/> at paras. 34, 35, 41-42, and 50-51.

258 While beyond the scope of this report, it may be worth noting that parental consent to daycare monitoring may not be as "freely and voluntarily" given as the OPC decision suggests, given the documented scarcity of available and affordable daycare spaces throughout Canada, in what has been referred to as a national "childcare crisis." See, e.g., "Child care crisis in Ontario: How to fix it?," *Global News* (13 April 2017) <https://globalnews.ca/video/3377473/chid-care-crisis-in-ontario-how-to-fix-it>; "Short notice of daycare closure leaves parents in limbo, highlights child-

prior consent, the children could not attend the daycare and thus be exposed to the webcam. Meaningful, informed, and freely and voluntarily given consent in the context of stalkerware applications is precisely what may be missing or be questionable in its validity, if the application in question is used in the context of intimate partner abuse or gender-based violence.

The emphasis on meaningful consent in determining whether activities are legal under PIPEDA was highlighted in PIPEDA Report of Findings #2017-002, *Canadian adware developer Wajam Internet Technologies Inc. breaches multiple provisions of PIPEDA*. In this case, Wajam installed advertising software onto users' computers via intermediary distributors. The software was "designed to track the individual's online search queries and to overlay, onto existing search engine results, search results derived from content shared by an individual's 'friends' and others known to the individual on social media."[259] The OPC determined that Wajam's activities violated multiple principles under PIPEDA, including failing to obtain meaningful, informed, express consent; preventing withdrawal of consent; failing to identify the purpose of data collection at or before time of collection; unclear data retention policies and practices; storing "raw user information in unencrypted form;" and transmitting user data without encryption.[260]

Notably, the OPC did not find that Wajam had met its PIPEDA obligations even though the company attempted to bind its distributors to compliance through explicit provisions in their contract agreements. The OPC found that Wajam violated its consent obligations under PIPEDA because its efforts to enforce distributors' compliance with privacy obligations were inadequate, given Wajam's knowledge of distributors' violations of agreement provisions, and given the company's failure to obtain meaningful consent from users.[261]

---

care crisis in Toronto," *CBC News* (26 June 2018) <https://www.cbc.ca/news/canada/toronto/humberside-daycare-closing-childcare-crisis-1.4723855>; Joshua Ostroff, "It's Time To Rip The Band-Aid Off Canada's Daycare Crisis," *Huffington Post* (27 April 2017) <https://www.huffington-post.ca/joshua-ostroff/justin-trudeau-parental-leave_b_9778552.html>; David MacDonald and Thea Klinger, "They Go Up So Fast: 2015 Child Care Fees in Canadian Cities," *Canadian Centre for Policy Alternatives* (December 2015) <https://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2015/12/They_Go_Up_So_Fast_2015_Child_Care_Fees_in_Canadian_Cities.pdf>; Iglika Ivanova, "Solving BC's Affordability Crisis in Child Care," *Canadian Centre for Policy Alternatives* (July 2015) <https://www.policyalternatives.ca/sites/default/files/uploads/publications/BC%20Office/2015/07/ccpa-bc-solving-childcare-summary_0.pdf>.

259 Office of the Privacy Commissioner of Canada, "Canadian adware developer Wajam Internet Technologies Inc. breaches multiple provisions of PIPEDA," PIPEDA Report of Findings #2017-002 (17 August 2017) at para. 2.

260 *Ibid*.

261 *Ibid* at paras. 8, 145, and 147.

In another decision involving reliance on contractual agreements, the OPC and OIPC BC's joint investigation into Facebook determined that its contractual measures to protect users' personal information, as well as its monitoring and enforcement measures, "did not represent adequate safeguards."[262] During the investigation, Facebook claimed that it had implemented a number of safeguards of users' personal information.[263] In analyzing these measures, the OPC and OIPC BC found the following:

> Facebook relied on contractual terms with apps to protect against unauthorized access to users' information, but then put in place superficial, largely reactive, and thus ineffective, monitoring to ensure compliance with those terms. Furthermore, Facebook was unable to provide evidence of enforcement actions taken in relation to privacy related contraventions of those contractual requirements.[264]

The OPC and OIPC BC found it a particular failure on Facebook's part, in respecting users' personal information, that the company declined to "pursue a proper review of the TYDL app in the face of such obvious red flags," which the TYDL app raised in a request for extended permissions to user data.[265] Sufficient evidence had presented itself to put Facebook on notice that the app developer may have been abusing their privileges on the platform, yet Facebook did not take the "next logical step" of investigating the app to ensure compliance, thus falling into contravention of PIPEDA. This reasoning would also apply to the stalkerware context, where stalkerware companies have evidence of potential abuse in the form of customer support requests for assistance in engaging in intimate partner surveillance, public reviews of their apps used or attempted to be used for such purposes, and media coverage of their software used for intimate partner violence, abuse, and harassment.

---

262 Office of the Privacy Commissioner of Canada, "Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia," PIPEDA Report of Findings #2019-002 (25 April 2019) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/> at para. 146.

263 These safeguards included: requiring app developers to agree and adhere to Facebook's Platform Policy, which contained provisions regarding explicit consent for new purposes, restrictions on the use of users' friends' data, and enforcement; using automated tools to detect some types of violations; conducting manual reviews of popular and other select apps for compliance; and relying on user reports, media stories, and employee tips. Facebook also stated that it conducted an app review process after transitioning to a more restricted application programming interface (API) for third-party app developers to use. After learning the TYDL App's developer had transferred personal information to third parties in violation of the Platform Policy, Facebook "took action to ensure that the data was deleted" and removed the app from its platform—without, however, notifying either Affected Users or users who had installed the app. *Ibid*. at para. 137.

264 *Ibid*. at "Overview."

265 *Ibid*. at paras. 148-153.

The decisions regarding Wajam and Facebook together suggest that stalkerware companies would be unable to escape liability by pointing to clauses, statements, or terms in standardized non-negotiated agreements that in effect merely inform users that the purchased software should only be used legally and with the knowledge and consent of those tracked. Moreover, despite such disclaimers commonly appearing among the ToS or EULAs of stalkerware apps, "examples of conflicting or contradicting messages between the content of disclaimers and marketing claims are numerous," such that while stalkerware companies' disclaimers admonish against illegal or abusive uses, the same companies' marketing language sometimes seems to encourage precisely such uses, or appeal to them to drive sales.[266] At minimum, stalkerware companies would have to not only stop appealing to such uses in any form of marketing, but more rigorously discourage and prevent such uses, including implementing proactive monitoring and enforcement regimes to ensure their customers' compliance with the companies' contractual provisions and with privacy and data protection laws. Notably, purely reactive measures would be insufficient to comply with PIPEDA, as the joint investigation into Facebook established.

d) Need for Regulatory or Legislative Reform

The analysis in this section demonstrated that under current law, there are three possible routes that stalkerware companies may take to assert that their activities are either exempt or beyond the scope of PIPEDA, or that they are compliant with the Act. It is true that, in light of the distinguishing factors and public policy considerations also discussed above, this may not turn out to be the case in the event a privacy complaint is launched against one of these companies or they are brought before the courts.

For absolute clarity, however, the Office of the Privacy Commissioner of Canada, and its provincial counterparts, should issue an interpretation bulletin or additional accompanying statement, addressing stalkerware, to the *Guidelines for obtaining meaningful consent* or *Guidance on inappropriate data practices*. This bulletin or statement should specifically address the use of stalkerware in abusive contexts, such as intimate partner abuse or gender-based harassment. Additionally, Parliament may consider amending consumer data protection legislation to close these loopholes, by drafting new provisions to address stalkerware-facilitated privacy violations specifically.

266 As only one example among many, "'Highster' advises against non-consensual installation of the software. Elsewhere on their website, however, 'Highster' makes claims that it can support non-consensual, unilateral, and surreptitious installation (see Figure 12) while also stating that 'it is difficult to get caught while using this software' (Highster, 2019).": Diarmaid Harkin, Adam Molnar & Erica Vowles, "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry" (2019) *Crime Media Culture* 1 at 18.

Stalkerware-facilitated abuse is a privacy and data protection matter, and such abuse is systematically made possible through the commercial activities of stalkerware vendors and developers. However, without the additional clarifications described in the previous paragraph, PIPEDA risks being of limited use in providing remedy to targeted individuals or upholding companies' compliance with Canada's data protection laws.

iii. Privacy Rights and Obligations under PIPEDA

PIPEDA protects a slate of privacy and data protection rights in the context of commercial entities collecting, using, and disclosing the personal data of customers and other individuals.[267] Stalkerware implicates three major principles in particular. First, a business must obtain meaningful and valid consent from the individual whose personal data is concerned. Second, the collection, use, or disclosure of personal data must be for a reasonable or appropriate purpose, and that purpose must be explained to the individual when or before they consent to providing their personal data. Third, a business that uses, collects, stores, or discloses personal data must implement adequate safeguards to ensure that the personal data is secured from exposure or unauthorized access. The following subsections will discuss each of these rights—and the corresponding obligations for businesses—in turn and apply them to the stalkerware context specifically.

a) Meaningful Consent

The ability to give, refuse, and withdraw consent is a core right that PIPEDA protects with respect to individuals' personal information.[268] The PIPEDA guidance page on consent clearly establishes the critical notion that organizations must obtain informed consent from "*the individual whose personal information is collected, used or disclosed*."[269] This wording ensures that consent and knowledge are tied to the

267 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1, "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information" [PIPEDA Schedule 1]. These are colloquially referred to as the "Fair Information Principles," and provide the central foundation of rights and obligations under PIPEDA, as demonstrated throughout OPC decisions and reports.

268 See generally PIPEDA Schedule 1, section 4.3 ("Principle 3 - Consent"); Office of the Privacy Commissioner of Canada, "Form of Consent" PIPEDA Interpretation Bulletin (11 December 2015) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_07_consent/>; and Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent" (24 May 2018) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

269 Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principle 3 – Consent," (8 January 2018) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-per-

individual whose personal information is implicated and, as a result, does not allow for confusion or loopholes dependent on who is considered, for instance, the "user" of an app. Stating that consent must be obtained from the person whose personal data is collected, used, or disclosed also prevents obfuscation of obligations that might follow from questions of who is the *true* user based on relationship with the stalkerware app company. Explicitly requiring consent from the person being tracked avoids the danger that consent is tied to financial control, for instance, where the targeted individual may not be formally tied to their own device (such as if they are in an abusive relationship where the operator legally owns the target's device or is paying for the target's phone plan).

Organizations must fulfill a set of obligations in order to lawfully collect, process, transfer, or disclose someone's personal information. Under section 4.3 of Schedule 1 in PIPEDA, organizations must obtain consent (4.3.1) and the consent must be informed (4.3.2). The form of consent should correspond with the sensitivity of the personal information (4.3.4), and obtaining consent must take into account the individual's reasonable expectations of how the organization would presumably use their information. Consent cannot be obtained through deception (4.3.5). Further, organizations should seek express consent where the information is likely considered sensitive (4.3.6), and individuals should be able to withdraw consent at any time, subject to law, contractual obligations, and reasonable notice (4.3.8).

Stalkerware applications are often surreptitiously installed on a targeted person's mobile device(s), the targeted persons are coerced into having the stalkerware installed, or the operator repurposes an otherwise legitimate or innocuous application on the target's device into a form of stalkerware. These deployment characteristics mean that the software will routinely fall afoul of PIPEDA's consent obligations. Specifically, many stalkerware applications do not seek or obtain consent from the targeted individual (4.3.1), nor are the full implications of such applications made clear to the targeted individual whose personal information is collected and disclosed (4.3.2). Indeed, stalkerware marketing often emphasizes the notion that operators may use the respective companies' products and services without the targeted individuals ever knowing about the applications' presence on

sonal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/> (emphasis added). Similarly, while section 6.1 of PIPEDA speaks more to an individual's capacity to consent and may be more relevant in situations of parent-child monitoring, the language here too specifies that "the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting:" *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 6.1.

their infected devices, let alone such applications' uses and implications for the targeted individual's personal data.[270]

Stalkerware apps regularly collect sensitive or highly sensitive information, such as personal conversations and web-browsing history, without seeking consent (4.3.4). An individual would not reasonably expect that using their phone would result in extensive logging, tracking, and monitoring of their GPS location and all their digital activity across several different applications and platforms, for the systematic compilation and delivery to another private individual who has specifically targeted them for ongoing tracking and surveillance in a personal context.[271] Consent is either not obtained, or is otherwise "obtained" through deception or coercion and thus cannot be considered to have been obtained (4.3.5).[272] Further, stalkerware businesses often do not seek or obtain express or otherwise valid consent from targeted individuals; instead, they entrust this obligation to operators through Terms of Use or EULAs. Individuals cannot withhold or withdraw consent from an activity or arrangement to which they never consented nor were ever alerted to (4.3.8). Moreover, stalkerware businesses' lack of regard for obtaining consent persists regardless of the sensitivity of information collected, processed, or disclosed to operators (4.3.6).

The OPC differentiates between an individual granting an application permission to have the capability to access their personal information and consenting to the application in fact collecting their personal information. In a case involving Google, the OPC established that "the act of granting app permissions does not, by itself, equate to consent for the collection, use or disclosure of associated personal information." The OPC reached this conclusion partly because the purposes of collection, use, or disclosure were not identified at the point of asking for permission.[273] Stalkerware companies thus cannot rely on this step of obtaining

270 Diarmaid Harkin, Adam Molnar & Erica Vowles, "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry" (2019) *Crime Media Culture* 1 at 18.

271 We specify "for delivery to another private individual who has specifically targeted them. . .in a personal context" to differentiate the core activity of stalkerware applications from such tracking and monitoring that online businesses and websites engage in for the purposes of user data analytics and targeted or third-party advertising. See **Information Box 11: Privacy, Consent, and Mobile Apps in the Digital Economy.**

272 Danielle Keats Citron, "Spying Inc.," (2015) 72:3 *Washington and Lee L Rev* 1243 (1 June 2015) <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=4464&context=wlulr> at 1250-51.

273 Office of the Privacy Commissioner of Canada, "Agreement to an app's 'permissions' does not, by itself, equal consent to collect, use and disclose personal information - *Google encouraged to provide users with greater clarity to avoid misperception*," PIPEDA Report of Findings #2014-008 (14 May 2014).

the targeted person's consent—that is, the acceptance of the capacity to access personal information—as a basis to collect the targeted person's data without express consent to that collection. This line of argumentation, however, is likely moot in cases where an operator installs a stalkerware application onto the targeted person's phone without the latter knowing, or where the operator, unbeknownst to the targeted person, repurposes a find-my-phone or otherwise innocuous app that was already installed on the targeted person's mobile device.

PIPEDA contains exceptions that authorize an organization to collect, use, or disclose personal information without knowledge or consent, such as if the collection is "clearly in the interests of the individual and consent cannot be obtained in a timely way" or if ensuring knowledge and seeking consent would compromise an investigation of legal wrongdoing. Consent may also be waived if disclosure is required to comply with a subpoena, warrant, or court order, among other exceptions.[274] These exceptions would not seem to apply to cases where an organization collects a private individual's personal information in order to use it to monitor and track that individual's activities as part of a paid service, and subsequently discloses it to another private individual without the former's knowledge or consent, in the course of the business's commercial activities.[275]

Information Box 13: Guidelines for Obtaining Meaningful Consent

In September 2017, the Office of the Privacy Commissioner of Canada concluded an extensive national consultation on consent in the context of PIPEDA.[276] The consultation resulted in a report to Parliament and two guidance documents: "Guidelines for obtaining meaningful consent" ("Meaningful Consent Guidelines," or "Guidelines") (effective as of January 1, 2019) and "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)" ("Inappropriate Data Practices Guidance") (effective as of July 1, 2018).

The Meaningful Consent Guidelines document sets out seven elements of meaningful consent, discusses key factors relevant to determining appropriate form of consent, and emphasizes additional general considerations for organizations to keep in mind. These guidelines highlight the extent to which stalkerware businesses fail to fulfill core obligations to obtain meaningful consent from the individuals whose personal data they collect, use, and disclose.

274 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 at s. 7(1) (collection), 7(2) (use), and 7(3) (disclosure).

275 To the extent that stalkerware app developers and vendors may be able to argue that they fall under a particular exception that permits them to dispense with consent obligations, see the analysis above in Section C(ii), "Exceptions that May Remove Stalkerware Companies from PIPEDA's Ambit."

276 Office of the Privacy Commissioner of Canada, "Consultation on consent under the *Personal Information Protection and Electronic Documents Act* (updated online 24 May 2018) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/>.

Circumstances involving abusive stalkerware use tend to contravene the seven elements of meaningful consent set out in the Meaningful Consent Guidelines. One of these elements is emphasizing, to the individual whose data is being processed, key aspects of the data collection, use, or disclosure, such as the risk of harm and other consequences. Stalkerware applications typically do not inform the targeted person of the application's existence on the person's device at all, let alone the app's activities and associated risks, harms, or consequences.

Other elements of meaningful consent entail "providing individuals with clear options to say 'yes' or 'no;'" considering the consumer's perspective (such as whether they understand what they are consenting to); and treating consent as "a dynamic and ongoing process" (as opposed to a one-time affair).[277] Stalkerware applications do not normally provide targeted individuals with "just-in-time" alerts or persistent notifications that they are being monitored, tracked, or recorded. These applications also do not necessarily provide targeted individuals with the option to refuse or stop such surveillance if it is discovered. For example, the Citizen Lab found one instance where operators appeared to be given the option to turn on a feature that prevents the device user (i.e., the targeted person) from uninstalling the app.

To determine the appropriate form of consent, the Guidelines stress the importance of considering the sensitivity of the collected, used, or disclosed personal information. The Guidelines also emphasize the need to take into account the individual's reasonable expectations for what will be done with their data or where their data will go: "an individual would not reasonably expect disclosure to individuals who are merely curious or seek the information for nefarious purposes."[278] An organization must implement practices based on risk of harm to the impacted individual. By nature, stalkerware applications under the spyware category operate in a way that necessarily deprioritizes respecting the sensitivity of the target's information and their risk of harm. These applications exfiltrate personal information and sensitive data and deliver it to the stalkerware operator, while also potentially making the data accessible to the app company and rendering the data vulnerable to security risks such as data breaches.

The Guidelines additionally emphasize that individuals have the right to withdraw consent, and that "[c]onsent is not a silver bullet."[279] Specifically, "an individual's consent is not a free pass for organizations to engage in collecting and using personal information indiscriminately for whatever purpose they choose."[280] This position reinforces the centrality of meaningful consent to business activities being compliant under PIPEDA,. It also speaks to broader considerations that question the validity of consent in the context of an operator using stalkerware to target an individual in a violent or abusive situation, as discussed in Part 1. The inability of many targeted individuals to unilaterally uninstall a stalkerware app from their device, or uninstall

277 Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent," (May 2018) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

278 Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent," (May 2018) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

279 *Ibid*.

280 *Ibid*.

> the app without fear of violent repercussions— let alone avoid or be protected from surreptitious surveillance in the first place—hollows out any sense of ongoing consent regardless of whether or not they may have initially consented to having the stalkerware application installed on their device.

b) Appropriate Purpose for Collection, Use, and Disclosure of Personal Information

PIPEDA contains an overriding obligation in section 5(3), which states that "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[281] The OPC's "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)" ("Inappropriate Data Practices Guidance") describes this provision as "a critical gateway that either allows or prohibits organizations to collect, use and disclose personal information, depending on their purposes for doing so. It is the legal boundary that protects individuals from the inappropriate data practices of companies."[282] If an organization fails to pass muster under section 5(3) and it collects or processes information for an inappropriate purpose, it does not matter if the organization meets any other of PIPEDA's obligations, such as obtaining consent, limiting collection, implementing safeguards, or ensuring data accuracy.[283]

Evaluating whether an organization's collection, use, or disclosure is appropriate involves a four-part test that Canadian courts have adopted and applied in cases where the appropriateness of an organization's data practices has been in issue.[284] This test assesses whether:

a) the purpose is a legitimate need or *bona fide* business interest;

b) the collected or processed information would effectively meet the organization's need;

c) a less invasive means of achieving that need exists; and

d) the privacy loss is proportional to the benefit gained.[285]

281 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 at s. 5(3).

282 Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subjection 5(3)," (May 2018) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/>.

283 *Ibid*.

284 See, e.g., *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 at paras. 126-129 and 174-182; and *T. (A.) v. Globe24h.com*, 2017 FC 114 at paras. 73-76.

285 *Ibid*.

Where a stalkerware application is purpose-built to enable paying customers to covertly, or without consent, monitor and track the digital activities of those they are in personal relationships with—possibly as part of a broader situation of intimate partner abuse or gender-based violence or harassment—it is difficult to imagine the stalkerware app, and its vendor or developer, would not be considered to violate section 5(3) of PIPEDA. The analysis becomes more complicated where a stalkerware business does not explicitly market its services for such purposes and, instead, brands its software as a child monitoring, employee monitoring, or find-my-phone application, but is nonetheless used by customers to monitor and track targeted individuals without their knowledge or consent. In these cases, the extent of the stalkerware company's obligations and liability may turn on specific facts, such as the level of knowledge that the company possesses regarding such uses and what measures the company has taken, if any, to ensure that its software is not used for harmful or abusive purposes.[286]

The Inappropriate Data Practices Guidance, which the OPC issued alongside the Meaningful Consent Guidelines as a result of its 2017 consent consultation, adds an additional factor to consider: the degree of sensitivity of the personal information at issue. The Guidance also goes beyond the four-part test to establish explicit "No-Go Zones" under section 5(3) of PIPEDA. Such zones constitute practices or activities that the OPC regards would be considered "'inappropriate' by a reasonable person" based on "more than fifteen years of applying PIPEDA, and comments received during [the] consultation on consent."[287]

Stalkerware companies' collection and disclosure of targeted individuals' personal information likely ventures into at least three of the six (at time of writing) No-Go Zones that are established in the Inappropriate Data Practices Guidance. We discuss here the three designated inappropriate purposes and their respective applications to the stalkerware context.

- **Collection, use, or disclosure that is otherwise unlawful:** "Organizations should have knowledge of all regulatory and legislative requirements that may govern their activities, and individuals should be safe in the knowledge that collection, use or disclosure of their personal information will not be

286 For further discussion on this point, see Section 3.2.3 (Delegating PIPEDA Compliance through Terms of Use and License Agreements).

287 Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subjection 5(3)," (May 2018) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/>.

done for purposes that contravene the laws of Canada or its provinces."[288] The use and sale of stalkerware applications constitute or directly enable activities that likely implicate and contravene a range of Canadian laws and regulatory requirements, including privacy laws such as PIPEDA obligations to obtain meaningful consent.

- **Collection, use, or disclosure for purposes that are known or likely to cause significant harm to the individual:** "By 'significant harm', we mean 'bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on (one's) credit record and damage to or loss of property'."[289] Stalkerware applications are often closely tied to intimate partner abuse and violence against women and have been used to stalk, harass, intimidate, and further abuse women who have left situations of intimate partner violence.[290] The only reason a stalkerware company collects and discloses a targeted individual's personal information is by virtue of another person (i.e., the operator) engaging the company and its technology to do so. The company also relies on these customers and positions itself as specifically and exclusively in the business of facilitating personal surveillance. Such collection and disclosure is known, or is likely or ought to be known, to cause significant harm to an individual who has not freely, voluntarily, and meaningfully consented to this collection and disclosure, and yet has their information collected and disclosed.
- **Surveillance by an organization through audio or video functionality of the individual's own device:** "Nothing can be more privacy-invasive than being tracked through the audio or video functionality of an individual's device either covertly, that is without their knowledge or consent, or even with *so-called* consent, when doing so is grossly disproportionate to the business objective sought to be achieved. […] It may be permissible for the audio or video functionality of a device to regularly or constantly be turned on in order to provide a service if the individual is both fully aware and in control of this fact, and the captured information is not recorded, used, disclosed or retained except for the specific purpose of providing the service."[291] Some

288 *Ibid*.

289 *Ibid*.

290 Rachel Williams, "Spyware and smartphones: how abusive men track their partners," *The Guardian* (25 January 2015) <https://www.theguardian.com/lifeandstyle/2015/jan/25/spyware-smartphone-abusive-men-track-partners-domestic-violence>.

291 Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subjection 5(3)," (May 2018) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/> (emphasis in original). See also Office of the Privacy Commissioner of Canada, "Guidelines for Overt Video Surveil-

> of the features included in stalkerware apps involve recording audio and video of the targeted individual through their device. Even in cases where the company might claim that the targeted person's consent has been obtained or where the individual is fully aware (e.g., where their partner had pressured or coerced them into installing the app), the individual still could not be said to have control over such recording, for several reasons. First, the individual may lack technical control if they cannot tell whether their device is actively recording them (due to lack of just-in-time or persistent notifications) and if they cannot prevent the operator from remotely turning on the feature at will, even if the targeted person can turn it off. Second, the individual would not have control over copies of recordings that the stalkerware application exfiltrates from their device and uploads to the company's servers, and also delivers or makes accessible to the stalkerware operator. Third, the individual may not be able to halt the recordings or their collection and disclosure if they occur in the context of an abusive relationship, which may include dynamics of control and manipulation in addition to coercion and fear of harm or retribution for refusing the stalkerware operator's demands.

In addition to requiring an appropriate purpose, those collecting, using, or disclosing personal information must also identify the purpose behind such activities to the individual whose personal information is collected, used, or disclosed.[292] Stalkerware applications run afoul of this requirement by design where they enable and advertise surreptitious monitoring and tracking of a targeted individual's activities and whereabouts. Such violations of PIPEDA are further accentuated where data is collected in order to send that information to someone who may represent a source of harm, harassment, or otherwise unwanted attention to the targeted person. Individuals who have their personal information collected by stalkerware are thus unlikely to be notified either before or at the time of such collection, let alone also be informed of why the application is collecting and disclosing their personal information. Although stalkerware companies may attempt to delegate the requirements to obtain consent and provide notice of use, along with other legal obligations, to operators through Terms of Service or EULAs, these companies retain an obligation to take reasonable measures to ensure that the operators are, in fact, complying with such obligations.[293]

---

lance in the Private Sector," (March 2008) <https://www.priv.gc.ca/en/privacy-topics/surveillance-and-monitoring/gl_vs_080306/>.

292 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1 at s. 4.2.3.

293 For more, see the discussion in Section 3.2.2 Implied Consent of Third Parties.

c) Safeguards

PIPEDA requires organizations to safeguard personal information in their custody and to safeguard the information in ways that are proportionate with the data's degree of sensitivity.[294] Given the type and volume of personal information that is potentially collected and stored about victims whose devices are infected with stalkerware—and setting aside other legal issues around these companies' collection, use, and possession of information—these vendors' obligations under PIPEDA demand that they undertake significant measures to protect the data in their possession so it is not exposed to (additional) unauthorized parties.

There have been multiple cases where vendors selling stalkerware have lost control of the personal data in their possession.[295] In 2017, FlexiSPY experienced a data breach in which a hacker obtained "email addresses of customers, internal company files, a number of emails, and alleged partial credit card information."[296] Another hacker targeted Retina-X in 2016—the company responsible for developing the apps MobileSpy, PhoneSheriff, and SniperSpy—and obtained "customer account logins, alleged GPS locations of surveillance victims, and photos and communications ripped from devices by the malware" and, additionally, erased data from all of the company's servers.[297] In May 2019, yet another data leak occurred, where the spyware company Mobiispy "left more than 95,000 images and more than 25,000 audio recordings on a database exposed and publicly accessible to anyone on the internet," amounting to 16 GB of images, including intimate images, and 3.7 GB of audio recordings.[298]

---

294 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1 at s. 4.7, "Principle 7 – Safeguards;" and Office of the Privacy Commissioner of Canada, "Safeguards," PIPEDA Interpretation Bulletin (10 June 2015) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_08_sg/>.

295 See, e.g., Joseph Cox & Lorenzo Franceschi-Bicchierai, "'Stalkerware' Website Let Anyone Intercept Texts of Tens of Thousands of People," *Motherboard* (31 October 2018) <https://motherboard.vice.com/en_us/article/pa97g7/xnore-copy9-stalkerware-data-breach-thousands-victims>; and Lorenzo Franceschi-Bicchierai, "Spyware Company That Marketed to Domestic Abusers Gets Hacked," *Motherboard* (28 August 2018) <https://motherboard.vice.com/en_us/article/mb4y5x/thetruthspy-spyware-domestic-abusers-hacked-data-breach>.

296 Joseph Cox & Lorenzo Franceschi-Bicchierai, "'I'm Going to Burn Them to the Ground': Hackers Explain Why They Hit the Stalkerware Market," *Motherboard* (19 April 2017) <https://motherboard.vice.com/en_us/article/vvabv3/hackers-why-they-hit-stalkerware-flexispy-retina-x>.

297 *Ibid*. See also, Lorenzo Franceschi-Bicchierai, "A Hacker Has Wiped a Spyware Company's Servers—Again," *Motherboard* (16 February 2018)<https://motherboard.vice.com/en_us/article/3k7a5k/hacker-wipes-spyware-retina-x-flexispy>.

298 Lorenzo Franceschi-Bicchierai, "This Spyware Data Leak Is So Bad We Can't Even Tell You About It," *Motherboard* (22 March 2019) <https://motherboard.vice.com/en_us/article/j573k3/spyware-data-leak-pictures-audio-recordings>; Lorenzo Franceschi-Bicchierai, "Hosting Provider Finally Takes Down Spyware Leak of Thousands of Photos and Phone Calls," *Motherboard* (26 March 2019) <https://motherboard.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy>.

In interviews with journalists, hackers have indicated that breaching stalkerware companies' systems was "[n]ot particularly difficult … I didn't need any 0days [zero-day vulnerabilities]," in FlexiSPY's case,[299] and required, in the case of Retina-X, "[n]ot really any advanced techniques anywhere, just lots of digging to find useful vulnerabilities with the info I already had.[300] In fact, the same hacker breached Retina-X a second time in 2018; the hacker then deleted all of the data on some of the company's servers. Much of this data comprised photos and other data taken from stalkerware victims' devices.[301]

PIPEDA requires organizations to implement "appropriate security safeguards to provide necessary protection," including physical, organizational, and technological measures, such as encryption.[302] In the case of Retina-X, the hacker found a critical key and credentials that were required to access a server that held the private data taken from stalkerware targets; this information was stored in plaintext.[303] Similarly, in 2018, mSpy "leaked millions of sensitive records online, including passwords, call logs, text messages, contacts, notes and location data secretly collected from phones running the stealthy spyware"[304] after previously being hacked in 2015.[305]

The Office of the Privacy Commissioner of Canada does not consider the inadvertent disclosure of personal information, in and of itself, to automatically mean that there were inadequate safeguards in place.[306] However, the track record of data breaches

299 Joseph Cox & Lorenzo Franceschi-Bicchierai, "'I'm Going to Burn Them to the Ground': Hackers Explain Why They Hit the Stalkerware Market," *Motherboard* (19 April 2017) <https://motherboard.vice.com/en_us/article/vvabv3/hackers-why-they-hit-stalkerware-flexispy-retina-x>.

300 *Ibid*.

301 Lorenzo Franceschi-Bicchierai, "A Hacker Has Wiped a Spyware Company's Servers—Again," *Motherboard* (16 February 2018) <https://motherboard.vice.com/en_us/article/3k7a5k/hacker-wipes-spyware-retina-x-flexispy>.

302 Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principle 7 – Safeguards," (updated online January 2018) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_safeguards/>.

303 Lorenzo Franceschi-Bicchierai, "A Hacker Has Wiped a Spyware Company's Servers—Again," *Motherboard* (16 February 2018) <https://motherboard.vice.com/en_us/article/3k7a5k/hacker-wipes-spyware-retina-x-flexispy>.

304 "For 2nd Time in 3 Years, Mobile Spyware Maker mSpy Leaks Millions of Sensitive Records," *KrebsonSecurity* (4 September 2018) <https://krebsonsecurity.com/2018/09/for-2nd-time-in-3-years-mobile-spyware-maker-mspy-leaks-millions-of-sensitive-records/> ("mSpy has a history of failing to protect data about its customers and — just as critically — data secretly collected from mobile devices being spied upon by its software.").

305 "Mobile Spyware Maker mSpy Hacked, Customer Data Leaked," *KrebsonSecurity* (4 May 2015) <https://krebsonsecurity.com/2015/05/mobile-spy-software-maker-mspy-hacked-customer-data-leaked/>.

306 Office of the Privacy Commissioner of Canada, "Safeguards," PIPEDA Interpretation Bulletin (June 2015) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-in-

and leaks associated with stalkerware companies, combined with the obligation to provide higher protection and security where information is more sensitive, suggests that stalkerware app companies may be failing in their obligations to implement safeguards that are commensurate with the sensitivity of the data they collect and store. For instance, after investigating the data breach of Ashley Madison, an online dating website for married individuals seeking to have affairs, the OPC stated that assessing the adequacy of safeguards "should not focus solely on the risk of financial loss to individuals due to fraud or identity theft, but also on their physical and social well-being at stake, including potential impacts on relationships and reputational risks, embarrassment or humiliation."[307] The OPC went on to find that Avid Life Media (which owned and operated Ashley Madison) had not sufficiently complied with PIPEDA's safeguard obligations, given the particular sensitivity of users' data in the context of its website and business. This conclusion was reached despite the company having implemented a number of physical, technological, and organizational safeguards. Given that stalkerware apps typically collect, store, and transmit targets' personal information from dating apps, all major messaging and social media apps, browsing history, and phone conversation logs, this would seem to necessitate, commensurately, implementing the greatest possible security for the data of targeted individuals.

To the extent that stalkerware companies remain in operation, it is imperative that they do not put people targeted by their apps into situations where the targeted individuals are doubly harmed: first, by having their personal information collected, used, and disclosed covertly or without their consent, and second, by having their personal data published or further disclosed as the result of a major data breach. However, it may also be the case that the very functionality of stalkerware, which is to grant a private individual unauthorized access to a targeted person's personal information, inherently constitutes a fundamental breach of the obligation to implement technical safeguards.[308] On a certain level, it is challenging to meaningfully speak of stalkerware applications' safeguard obligations when stalkerware itself is a form of malware against which such safeguards are typically intended to protect against. To discuss safeguards with stalkerware also involves a certain suspension

formation-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_08_sg/>.

307 Office of the Privacy Commissioner of Canada, "Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner," PIPEDA Report of Findings #2016-005 (22 August 2016) at para. 44.

308 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1, s. 4.7.1 ("The *security safeguards shall protect personal information against* loss or theft, as well as *unauthorized access*, disclosure, copying, use, or modification." (emphasis added)).

of the finding that such software should not be in operation to begin with, because it likely violates section 5(3) of PIPEDA (use, collection, or disclosure of data for an "appropriate purpose"), such that safeguard obligations are rendered moot.

iv. General Data Protection Regulation (GDPR) (European Union)

The General Data Protection Regulation (GDPR) implemented sweeping privacy and data protection legal reform in the European Union (EU). The EU passed the law in 2016 and began enforcing it in May 2018, after a two-year grace period for businesses to bring themselves into compliance with the new requirements. While the GDPR is not Canadian legislation, it does apply to stalkerware operated and sold in Canada, and additionally illuminates how Canadian lawmakers might strengthen protection for targets of stalkerware abuse.

First, the GDPR applies to all entities that process personal data "in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."[309] This means that European stalkerware companies whose software is sold to customers in Canada or is used to target individuals in Canada are subject to the GDPR. Second, the GDPR applies extraterritorially to any businesses that collect or process the data of European citizens. Thus, if a stalkerware company were based in Canada, but collected or processed the personal data of an individual in Europe—whether because their device had been infected or because that individual was in contact with a targeted individual in Canada—the GDPR would apply with equal force to this Canadian company. This extraterritorial application of GDPR would also apply to stalkerware companies based in the United States or anywhere outside the EU.[310]

Many technology companies have taken their obligations under the GDPR seriously. Their recognition of those obligations and corresponding changes to their business practices may have been incentivized by the penalties for violating any of several key provisions or fundamental principles of the law. Specifically, these penalties include fines of the higher of 20 million euros or 4% of a company's annual global profits.

309 European General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC at Art. 3 [GDPR].

310 For clarity, the GDPR is based on geographical location and not citizenship; thus, the protections would apply to non-EU citizens who reside in an EU country, and would not apply to EU citizens who are living outside of the EU, unless the data processing business itself provided the requisite nexus engaging GDPR.

Both Google and Apple, for example, appeared to intensify their enforcement efforts to ensure that developers complied with key privacy and data protection provisions of each company's respective app stores policies and developer agreements. Many considered these moves to be encouraged by the imminent enforcement date of the GDPR. Two weeks before the GDPR compliance deadline in May 2018, Apple contacted all developers whose applications in the Apple App Store appeared to violate Apple's developer guidelines by transmitting users' location data without consent, without stating their purpose for collecting and using that data, without explaining how such data was shared or disclosed, or without an approved purpose for collecting and using location data. Apple also removed applications that sold user location data to third parties and notified developers that they could resubmit their applications for review after bringing them into compliance with Apple's store guidelines and policies.[311]

As of June 2018, Apple also began requiring all applications to include privacy policies, and such policies had to "detail any third parties that [user] data is shared with—such as analytics tools, advertising networks, and third-party SDKs [software development kits]—and must ensure these parties are also compliant with the new policy."[312] Notably, developers who submitted new apps for review could not edit their privacy policies after obtaining approval for distribution on Apple's App Store. Instead, they could change their policy only alongside subsequent versions of their app, which would also be submitted for review. Similarly, Google increased enforcement of its own data protection and user privacy policies with respect to call logs, SMS logs, and specific provisions against stalkerware.[313]

a) Privacy Obligations under GDPR

Many of the GDPR's key provisions and principles align with those of Canadian consumer privacy law under PIPEDA and substantially similar provincial legislation. Stalkerware faces as many if not more legal difficulties under the GDPR as it does under PIPEDA. The GDPR defines personal data as "any information relating to an

311 Christian Zibreg, "GDPR is coming soon so Apple starts clamping down on apps that sell your location data," *iDB* (9 May 2018) <https://www.idownloadblog.com/2018/05/09/apple-removing-apps-location-data>; and William Judd, "Apple removes location leaking apps ahead of GDPR deadline," *Developer* (11 May 2018) <https://www.developer-tech.com/news/2018/may/11/apple-removes-leaky-apps-ahead-gdpr-deadline/>.

312 Danny Palmer, "Apple looks to plug App Store privacy hole with new personal data policy," *ZDNet* (3 September 2018)<https://www.zdnet.com/article/apple-looks-to-plug-app-store-privacy-hole-with-new-personal-data-policy>; and Apple App Store, "App Store Review Guidelines," (last updated December 2018) <https://developer.apple.com/app-store/review/guidelines/#data-collection-and-storage>.

313 See **Information Box 14: Apple and Google Enforcement Actions against Apps Violating App Developer Policies and Agreements**, in Part 4.

identified or identifiable natural person," including online identifiers, and it sets out a higher level of obligations for collecting and processing "special categories" of more sensitive data, such as biometric data, health data, sexual orientation, union membership, political opinions, and religious belief.[314] Stalkerware routinely captures personal data and sensitive data due to the breadth and depth of information that it exfiltrates from a targeted person's mobile device.

The GDPR sets out different obligations depending on whether an entity is a "controller" or "processor" of data. A "controller" decides what data is collected and why, whereas a "processor" handles the data in accordance with the controller's decisions. Unless a stalkerware company outsourced their user dashboards, they would presumably be both a data controller and processor. The GDPR would require a stalkerware business, as a controller, to conduct a Data Protection Impact Assessment (DPIA) (Art. 35), obtain explicit consent for collecting special or sensitive data, appoint a data privacy officer (DPO) (Art. 37), maintain records of their data processing activities (Art. 30), and notify the local supervisory authority of any data breaches within 72 hours of awareness (on pain of up to 10 million euros, or 2% of annual worldwide turnover, whichever is higher) (Art. 33). As a processor, the stalkerware company would have to additionally implement and ensure "appropriate technical and organisational" security measures (Art 32) and cooperate with the relevant supervisory authority (Art. 31). Various stalkerware companies have been documented as neglecting or acting contrary to several of these obligations, such as requiring explicit consent from the data subject or notifying a data protection authority of a data breach.[315]

The GDPR sets out two sets of conditions under which collecting personal data is lawful. The first set applies to collecting personal data in general; the second set applies to collecting sensitive data in special categories designated by the law. Processing personal data is lawful only if the data subject has consented, or if the processing is necessary to any of the following objectives: fulfilling a contract with the data subject, complying with legal obligations, protecting the data subject's or another individual's vital interests, performing a public interest task, or exercising official authority. Processing is also lawful where it is necessary for the "legitimate interests" of the controller or a third party, "except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data."[316]

314 GDPR, Art 9.

315 See e.g., "More Evidence of mSpy Apathy Over Breach," *Krebs on Security* (27 May 2015) <https://krebsonsecurity.com/2015/05/more-evidence-of-mspy-apathy-over-breach/>.

316 GDPR, Art. 6(1)(f).

Based on the details of stalkerware as described throughout earlier sections of this report, a cursory analysis suggests that stalkerware activities would not meet any of the GDPR conditions with respect to the data subject—the individual whose personal data and sensitive data is collected, processed, and disclosed by the stalkerware company.

The GDPR outright prohibits processing sensitive personal data, designated in special categories, with a number of specified exceptions. Exceptions include the following circumstances: the data subject has given explicit consent, provided the law did not make their data protection right inalienable; the processing is necessary to meet obligations or exercise rights under employment, social security, or social protection law; the processing is to protect the data subject's or another individual's vital interests where the person is "physically or legally incapable of giving consent;" the data subject has "manifestly made public" the sensitive personal data; or the processing is necessary to pursue or defend legal claims, for "substantial public interest," for public health reasons in the public interest, or for public interest archiving purposes, scientific or historical research purposes, or statistical purposes.[317]

In addition to meeting one of the above conditions for lawful collecting or processing of data, organizations and businesses subject to the GDPR must also adhere to six overarching privacy principles in Article 5:

a) Lawful, fair, and transparent processing;

b) Specified, explicit, and legitimate purposes;

c) Data minimization (collecting only what is adequate, relevant, and necessary);

d) Accuracy and currency of personal data;

e) Storage limitation (data subjects are identifiable only for as long as necessary for the processing purpose); and

f) Ensuring appropriate technical or organizational security measures against unauthorised or unlawful processing and accidental loss or damage of the personal data.[318]

317 GDPR, Art. 9.

318 GDPR, Art. 5.

The GDPR mandates that companies integrate privacy by design[319] and privacy by default into their data practices; stalkerware applications contravene both of these kinds of data practices. Specifically, article 25 of the GDPR centers on user control over what happens to their data. Privacy by design speaks to building privacy into the technology itself where possible and contemplating privacy as part of the engineering challenge from the start, rather than an afterthought or after-the-fact component that is tacked on. Privacy by default means that where an app or website gives users the choice to share their data, the default option is to *not* share, so that the user must actively opt in to sharing their data (rather than remain constantly vigilant about opting out of defaults set to share their data). Contrary to these principles, stalkerware is openly and specifically designed to circumvent the privacy and control of the targeted data subject, while simultaneously denying the targeted person a choice about the collection, processing, and disclosure of their personal and sensitive data.

b) Consent and Privacy Rights under GDPR

Consent plays a central role in the GDPR. The regulation defines consent as "freely given, specific, informed and unambiguous indication of the data subject's wishes . . . by a statement or by a clear affirmative action"[320] that agrees to the requested processing of their personal data. In elaborating on "freely given consent," Recital 43 notes that consent is not a valid legal ground for processing data if there is a "clear imbalance" between the data subject and the controller.[321] While this refers to the business or organization collecting and processing the user's data, it is significant that the GDPR recognizes the invalidating impact of power dynamics on the validity of consent. This recognition could, and should, also apply to power imbalances associated with the context of intimate partner abuse and gender-based violence in which the stalkerware industry operates.

Article 7 sets out "conditions for consent," which include the data subject having the right to withdraw their consent "at any time." The GDPR states that "it should be as easy to withdraw as to give consent"—a particularly pertinent mandate in contexts where the data subject may not have been given an opportunity to consent in the first place. Recital 32 further elaborates on conditions for consent by describing various forms of obtaining consent as examples of legitimate or illegitimate ways

319 Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario (January 2011) <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

320 GDPR, Art. 4(11).

321 GDPR, Recital 43.

to obtain consent for the purpose of GDPR compliance. For example, "[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent."[322]

The GDPR's emphasis on valid consent, on the particular form of consent, on what constitutes meaningful consent (i.e. freely given, specific, informed, and unambiguous), and on the conditions in which a data subject is asked for and gives consent, highlights the importance of ensuring that individuals understand and have control over what is done with their data. However, the protection does not stop at individual control in and of itself: the GDPR as a whole, including its focus on consent, upholds the principle of human dignity and autonomy that has driven European privacy law.[323] Similarly, in Canadian law, the Supreme Court of Canada has recognized that "[w]hile all aspects of privacy — both from the state and from other individuals — serve to foster the values of dignity, integrity and autonomy in our society, the connection between personal privacy and human dignity is especially palpable."[324]

Rooting privacy rights in fundamental human dignity and autonomy is critical in the context of stalkerware and similarly abusive technology because the nature and purpose of such technologies and gender-based abuse often strips the targeted individual of power, choice, autonomy, and control. The loss of autonomy and corresponding impairment of human dignity is at the core of what the GDPR aims to prevent or remedy in the context of activities such as applying data analytics for the purpose of targeted advertising, which would generally not be considered abusive on the level of stalkerware. The GDPR provisions thus likely apply with even greater force where the very purpose of collecting and processing an individual's data directly engages core harms to privacy, autonomy, and dignity, separate and apart from poor data collection practices.

While the GDPR promotes and protects individuals' privacy and data protection rights in many ways, certain user rights and remedies are particularly salient in the context of stalkerware-facilitated abuse. These include provisions such as the right to be given particular details when one's data is collected, such as the purpose of processing and the identity of any others who will receive the data (Arts. 13 and 14); the right to request erasure of data (Art. 17); and the right to restrict processing of one's data (Art. 18).

322 GDPR, Recital 32.

323 Avner Levin & Patricia Sánchez Abril, "Two Notions of Privacy Online" (2009) 11:4 *Vanderbilt J of Ent and Tech L* 1007 at 1007-17.

324 *R. v. Jarvis*, 2019 SCC 10 at para. 65.

Article 13 mandates what information the controller must provide to the data subject when their personal data is collected, while Article 14 mandates what information must be given to the data subject if that person's personal data is collected from *someone else*. These provisions, together, indicate that if a stalkerware company is a controller or processor of the targeted individual's personal data, then they must inform that person of a number of details surrounding the data collection and processing at the time it occurs. The company must inform the targeted individual regardless of whether the company is considered to have collected the data directly from them (i.e., as a result of exfiltrating communications logs and application data from their device), or whether the company is considered to have obtained the personal data from someone other than the data subject (i.e., from the stalkerware operator who facilitated the collection and processing by installing the stalkerware onto the targeted person's device).

Article 17, the right to erasure, is also known as the "right to be forgotten." Experts have noted that this provision raises troubling implications for freedom of expression and access to information rights.[325] However, confined to the context of stalkerware, Article 17 provides targeted persons with an effective tool to exercise core data protection rights against stalkerware vendors and developers who have collected or processed their personal or sensitive data without consent. For example, a targeted individual could request that a stalkerware company erase their personal data "without undue delay" on grounds that the data was unlawfully processed.[326] Using Article 17 for the specific purpose of providing remedy to stalkerware victims may not engage, to the same extent, issues and concerns associated with applying erasure rights to user-generated content or information in the public interest.

Article 18 allows data subjects to restrict processing of their personal data under any of four circumstances: contested accuracy of data; unlawful processing (in cases where the data subject does not desire the data to be erased); lack of further need for the data by the controller or processor; or if the data subject has objected to processing under Article 21. This provision may be useful when a targeted individual requests that a stalkerware company stop collecting and processing their data, but also asks that the already-collected data remain intact. This request could enable the individual to use the exfiltrated data as evidence to support legal action against

325 See, e.g., Daphne Keller, "The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation," (2017) 33 *Berkeley Tech LJ* 297; and Michael Geist, "Why a Canadian right to be forgotten creates more problems than it solves," *Globe and Mail* (26 January 2018) <https://www.theglobeandmail.com/report-on-business/rob-commentary/why-a-canadian-right-to-be-forgotten-creates-more-problems-than-it-solves/article37757704/>.

326 GDPR, Article 17(1)(d).

either the stalkerware vendor or developer, or against the operator who installed the stalkerware on the targeted person's device.

c) Comparing Regulatory Enforcement Powers under GDPR and PIPEDA

The GDPR provides robust protection for individuals whose data is collected and processed and provides meaningful enforcement of data protection rights and obligations. Such enforcement capabilities have implications for the viability of stalkerware under the GDPR and serve as a model to which Canadian privacy law may aspire when it comes to addressing abusive technology. For example, in addition to the ability to impose non-negligible financial penalties, the GDPR confers numerous other powers on the relevant supervisory authority to enforce compliance. The following items provide some examples of these powers:

- Ordering compliance with GDPR provisions;
- Ordering compliance with an individual's data protection request that the GDPR has provided for;
- Imposing a ban on processing data; or
- Ordering the suspension of cross-border data transmissions.

The Office of the Privacy Commissioner of Canada, by contrast, does not have the power to impose administrative financial penalties (AMPs), nor may it directly order an entity to comply with its own recommendations or PIPEDA. Rather, the OPC must rely on public interest disclosures ("name and shame"), on regulated entities' voluntarily implementing recommendations after a complaint investigation, or on compliance agreements negotiated with a non-compliant entity. The OPC cannot directly enforce an order on its own authority. Instead, it must apply to the Federal Court of Canada for a hearing to obtain a court order that requires the company to comply with the OPC's recommendations.[327] There is comparatively little meaningful recourse in the way of either preemptive deterrence or remedy and enforcement after the fact. This lack of recourse is particularly the case with stalkerware businesses, which are no stranger to and demonstrably inured to public shaming.[328] As such, legislative reforms that confer on the OPC powers similar in

327 Office of the Privacy Commissioner of Canada, "Enforcement of PIPEDA," (last updated April 2017) <https://www.priv.gc.ca/biens-assets/compliance-framework/en/index#>.

328 Joseph Cox, "Meet FlexiSpy, The Company Getting Rich Selling 'Stalkerware' to Jealous Lovers," *Motherboard* (21 April 2017) <https://motherboard.vice.com/en_us/article/aemeae/meet-flexispy-the-company-getting-rich-selling-stalkerware-to-jealous-lovers>; "More Evidence of mSpy Apathy Over Breach," *KrebsonSecurity* (27 May 2015) <https://krebsonsecurity.com/2015/05/more-evidence-of-mspy-apathy-over-breach/>; Lorenzo Franceschi-Bicchierai, "'Stalkerware' Seller Shuts Down Apps 'Indefinitely' After Getting Hacked Again," *Motherboard* (6 March 2018)

nature to those assigned to European data protection authorities under the GDPR are likely required, at minimum, for the OPC to be able to effectively regulate or discipline spyware companies, where their products and services facilitate gender-based or intimate partner violence, abuse, and harassment.

D. Canada's Anti-Spam Legislation

A stalkerware company that assists with the installation of stalkerware app in the course of their commercial activity may face administrative penalties under Canada's Anti-Spam Legislation (CASL) if the company doesn't comply with its consent requirements.[329] The CASL regulates electronic methods of carrying out commercial activity in Canada. Vendors or developers who install a computer program on another person's computer while acting within the course of commercial activity have such activities regulated under s. 8 of the CASL.[330]

Stalkerware vendors may run afoul of the CASL where they directly assist with the installation of stalkerware in the course of their commercial activities (as opposed to where the operator installs the program after purchase).[331] Where companies assist with installation of a computer program in the course of commercial activity, the company must comply with the CASL's regulatory framework. The framework

<https://motherboard.vice.com/en_us/article/neqgn8/retina-x-spyware-shuts-down-apps>.

329 *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23 [CASL].

330 Section 8 of the CASL restricts any "person" acting in the course of commercial activity, from installing or causing the installation of a computer program on another individual's computer system without either the consent of the owner or authorized user of the computer, or a court order authorizing the installation. The Canadian Radio-television and Telecommunications Commission (CRTC) is one of the government agencies that enforces the CASL, and it published explanatory comments concerning what it means to *cause* the installation of a computer program. Specifically, if software is concealed within another software program that is installed by the owner or authorized user of a computing device, the commercial provider of the concealed software may be liable, even if they were not responsible for the actual installation (s. 10(5)). In the case of stalkerware, this means that if the stalkerware were hidden or concealed in another application, the developer or distributor of the stalkerware may be liable for the installation even though it was the stalkerware operator who actually installed the surveillance software.

331 The CASL does not generally apply where the owner or authorized user of a computer installs software on his or her own device. Several spyware companies do offer direct installation assistance, for an additional fee. See, e.g., FlexiSPY <https://www.flexispy.com/en/flexispy-remote-installation-service-standalone.htm>; and mSpy, "Frequently Asked Questions" <https://www.mspy.com/faq.html> ("With mAssistance, we'll gladly perform initial installation of mSpy on your target mobile device as well as complete Keylogger setup, Locations, disable SMS apps, activate USB-debugging and more. We will also perform full Jailbreak/Rooting procedure for you remotely") and <https://www.mspy.com/support-options.html> ("Advanced mAssistance Package (special assistance in rooting/jailbreaking and installation of mSpy through Team Viewer (for Android devices)").

sets out particularly strict consent requirements in circumstances involving a computer program with the particularly invasive functions that are commonplace in stalkerware apps.[332]

The adequacy of the CASL's protection is somewhat reduced by the fact that consent to the installation can be provided by either the *owner or authorized user* of a device. As a result, if the device is owned by an abusive spouse, consent from the operator or owner of the device would be sufficient under the CASL, even when invasive spyware that causes the computer device to "operate in a manner that is contrary to the reasonable expectations of the owner or an authorized user of the computer system" is installed.[333] The CASL would be more effective in mitigating the harms of stalkerware if the legislation were amended to expressly require meaningful consent from either the *primary user* of a device, or from *all authorized users* of a device, before installation of the software in question.

332 CASL at s. 10(5). Such invasive features include collecting personal information stored on the computer; sending covert communications to another computer; interfering with the authorized user's control over the computer system; changing computer settings without the knowledge of the authorized user; allowing a third party to operate a computer program remotely without the knowledge of the authorized user; or, changing or interfering with data that is stored on the computer system in a manner that obstructs, interrupts or interferes with lawful access to or use of that data by the authorized user of the computer system.

333 CASL at s. 10(5).

Part 4: Legal Analysis of Third-Party Distribution of Stalkerware by Online Intermediaries

An online intermediary, also known as an Internet intermediary or intermediary platform, is a website or service that facilitates others' online activities. Intermediary platforms facilitate social, economic, and other transactions at different levels of the Internet, including: hosting user-generated content (e.g., YouTube, Instagram); facilitating e-commerce (e.g. Etsy, Shopify); providing a public forum (e.g., Twitter, Facebook); enabling crowdfunding (e.g. Patreon, Kickstarter); facilitating gig economy work (e.g., Uber, Airbnb); providing socially mediated information resources (e.g., Wikipedia, Yelp); or providing the underlying infrastructure of the Internet (e.g., Internet service providers or cloud service providers, such as Amazon Web Services [AWS] or Microsoft Azure). In each of these cases, the intermediary derives monetary or other benefits from the activities of users or customers who pursue their own ends on the intermediary's platform.[334] The intermediary itself does not take part in any substantive activity beyond providing and managing the platform.[335]

Intermediaries have attracted legal, regulatory, and political attention due to their fundamental role as gatekeepers of online activities—albeit often with offline impacts—that encompass increasingly greater spheres of democratic society itself.[336] Whether persecuting individuals for copyright infringement or counterfeit products, unmasking anonymous abusers online, combating hate speech, or

334 For more information on online intermediaries, see e.g., Organisation for Economic Co-operation and Development, "The Role of Internet Intermediaries in Advancing Public Policy Objectives," (14 September 2011), cited in Adrian Fong, "The role of app intermediaries in protecting data privacy," (2017) 25(2) *International Journal of Law and Information Technology* 85–114.

335 The level of passivity or active intervention with which intermediaries regulate users' activities and their limits is often a point of contention when it comes to questions of how liable or accountable an intermediary may be held for wrongdoing that occurs on their platform. This is particularly the case when it comes to expression-based platforms that involve active content moderation and curation by the intermediary, such as occurs with Facebook, Twitter, and Google Search. See, e.g., Daphne Keller, "Who Do You Sue? State and Platform Hybrid Power over Online Speech," Hoover Working Group on National Security, Technology, and Law, *Aegis Series Paper* No. 1902 (29 January 2019) <https://www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf>.

336 The impacts of online intermediaries on democracy are especially significant given that many Internet intermediaries effectively enjoy monopoly-like status in the fields they respectively occupy (e.g., Google for search, YouTube for online videos, Facebook for community organizing). See e.g. Luca Belli & Nicolo Zingales, eds, *Platform regulations: how platforms are regulated and how they regulate us. Official outcome of the UN IGF Dynamic Coalition on Platform Responsibility*, 1st ed (Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2017).

mitigating the spread of disinformation, lawmakers and policy stakeholders often view intermediaries as vehicles through which to control, influence, or terminate individual users' activities and behaviours that they consider to be inappropriate, societally undesirable, or illegal. Intermediary liability arises when the law imposes obligations upon platform companies and holds them indirectly or directly responsible for what their users do; such liability typically requires intermediaries to engage in active efforts to address the identified wrongdoing, to assist law enforcement in identifying the purported wrongdoer, or to face legal consequences for inaction.[337]

The availability of stalkerware applications implicates several kinds of online intermediaries, including mobile app stores, payment processors, and stalkerware developers or vendors that are themselves a platform for online activity. For example, PayPal, a well known payment processor, has facilitated the sale of the stalkerware app, HelloSpy. HelloSpy's website "includes multiple references to using its malware for catching cheating spouses."[338] PayPal facilitated such sales despite the company's refusal to support other categories of products and services, such as adult content and VPNs.[339] PayPal stopped providing support to HelloSpy only after being asked for comment by a news publication,[340] suggesting that either the company did not have effective measures to determine if companies were inappropriately being given access to PayPal's services or that the company tacitly accepts stalkerware companies' business until doing so might become difficult for public relations reasons.

Entities such as Internet service providers and transport service providers are also intermediaries: they act as conduits over which other parties conduct their activities. Cloud computing providers similarly engage in intermediary functions.[341]

337 While beyond the scope of this report, intermediary liability is itself a significant area of law and policy at the intersection of technology and human rights, particularly with respect to user-generated content involving hate speech, copyright, defamation, online harassment, disinformation, and censorship. See e.g., "Intermediary Liability," Stanford Law School: Center for Internet and Society, <cyberlaw.stanford.edu/focus-areas/intermediary-liability>.

338 Joseph Cox & Lorenzo Franceschi-Bicchieri, "PayPal Processes Payments for 'Stalkerware' Software Sold to Abusive Partners," *Motherboard* (20 February 2019) <https://motherboard.vice.com/en_us/article/7xnwa9/paypal-payments-stalkerware-software-abusive-partners>.

339 Jordan Pearson, "PayPal Cuts Off VPN Service Canadians Use to Watch Netflix," *Motherboard* (5 February 2016) <https://motherboard.vice.com/en_us/article/xygdg7/paypal-cuts-off-vpn-service-canadians-use-to-watch-netflix-unotelly>.

340 *Ibid*.

341 Peter Mell & Timothy Grace, "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," *United States Department of Commerce: National Institute of Standards and Technology*, Special Publication 800-145 (September 2011) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

These intermediaries constitute the underlying infrastructure of the Internet and are not providing the top-layer applications and online services (such as social media, blogging platforms, email, travel forums, or review sites) that operate on the surface of the Internet (from the user's perspective). Infrastructure-level providers do not tend to exercise any discretion with respect to whom they provide services to; in fact, in some cases, they are legally prohibited from doing so (e.g., in cases where net neutrality laws apply to Internet service providers[342]). What we have defined here as infrastructure intermediaries are thus excluded from the scope of this report.[343]

The analysis in Part 4 focuses on mobile app stores, in particular. Due to their role as central marketplaces for consumer app purchases, app stores are the highest-profile intermediary platforms most commonly associated with stalkerware apps. Based on our examination of two app store companies specifically—Google and Apple—we conclude that these companies' app developer policies and agreements are not necessarily lacking when it comes to addressing the problem of stalkerware being sold or made available on their platforms. Rather, the deficiency appears to lie in inconsistent or inadequate enforcement of the companies' policies and agreements with app developers.

A. Mobile App Stores and Stalkerware

i. Mobile App Stores as Stalkerware Intermediaries

Mobile app stores are intermediaries that connect potential customers and operators to stalkerware apps. Such platforms provide a popular and user-friendly way for developers to sell a wide variety of apps and for consumers to purchase them. The most well-known and popular mobile app stores in Canada are the Apple App Store, which facilitates and manages the sale of apps for iOS, and the Google Play Store, which does the same for Android.

342 Canadian Radio-television and Telecommunications Commission, "Strengthening net neutrality in Canada" (26 January 2018) <https://crtc.gc.ca/eng/internet/diff.htm>.

343 See, however, the role that database hosting provider Codero played in shutting down spyware company's MobiSpy's website in response to a major and publicly reported data leak of collected images and recordings. Lorenzo Franceschi-Bicchierai, "Hosting Provider Finally Takes Down Spyware Leak of Thousands of Photos and Phone Calls," *Motherboard* (26 March 2019) <https://motherboard.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobispy>; Danny Bradbury, "Spyware app exposes private photos, hosting provider steps in," *Naked Security* (28 March 2019) <https://nakedsecurity.sophos.com/2019/03/28/hosting-company-intervenes-in-another-negligent-app-takedown/>.

Google and Apple vet and curate apps to be sold in their respective app stores and profit from the sale of each app.[344] These companies are thus involved, to a certain extent, in facilitating the sales of stalkerware and spyware apps that continue to be made available through their app stores. Moreover, the mobile platforms are widely known to have mandatory standards and criteria for apps that are sold. Apple, in particular, is known for rigorous vetting and bans apps to guarantee a degree of quality control.[345] The companies also bind app developers to certain contractual agreements, policies, and guidelines. As a result of these companies' app curation and developer management activities, the apps in the respective companies' stores enjoy a tacit veneer of approval or legitimacy. Such approval processes may place Google and Apple (and other mobile app store companies) in a position of at least partial responsibility for addressing the stalkerware problem. App stores can meet this responsibility through consistent and robust application of their own vetting processes to all apps, and through sustained efforts to ban app developers who attempt to sell illegal stalkerware apps (those apps that are predominantly useful for covert surveillance or intercepting private communications such as text messages).

The following sections focus on the Apple and Google Play app stores because they dominate the Canadian marketplace. However, the analysis applies to other mobile app stores that facilitate the availability of stalkerware apps or the abusive use of other kinds of monitoring apps. Some sources of stalkerware apps are not specialized platforms, such as app stores; instead, they are third-party websites that make the apps available for purchase and download.[346] The app store analysis applies to these websites to the extent that they also vet and select the apps that they sell, profit from such sales, and hold app developers to terms of service or other agreements regarding app sales.

344 See Apple, "Auto-Renewable Subscriptions," online: App Store <https://developer.apple.com/app-store/subscriptions/> and Google, "Transaction fees," online: Play Console Help <https://support.google.com/googleplay/android-developer/answer/112622?hl=en>.

345 "The [Apple] App Store operates a preapproval process (enforced by a Developer Agreement and explained through Review Guidelines and Human Interface Guidelines), and it is this process that frequently triggers media coverage of the rejection of an app. An iPhone, without modification, can be used only to download or run applications made available to App Store, so acceptance of an app in the iOS App Store is a critical part of any developer's strategy. If approved, the revenue from an app is split, with 30 per cent retained by Apple and 70 per cent passed to the developer": Daithi Mac Sithigh, "App Law Within: Rights and Regulation in the Smartphone Age," (2013) 21:2 *International Journal of Law and Information Technology* 154 at 159; See also, Sarah Mitroff, "Android is Bigger, But Here's Why Apple is Still the Undisputed App Cash King," *WIRED* (18 December 2012) <https://www.wired.com/2012/12/ios-vs-android/>.

346 E.g. https://download.cnet.com/Spy-Phone-App/3000-2162_4-75999583.html; https://www.detective-store.com/

ii. Availability of Stalkerware Apps on Leading Mobile App Stores

App stores operate as online intermediaries for stalkerware apps and, as such, could potentially be liable or accountable for the harm and abuse that such apps enable or are specifically designed to enable. In 2018, Chatterjee et al found "hundreds of [Android compatible] applications capable of facilitating IPS [intimate partner surveillance]" available online through various websites, with at least 61 of them available in the Google Play Store.[347] The researchers also found over 2,700 Apple compatible apps that matched stalkerware-related search terms on iTunes (a main portal for the Apple App Store) and through a site-specific search ("site: itunes.apple.com") using Google's search engine. Manual review of a random sample of 500 apps found that approximately 20% of them could be used as stalkerware.[348] Many apps were available for Android OS (Google) and iOS (Apple), though some capabilities were blocked by the latter due to different security permissions.[349] The researchers discovered these spyware apps in each company's app store through Internet searches conducted outside both app stores' platforms, if not within the app stores themselves.[350]

Chatterjee et al. note that Google responded to their findings by investigating the apps that were brought to their attention.[351] However, a cursory in-store search several months later by the report's authors (on 18 July 2018) found several dual-use spyware or stalkerware apps still available for purchase on the Google Play Store. We found apps such as "SMS Tracker," "iSpyTracker," "Chat spy for Whatscan App," "Mobile Tracker by mLite: Phone Tracker," and "Text, Message, Notification, Location Remote Spy."[352]

Both Google and Apple made policy changes to their app stores and renewed enforcement measures to remove non-compliant apps in late 2018. Despite these efforts, stalkerware apps continued to appear in both app stores as of May 2019. Searching the Google Play store revealed apps such as "SMS Tracker," "Phone Parent Phone Tracker," "Cell Phone Tracker," and "Spy Tracker."[353]

347 Rahul Chatterjee, et al, "The Spyware Used in Intimate Partner Violence," (2018) *IEEE Symposium on Security and Privacy* <https://www.ipvtechresearch.org/pubs/spyware.pdf> at p. 1.

348 *Ibid* at p. 15.

349 *Ibid*.

350 *Ibid* at p. 1 and 15.

351 *Ibid* at p. 2.

352 Google Play Store, <https://play.google.com/store?hl=en> (accessed 18 July 2018).

353 Google Play Store, <https://play.google.com/store?hl=en> (accessed 10 May 2019).

A cursory in-store search through iTunes found no stalkerware apps in the Apple App Store. However, we applied Chatterjee et al's method of searching for apps in the Apple App Store by using Google's online search engine and including the filter term "site:itunes.apple.com." We added the filter term to each of the search terms "spy phone tracker," "spy on partner," and "spy tracking app" (resulting in three separate searches in total). The search results provided direct links to stalkerware apps within the Apple App Store, such as "Spy Phone Phone Tracker," "mSpy Lite Phone Tracker App," "iSpyTracker," "Phone Tracker for iPhones: GPS," and "SpyTecGPS."[354]

Many of the apps we found were advertised for tracking children or for "family safety," or marketed for employee monitoring. However, they typically claimed to provide features that include the same functionalities that characterize stalkerware, including features such as monitoring a person's location, viewing their messages on third-party apps such as WhatsApp and Facebook, reading their text messages and call logs, viewing their web browsing history, setting up geofences, and monitoring contact lists.

While some apps note that they cannot be concealed or will show persistent notifications while active, others overtly encourage spousal spying in their app descriptions. For example, on the Apple App Store, Phone Tracker for iPhones: GPS leads its description with, "[n]ow you can follow the movements of a friend, *your spouse*, your child, or a co-worker with your iPhone,"[355] while iSpyTracker states, "[e]ver wonder you could see where your children, friends, co-workers *or loved ones were before and where they are right now and what they did* on iPhone, iPad before? The spy panel enables you to view the activities easily."[356] On the Google Play app store, Spy Tracker lists "keep an eye on cheaters" under "Features" in its app description.[357]

Moreover, reviews of some of the apps included statements such as, "Here I am, an [*sic*] husband who works overseas paranoid of what his wife may be doing. I have consistently sought a way to monitor my wife. I used this app, it did it's [*sic*] bit but it wasn't enough;"[358] and "Downloaded this on my wife's iPhone 7. . . .It is suppose[d]

354 Search conducted online by Cynthia Khoo on 10 May 2019.

355 Apple App Store, "Phone Tracker for iPhones: GPS," <https://itunes.apple.com/us/app/phone-tracker-for-iphones-gps/id447442214?mt=8> (accessed 10 May 2019) (emphasis added).

356 Apple App Store, "iSpyTracker," <https://itunes.apple.com/us/app/ispytracker/id640483791?mt=8> (accessed 10 May 2019) (emphasis added).

357 Google Play Store, "Spy Tracker," <https://play.google.com/store/apps/details?id=com.phtrcatr.ptct> (accessed 10 May 2019).

358 Google Play Store, "Phone Tracker Free Official Site," <https://play.google.com/store/apps/de-

to be undetectable on the monitored device. This is misleading. ...We went back and forth and finally they recommended that I subscribe to a higher package. …It [sic] you have a some what [sic] smart spouse/child they will delete the messages as they go along with wiping history's & text messages."[359] Reviews for SMS Tracker on the Google Play app store include "its [*sic*] an amazing app.i really love it. . .my gf will never cheat again" and "i dont like how you have to install the app on the partys phone which you are trying to 'spy on'. lol defeats the purpose haha like seriously."[360] Based on this cursory survey, we conclude that Google and Apple continue to host, facilitate, manage, and derive revenue from the sales of at least some spyware or stalkerware apps, even if (in Apple's case) the apps are not easily found through an in-store search. These apps persist on the companies' respective app stores despite their respective efforts to strengthen stalkerware-related enforcement measures. Significantly, some of the public app descriptions and the public reviews from users are clear that the apps can be used and are in fact used or desired and attempted to be used for the purpose of surveilling intimate partners without consent.

iii. Mobile App Store Policies and Agreements

Mobile app store companies use a range of guiding and binding documents to govern the relationship between the intermediary (e.g., Google or Apple) and the app developers who sell apps on the intermediary's platform. Such documents also establish what developers can and cannot enable their apps to do. These guidelines and agreements are mandatory and non-negotiable, thus putting the app store platforms in a position to significantly influence what developers can do. In this section, we review Apple's and Google's policies and agreements that apply to app developers and assess their applicability to stalkerware apps.

Apple's and Google's agreements and guidelines reveal a number of provisions that these companies can—and to varying degrees already do—enforce to reject and ban intimate partner spyware and repurposed dual-use spyware from their respective app stores. Several instruments govern the activities of developers who sell apps on the Apple App Store; the following agreements and guidelines are most relevant for the purpose of this report:

1) **App Developer Agreement and App Developer Program License Agreement:** These are the main governing contracts between

tails?id=com.phonetrackerofficial1&showAllReviews=true> (accessed 10 May 2019).

359 Apple App Store, "mSpy Lite Phone Tracker App," <https://itunes.apple.com/us/app/mspy-lite-phone-tracker-app/id1182397829?mt=8> (accessed 10 May 2019).

360 Google Play Store, "SMS Tracker," <https://play.google.com/store/apps/details?id=com.stmrsa.htxt&showAllReviews=true> (accessed 10 May 2019).

Apple and the app developer, who is required to sign both. Apple's App Developer Program License Agreement stipulates their "[a]pplications may not be *designed or marketed* for the purpose of harassing, abusing, spamming, stalking, threatening or otherwise violating the legal rights (such as the rights of privacy and publicity) of others."[361]

2) **End-User License Agreement (EULA):** An EULA is a binding agreement between an app developer and the end user of the developer's app. Apple requires every developer to include an EULA between the app and their end users, using either a default EULA that Apple provides or use the developer's own EULA so long as it includes ten provisions mandated by Apple.

3) **App Store Review Guidelines:** This document sets out terms and conditions that an app must meet to pass the Apple App Store approval process. The App Store Review Guidelines establish criteria that require application developers to respect privacy and user consent. For example, apps must "request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity" while also stating that Apple will remove program developers from the App Store if they "use their apps to surreptitiously discover passwords or other private data."[362]

Google binds developers selling apps in the Google Play Store to the following:

1) **Google Play Developer Distribution Agreement:** This is the overall governing contract between Google and the developer. The Google Play Developer Distribution Agreement requires developers to adhere to the Developer Program Policies.

2) **Developer Program Policies:** These policies establish the terms and conditions governing apps in the Google Play Store and fall into several categories. The most relevant for this report are Restricted Content; Privacy, Security and Deception; Impersonation and Intellectual Property; and Enforcement. Google's Developer Program Policies include provisions that specifically address stalkerware apps. These provisions exist under the Malicious Behaviour

361 Apple App Developer Program License Agreement at 3.3.11 (emphasis added).

362 "App Store Review Guidelines," Apple Developer <https://developer.apple.com/app-store/review/guidelines/> at 2.5.14 and 5.1.1 (vi) (accessed July 2018).

> section of its Privacy, Security, and Deception policy. Specifically, "[a]pps that monitor or track a user's behavior on a device must comply with" requirements such as: not claiming to be a "secret surveillance solution," not hiding or misleading users about tracking features, including persistent notifications, and displaying a clearly identifying, unique icon.[363]

Many provisions—in addition to general preamble statements regarding privacy, trust, integrity, and honesty[364]—throughout Google's and Apple's app developer license agreements, policies, and documentation, bind app developers to requirements that stalkerware would appear to violate. These requirements generally fall into the following categories:

- **Legal and Regulatory Compliance:** Developers must ensure their apps adhere to all applicable criminal, civil, and statutory laws and regulations, and they must not use Google's or Apple's software or services to violate any criminal, civil, and statutory laws or regulations. Apps also must not encourage, facilitate, or promote criminal, illegal, or "clearly reckless" behaviour.[365] Given our findings in Parts 1 and 3 of this report that the use, possession, and sale of stalkerware apps (both intimate partner spyware apps and repurposed dual-use spyware apps) likely or do violate one or more of Canada's criminal, civil, and regulatory laws, stalkerware app developers may be violating their agreements with Google and Apple in using their app store services, and those selling intrusive spyware apps that enable surreptitious interception of another person's private communications almost certainly are doing so.
- **Privacy Rights, Prior Explicit Informed Consent, and User Notification:** App developers, in designing their apps, must respect user privacy and privacy laws in order to sell or provide apps in the Google Play and Apple App stores. Such requirements compel developers to adhere to high standards

363 Google Play Store, "Privacy, Security, and Deception: Malicious Behavior," <https://play.google.com/about/privacy-security-deception/malicious-behavior/> (accessed July 2018).

364 See, e.g., "App Store Review Guidelines," Apple Developer <https://developer.apple.com/app-store/review/guidelines/> at "Introduction" ("We will reject apps for any content or behavior that we believe is over the line."), 5.1 ("Protecting user privacy is paramount in the Apple ecosystem, and you should use care when handling personal data…"), 5.5 ("Customer trust is the cornerstone of the App Store's success. Apps should never prey on users [. . .] or engage in any other manipulative practices within or outside of the app."), and 4.2 ("If your App doesn't provide some sort of lasting entertainment value, or is just plain creepy, it may not be accepted").

365 "Google Developer Program Policies," <https://play.google.com/about/restricted-content/illegal-activities/> at "Illegal Activities;" Google Play Developer Distribution Agreement, <https://play.google.com/about/developer-distribution-agreement.html> at 4.6; Apple App Developer Agreement at 5; Apple App Developer Program License Agreement at 3.2, 3.3.11, 3.3.28, and 6.8.

of informed, explicit consent and clear user notification regarding app functionalities such as tracking, collecting, logging, recording, sharing, or transmitting user activities, behaviour, location, and other data, whether through their device's camera, microphone, or other inputs. User consent must be obtained without manipulation or deceit, and must be easily revocable. Apple requires apps to display "a reasonably conspicuous audio, visual or other indicator" whenever recording or capturing a user's images, video, or voice, and both companies' policies set out specific requirements for consent. These requirements include presenting the request with clear, complete, and unambiguous information; requiring affirmative user action; not considering navigating away or request dismissal or expiration as consent; making clear the purpose for data collecting or tracking; and making all disclosures and consent requests prior to any activities such as keylogging or location tracking. Developers who access health, fitness, or face data through Apple software must use such data only for related services and must not disclose such information to any third parties without prior and explicit informed user consent.[366]

- **Data, Device, and Network Security:** Developers' uses of Google Play and Apple App Store platforms must not interfere with, disrupt, damage, or otherwise access in unauthorized ways—or facilitate others accessing—users' or other third parties' devices, servers, or networks. Apps in the Apple developer program must also not "disable, override or otherwise interfere" with devices' pre-existing "system alerts, warnings, display panels, consent panels and the like;" must not contain "any malware, malicious or harmful code, program … which could damage, destroy, or adversely affect" Apple or other "software, firmware, hardware, data, systems, services, or networks;" and must not improperly divert users' network data or use such information to bypass user settings (such as tracking WiFi network data to determine location, if a user disabled geolocation).[367] These prohibitions mean that if a stalkerware app suppresses a system alert, for example, or improperly

366 "App Store Review Guidelines," Apple Developer <https://developer.apple.com/app-store/review/guidelines/> at 2.5.14, 5.1.1, 5.1.2, 5.1.5; Apple App Developer Program License Agreement at 3.3.8, 3.3.9, 3.3.10, 3.3.14, 3.3.38, 3.3.39, and 3.3.52; Google Play Developer Program Policies, <https://play.google.com/about/developer-content-policy/> at "Privacy, Security, and Deception: User Data: Personal and Sensitive Information: Prominent Disclosure Requirement;" and Google Play Developer Distribution Agreement, <https://play.google.com/about/developer-distribution-agreement.html> at 4.8.

367 Google Play Developer Distribution Agreement, <https://play.google.com/about/developer-distribution-agreement.html> at 4.9; Google Play Developer Program Policies, <https://play.google.com/about/developer-content-policy/> at "Privacy, Security, and Deception: Device and Network Abuse;" Apple App Review Store Guidelines at 1.6; and Apple App Developer Program License Agreement at 3.3.16, 3.3.21, and 3.3.26.

diverts the target's network data, such as routing it through the stalkerware company's servers and delivering it to the operator, the app and its developer may be violating these policies.

- **Deception, Harm, and Malicious Behaviour:** Developers' applications must not engage in, encourage, or facilitate behaviour or activities that may result in physical harm, threats, bullying, or harassment. Google Play's associated policies further expressly prohibit apps "that steal data, secretly monitor or harm users, or are otherwise malicious;" apps "that steal a user's authentication information (such as usernames or passwords) or that mimic other apps or websites to trick users…;" apps "*designed to secretly collect device usage, such as commercial spyware apps*," among other prohibitions; "apps that attempt to deceive users or enable dishonest behavior;" or "apps that help users to mislead others."[368] The latter prohibitions would apply to stalkerware apps that rely on misleading the target in some way, such as by spoofing legitimate messenger apps. In October 2018, Google added the following statement to its Malicious Behaviour policies: "[s]urveillance and Commercial Spyware apps are explicitly prohibited on Google Play." However, the prohibition comes with an exception for "parental (including family) monitoring or enterprise management [which may include employee monitoring]" apps.[369]
- **Transparency of App Functions:** Developers' applications must be transparent about the app's features and operations to the mobile platform companies (e.g., Google and Apple) and to users. Apps must not contain "hidden or undocumented features" and must provide transparent explanations and privacy policies where using, collecting, transmitting, sharing, or disclosing user data, with stricter requirements on personal or sensitive user data. Google sets out specific requirements for in-app disclosures of how user data is handled[370] and apps must notify users of how their data is handled. This policy is important because while some stalkerware apps may explain how they operate to their own customers (i.e., stalkerware operators), the apps

368 "App Store Review Guidelines," Apple Developer <https://developer.apple.com/app-store/review/guidelines/> at 1.4; Apple App Developer Program License Agreement at 3.2(f); and Google Play Developer Program Policies, <https://play.google.com/about/developer-content-policy/> at "Restricted Content: Inappropriate Content: Bullying and Harassment," "Privacy, Security, and Deception: Malicious Behavior," and "Privacy, Security, and Deception: Deceptive Behaviour."

369 Google Play Store, "Privacy, Security, and Deception: Malicious Behavior," <https://play.google.com/about/privacy-security-deception/malicious-behavior> (accessed 24 October 2018) (emphasis added).

370 Google Play Developer Program Policies, <https://play.google.com/about/developer-content-policy/> at "Privacy, Security, and Deception: User Data" (including "Privacy Policy & Secure Transmission" and "Prominent Disclosure Requirement"); and "App Store Review Guidelines," Apple Developer <https://developer.apple.com/app-store/review/guidelines/> at 2.3.1.

likely do not provide similar disclosure to the targeted individuals whom the apps track and monitor—particularly in cases where the app provides and the operator takes advantage of a self-concealment feature.

- **Impersonation and Intellectual Property Infringement:** Developers may not misappropriate another's trademarks, copyright, brand, logos, or name, or have their apps impersonate other apps.[371] This prohibition is relevant because some spyware apps, albeit in other contexts, have disguised themselves as popular messaging apps or other brands.[372] According to this policy, such behaviours ought to result in a given application being blocked or banned from either company's app store.
- **Apple iCloud:** One type of stalkerware that is particularly relevant to Apple is apps that monitor and transmit the targeted person's activities by accessing iPhone backups in the target's iCloud account. In this case, surveillance takes place through an iCloud account instead of through an app that is installed on the target's mobile device. After the stalkerware operator obtains and submits the target's Apple ID and password, the app transmits data from the target's iCloud to a portal that the operator may access through their stalkerware account.[373] Apple's App Developer Program License Agreement involves additional requirements for developers and apps using the iCloud. Specifically, Attachment 4 of the agreement arguably prohibits stalkerware-related activities. The provisions in this Attachment include, for instance,

371 "App Store Review Guidelines," Apple Developer <https://developer.apple.com/app-store/review/guidelines/> at 5.2.1; Apple App Developer Program License Agreement at 3.2(d); and Google Play Developer Program Policies, <https://play.google.com/about/developer-content-policy/> at "Impersonation and Intellectual Property."

372 See, e.g., Morgan Marquis-Boire, "For Their Eyes Only: The Commercialization of Digital Spying," *The Citizen Lab* (30 April 2013) <https://citizenlab.ca/2013/04/for-their-eyes-only-2/> ("We identify instances where FinSpy makes use of Mozilla's Trademark and Code. The latest Malay-language sample masquerades as Mozilla Firefox in both file properties and in manifest."); and Rene Millman, "Spyware found in more than 1,000 apps in Google Play store," *SC Media* (14 August 2017) <https://www.scmagazineuk.com/spyware-found-1000-apps-google-play-store/article/1474247> ("The most recent example of SonicSpy found on the Play Store, was called Soniac and was marketed as a messaging app. While Soniac does provide this functionality through a customised version of the communications app Telegram, it also contains malicious capabilities that provide an attacker with significant control over a target device.").

373 "According to Mobistealth, its non-jailbroken iOS stalkerware can monitor call logs and the phone's contact list, steal photos stored on the device, read all WhatsApp conversations, and remotely track the location of the phone using GPS. It can also log other communication apps, such as WeChat, Kik and LINE. (The company also sells spyware for jailbroken iPhones, normal Android devices, and computers.) . . .According to Apple's website, "iCloud backups include nearly all data and settings stored on your device." An attacker needs the Apple ID and password of the phone they want to monitor. After registering that account with Mobistealth, the company will start pulling data straight away, Mobistealth's website reads. Ostensibly, the monitoring solution would no longer work if the password for the Apple ID was changed:" Joseph Cox, "Paranoid Spouses Can Spy on Partners' iOS 10 Devices with iCloud Backups," *Motherboard* (27 February 2017) <https://motherboard.vice.com/en_us/article/4xpgnj/paranoid-spouses-can-spy-on-partners-ios-10-devices-with-icloud-backups>.

using iCloud-related software "only as expressly permitted by this Agreement and the iCloud Documentation, and in accordance with all applicable laws and regulations;" not transmitting "sensitive, individually-identifiable health information;" and agreeing to comply with all privacy, data protection, and other applicable laws, on pain of Apple suspending or revoking the developer's access to iCloud services, in the company's sole discretion.[374] An app that surreptitiously accesses a targeted person's iCloud account to exfiltrate information without the meaningful consent of the targeted person would appear to violate Apple's iCloud-related developer policies.

Based on this review of Google's and Apple's app developer policies and agreements, such instruments appear to address, in several ways, the abusive practices and functionalities associated with stalkerware. The problem associated with the continued presence of stalkerware apps in both app stores may thus lie with inadequate or inconsistent enforcement of these policies and agreements, rather than with the contents of the documents themselves.

iv. App Store Enforcement Efforts against Stalkerware

Apple and Google have taken action against stalkerware apps and developers on several occasions, or against apps with similar functionalities or which violated their app store and developer policies. Both companies have engaged in ongoing efforts to minimize malware in their respective app stores[375] and their efforts have increased to protect users' privacy rights, consent, and safety in recent years. Some commentators have attributed this galvanized attention to the European Union's General Data Protection Regulation (GDPR), which imposed robust privacy and data protection requirements on companies worldwide and impacted technology companies in particular.[376]

374 Apple Developer Program License Agreement, "Attachment 4: Additional Terms for the use of iCloud," at 1.1, 1.6, 2.2, 3.4, and 3.6; see also Apple Developer Program License Agreement at 3.3.33.

375 See, e.g., Ariel Yosefi, "Google Play has updated its Developer Program Policy Center," *Lexology* (29 March 2016) <https://www.lexology.com/library/detail.aspx?g=123be1d4-08f6-4c36-8061-64b0c29686a3>; and Joseph Cox, "Apple Removes 300 Infected Apps from App Store," *WIRED* (21 September 2015) <https://www.wired.com/2015/09/apple-removes-300-infected-apps-app-store/>.

376 See, e.g., Danny Palmer, "Apple looks to plug App Store privacy hole with new personal data policy," *ZDNet* (3 September 2018) <https://www.zdnet.com/article/apple-looks-to-plug-app-store-privacy-hole-with-new-personal-data-policy/>; and Anirban Ghoshal, "Why businesses need not break a sweat about Google Play Store's policy changes," *TechCircle* (17 October 2018) <https://www.techcircle.in/2018/10/17/why-businesses-need-not-break-a-sweat-about-google-play-store-s-policy-changes>.

Information Box 14: Apple and Google Enforcement Actions against Apps Violating App Developer Policies and Agreements

Apple began removing apps and notifying developers of apps that shared users' location data with third parties shortly before the GDPR was set to come into force in May 2018. App removals were justified on the basis that they violated the App Store Review Guidelines.[377] Apple also established a new provision that required developers to explain to users what an app would do with their data once it was collected, rather than merely asking users for permission to obtain the data.[378] In June 2018, Apple explicitly banned the practice of app developers accessing users' phone contacts to create a database of additional people's contact information for marketing or to sell to third parties.[379] The company continued efforts against app and privacy abuse in August 2018 when it compelled app developers to include a link to their app's privacy policy when submitting their app to the App Store for review (a requirement previously only applied to subscription apps).[380] In February 2019, Apple took action against apps that recorded user actions such as taps, swipes, and keystrokes without first obtaining consent, giving developers one day to remove such tracking capabilities from their apps, or face removal from the app store.[381]

Google has also increased enforcement measures against apps that violate user privacy. The company added new policies in October 2018 to mitigate the availability of abusive app practices and further emphasized its prohibition of commercial spyware apps being sold on, or made available in, its app store.[382] These new measures included a policy that stated that an app must be the default app for phone calls or for SMS (text messaging) in order to be able to collect phone logs or SMS (text message) history. While Google has provided exemptions from this policy for specific use cases, such as task automation and back-up apps,[383] the company's approach suggests that the new policy could pose a barrier to stalkerware apps that rely on covertly collecting call and SMS logs using the banned functionalities.[384]

377 Katie Collins, "Apple reportedly cracks down on apps sharing location data with third parties," *CNET* (9 May 2018) <https://www.cnet.com/news/apple-reportedly-cracks-down-on-apps-sharing-location-data-with-third-parties/>.

378 Lisa Vaas, "Apple boots out apps that abuse location data collection," Naked Security (11 May 2018) <https://nakedsecurity.sophos.com/2018/05/11/apple-boots-out-apps-that-abuse-location-data-collection/>.

379 Valentina Palladino, "Apple bans developers from creating, selling user Contacts databases," *Ars Technica* (13 June 2018) <https://arstechnica.com/gadgets/2018/06/apple-bans-developers-from-creating-selling-user-contacts-databases/>.

380 Benjamin Mayo, "New App Store rules will require all apps to have a privacy policy," *9to5Mac* (31 August 2018) <https://9to5mac.com/2018/08/31/new-app-store-rules-will-require-all-apps-to-have-a-privacy-policy/>.

381 Liam Tung, "iPhone snooping: Apple cracks down on apps that secretly record taps, keystrokes," *ZDNet* (8 February 2019) <https://www.zdnet.com/article/iphone-snooping-apple-cracks-down-on-apps-that-secretly-record-taps-keystrokes/>; and Zack Whittaker, "Apple tells app developers to disclose or remove screen recording code," *Techcrunch* (7 February 2019) <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

382 Google Play, "October 2018: Various updates as outlined below," Updates and Other Resources, <https://play.google.com/about/updates-resources/> (accessed 23 October 2018).

383 Google, "Use of SMS or Call Log permission groups," <https://support.google.com/googleplay/android-developer/answer/9047303?hl=en> (accessed 11 May 2019).

384 It is worth noting that a range of other avenues remain open to stalkerware operators who can manipulate dual-use spyware or repurpose more innocuous apps into serving stalkerware purposes. It is also unclear whether a workaround mechanism is available that would bypass

Apple and Google state in their app developer agreements and policies that each respective company may suspend, remove, terminate, or otherwise limit or close an app developer's account at any time. Platform companies' actions may include removing the offending apps from their respective app stores and platforms at the respective platform company's sole discretion.[385] Apple and Google also state that the companies may remove offending apps if a developer or their app has violated one or more provisions in a license or distribution agreement, such as violating users' privacy rights, failing to obtain informed express consent, or breaking local civil or criminal laws.[386]

App platform companies can also enforce policies against app developers through end user license agreements (EULAs). These agreements govern the terms of use between the app developer and a customer who buys and uses the app. In the stalkerware context, this is a license agreement between the stalkerware operator and the stalkerware app developer; the license is to use the software (as opposed to owning the software, which remains the developer's intellectual property). Apple provides a default EULA to app developers who do not use their own, and the platform company requires developers who create their own EULAs to include certain provisions. One of these provisions gives Apple "the right. . .to enforce the EULA against the End-User."[387] If Apple prohibited collecting third-party data without consent from the person whose personal data is being collected, that prohibition would bind all end users of stalkerware apps that they downloaded from the Apple App Store. Apple could then enforce the EULA against stalkerware operators, where

Google's policy and allow an operator to set up a spyware app to covertly collect and disclose a targeted person's call logs or text messages.

385 Apple App Developer Agreement ("Apple may terminate or suspend you as a registered Apple Developer at any time in Apple's sole discretion");"App Store Review Guidelines," Apple Developer <https://developer.apple.com/app-store/review/guidelines/> at 5.1.2 ("Apps that share user data without user consent or otherwise complying with data privacy laws may be removed from sale and may result in your removal from the Apple Developer Program."); Apple App Developer Program License Agreement at 2.8, 3.3.26, 5.4, and 11.2; Google Play Developer Distribution Agreement, <https://play.google.com/about/developer-distribution-agreement.html> at 8.3 ("Google reserves the right, at its sole discretion, to suspend and/or bar any Product and/or Developer from Google Play or from Devices. If Your Product contains elements that could cause serious harm to user devices or data, Google may at its discretion disable the Product or remove it from Devices on which it has been installed.") and 10.3 ("Google may terminate this Agreement with You for any reason with thirty (30) days prior written notice. In addition, Google may, at any time, immediately suspend or terminate this Agreement with You if (a) You have breached any provision of this Agreement. . .").

386 *Ibid*.

387 "10. Third Party Beneficiary: You and the End-User must acknowledge and agree that Apple, and Apple's subsidiaries, are third party beneficiaries of the EULA, and that, upon the End-User's acceptance of the terms and conditions of the EULA, Apple will have the right (and will be deemed to have accepted the right) to enforce the EULA against the End-User as a third party beneficiary thereof." Apple, "Legal - Instructions for Minimum Terms of Developer's End-User License Agreement," <https://www.apple.com/legal/internet-services/itunes/dev/minterms/> (accessed 25 October 2018).

the stalkerware app developer ignores (or expressly or implicitly encourages) violative uses of its app. Apple could also include terms that explicitly target abusive stalkerware app functionalities in its default EULA provided to developers.

In contrast to Apple, Google does not provide a default EULA or mandatory baseline terms to incorporate into developers' EULAs. However, the company's developer policy states that "to the extent [the developer's] EULA conflicts with this [Google's developer] Agreement, this Agreement will supersede the EULA."[388] Thus a stalkerware app developer cannot include terms that contravene those in its Agreement with Google, such as terms concerning covert surveillance, deception, privacy, consent, and malicious behaviour.

Based on our survey of the companies' enforcement measures, Google and Apple are engaging in good faith efforts to hold app developers accountable for how their apps operate with respect to user data, privacy, and consent. However, the continued existence of stalkerware apps that facilitate covert and illegal surveillance (including repurposed spyware apps), and continuing media coverage of the discovery of violations of app store policies related to stalkerware functionalities and practices (revealed by security researchers or the companies themselves), suggests that more should be done. However, any deficiencies appear to lie with inconsistent or insufficient enforcement, rather than inadequate policies or weak governing terms in agreements with developers.

Potential measures that may further address the problem of stalkerware app availability on app stores include the following:

- App stores must clarify their relevant policies and revise developer terms of agreement regarding user privacy, consent, data and device security, and malicious behaviour to expressly state that such protective policies apply to *the individual whose data is being collected, processed, or disclosed by the app*. Based on our review of Apple's and Google's documents, app store guidelines, policies, and developer agreements currently refer only to a generic 'user', and this can inappropriately or incorrectly be interpreted as referring to the stalkerware operator, as the purchaser of the app, rather than the targeted individual. This gap would leave vulnerable and unprotected the individuals who are most in need of protective measures regarding consent, privacy, and malicious behaviour, against the abusive use of stalkerware and spyware apps.

388 Google Play Developer Distribution Agreement, <https://play.google.com/about/developer-distribution-agreement.html> at 5.3.

- App store platforms could implement regular manual sweeps (such as on a quarterly basis), using the methods involved in identifying apps that violated app store policies and agreements during the crackdowns described in **Information Box 14: Apple and Google Enforcement Actions against Apps Violating App Developer Policies and Agreements**. These sweeps would aim to identify and remove apps that overtly violate policies aimed at preventing commercial spyware, and apps that overtly violate policies concerning user privacy, consent, deception, or malicious behaviour. App stores could also audit, on a less frequent basis (such as semi-annually), dual-use stalkerware apps that appear compliant on their face but could enable stalkerware activities. These sweeps should occur in addition to any automated malware detection or filtering methods that are used, particularly as the dual-use nature of stalkerware may cause some apps to be labelled as "legitimate" even where they are designed, marketed, or used for abuse.[389]
- App stores could implement a public recall process whenever they discover particularly egregious or abusive violations, to prevent the existence of "ghost apps."[390] Ghost apps are apps that have been removed or banned from an app store but continue to operate on users' devices, as the user was not aware of the app's violations, ban, or removal, and app store companies do not always remove banned apps directly from users' phones. Pushing an app recall notification to devices that have the app installed may be a particularly effective measure in the stalkerware context. The push notification would make it more likely that the targeted person sees the notice and is informed of the app's activity on their device and its violative capabilities, a situation they may have remained unaware of otherwise, particularly if the operator was surveilling the targeted individual covertly.

B. Application of PIPEDA to Intermediary Platforms

Section C in Part 3 of this report ("Consumer Privacy and Data Protection Law") canvassed issues that arise in applying the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to stalkerware businesses. However, the commercial activities of intermediary platforms, such as mobile app stores, bring these companies also within PIPEDA's purview. The following sections discuss the extent to which the Office of the Privacy Commissioner of Canada (OPC) could hold

389 See, for example, the analysis of anti-virus detection of stalkerware apps in the Citizen Lab's accompanying report to this one, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry".

390 Danny Palmer, "Ghost apps live on to torment Android users," *ZDNet* (28 February 2017) <https://www.zdnet.com/article/ghost-apps-live-on-to-torment-android-users/>.

an intermediary platform accountable under PIPEDA in a case where a stalkerware app that violates PIPEDA has been made available on an app platform.

i. Applying PIPEDA to Stalkerware Intermediaries (Distributors and Platforms)

The OPC has previously held a platform company liable, under PIPEDA, where the platform handled users' personal information in a way that contravened one or more data protection rights under PIPEDA.[391] The OPC has not tended to hold online platforms liable for their respective activities as intermediaries or for violations committed by the platforms' users. Rather, the Commissioner has typically pursued the wrongdoers directly, instead of placing accountability with the platform used to commit the wrongdoing.[392]

Several OPC decisions indicate how the Commissioner might respond if an individual targeted by stalkerware launched a complaint against an intermediary platform as a result of the stalkerware app having collected and disclosed their personal information. In PIPEDA Case Summary #2009-008, *Report Of Findings: CIPPIC v. Facebook Inc.*, the OPC determined that Facebook had breached several PIPEDA principles by allowing third-party application developers "potentially unlimited access" to users' personal information, without monitoring the developers and proactively ensuring compliance with Facebook's terms, as well as with privacy laws and principles such as those under PIPEDA.[393] Contractual terms did not suffice to discharge Facebook's responsibility for users' data:

> In the absence of any evidence of technological safeguards, I can only assume that, when Facebook speaks of limits on access to users' information, it speaks of contractual limits. In other words, as means of limiting access, it is *relying mainly upon certain prohibitions stated in policy documents, and upon trust in the application developers'*

391 See, e.g., Office of the Privacy Commissioner of Canada, "Use of sensitive health information for targeting of Google ads raises privacy concerns," PIPEDA Report of Findings #2014-001 (14 January 2014) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-001/>; Office of the Privacy Commissioner of Canada, "Google Inc. WiFi Data Collection," PIPEDA Report of Findings #2011-001 <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001/>; Office of the Privacy Commissioner of Canada, "Company's re-use of millions of Canadian Facebook user profiles violated privacy law," PIPEDA Report of Findings #2018-002 (12 June 2018) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-002/>.

392 See, e.g., Office of the Privacy Commissioner of Canada, "Company's re-use of millions of Canadian Facebook user profiles violated privacy law," PIPEDA Report of Findings #2018-002 (12 June 2018) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-002>.

393 Elizabeth Denham, Assistant Privacy Commissioner, "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.," PIPEDA Case Summary #2009-008 (16 July 2009) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/> at para. 193.

> *acknowledged agreement to abide by those prohibitions*. …
>
> When I speak of limits to access, and especially when I consider the vast amounts of Facebook users' personal information potentially available to large numbers of application developers, I believe something much more substantial in the way of safeguards is required. Specifically, I mean *technological safeguards that will not simply forbid, but effectively prevent, developers' unauthorized access to personal information that they do not need*. […]
>
> I find that Facebook does not have adequate safeguards in place to prevent unauthorized access to users' personal information by application developers and is thus in contravention of Principles 4.7, 4.7.1, and 4.7.3.[394]

In April 2019, a joint investigation by the OPC and the Office of the Information and Privacy Commissioner for British Columbia (OIPC BC) again found Facebook to have violated PIPEDA as a result of third-party apps collecting, using, or disclosing users' personal information without first obtaining meaningful consent.[395] As described in Section C(ii)(c) of Part 3, "Delegating PIPEDA Compliance through Terms of Use and License Agreements," Facebook was in contravention of the *Act* in part because the company attempted to protect users' personal information and privacy rights through contractual agreements and policies with third-party app developers, in conjunction with reactive and inadequate monitoring and enforcement measures. The regulators found these measures insufficient to safeguard users' personal information, which had been collected, used, and disclosed by such third-party apps, and thus considered Facebook in violation of PIPEDA.

The OPC's reasoning in the 2009 Facebook case, and the OPC and OIPC BC's analysis in the 2019 Facebook case, may apply to app stores and similar online platforms that do not proactively monitor or investigate app developers for compliance, nor effectively enforce developer agreements, policies, or terms of service against stalkerware apps on their platforms. Intermediary app providers such as Apple and Google (in addition to Microsoft, Amazon, and other app store companies) who fail to engage in such proactive enforcement may be found to have run afoul of PIPEDA, where such enforcement would mitigate or prevent the availability or harms of stalkerware across their respective stores and platforms.

ii. Intermediary Liability under PIPEDA for Third-Party Personal Information

When a stalkerware operator surveils a targeted person, the operator and the

394 *Ibid* at paras. 199-202 (emphasis added).

395 See generally Office of the Privacy Commissioner of Canada, "Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia," PIPEDA Report of Findings #2019-002 (25 April 2019) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/>.

stalkerware app also access the personal data of third parties who communicate with that person, such as their friends, family, colleagues, support workers, or others with whom the targeted person exchanges messages with through mobile apps. Communication with the targeted person results in these third parties' personal data also being collected and disclosed by the stalkerware apps and made available to the operator. These third-party contacts should be entitled to privacy remedies and assistance from intermediary platforms that facilitate stalkerware sales.

The OPC has pursued multiple cases, involving Facebook, that can be implicitly read together as acknowledging concerns with third-party privacy rights and giving rise to an obligation on intermediary platforms to provide privacy remedies to third parties whose data protection rights have been violated. The reasoning in these cases may be extended to apply similar obligations to protect third parties whose data rights have been violated by stalkerware apps targeting a given individual.

For example, in 2009, developers accessed both the personal information of individuals who added an app to their own account and the personal information of friends of those individuals. These friends' information was obtained without their informed and express consent. In finding Facebook's data protection practices non-compliant with PIPEDA, the Commissioner stated:

> "I do not consider it appropriate for Facebook to put on users the onus of informing themselves and opting out of the disclosure of their personal information when friends and fellow network members add applications. Nor do I believe that the practice meets the reasonable expectations of users."[396]

The Commissioner's logic should apply to people who communicate with individuals targeted by stalkerware operators: the targeted individuals' contacts should not bear the burden of discovering and "opting out" of the surveillance. It would also not be reasonable for these contacts to expect that all of their communications with a given individual would be monitored and disclosed to third parties such as the stalkerware developer and the operator who installed the stalkerware or repurposed spyware onto the targeted individual's device.

A 2013 OPC decision further suggests that third parties incidentally affected by stalkerware apps should have access to a remedy provided by the stalkerware app or intermediary. In this case, a teenage student's classmate created a fake account on Facebook that impersonated her and interacted inappropriately with other

396 *Ibid* at para. 208.

classmates on the website.[397] The impersonated student did not use Facebook nor have an account, yet suffered violation of her data protection rights under PIPEDA (to amend and ensure the accuracy and completeness of her personal information). The OPC expressed particular concern with non-users' lack of remedy since, by definition, they lacked access to any in-platform dispute resolution mechanism. In requesting that Facebook help non-users to "reinstate their online reputation" and provide remedy to the student and any others in her situation in the future, the OPC stated:

> We emphasized the need for Facebook, particularly in these non-user cases, to take some measure of responsibility for its business model, which allows imposter accounts to occur in the first place and to take appropriate means to help address or mitigate the emotional and reputational damage resulting from such privacy-infringing events.[398]

Drawing on this statement, "non-users" of stalkerware apps (i.e., the targeted individuals and their friends, family, colleagues, and contacts) should have access to privacy remedies provided by the stalkerware app developer. The OPC's reasoning in the Facebook case may also extend to "non-users" of app stores from which operators purchase stalkerware apps. In this case, "non-users" are the targeted individuals, as they did not access or purchase anything from the app store so far as the stalkerware app is concerned.

C. Extending Canadian Intermediary Liability Law to Stalkerware

Part 4 of this report thus far has discussed online platforms and app stores as intermediaries that play an indirect role in the harms that result from stalkerware apps. This section examines two additional possibilities to address stalkerware through intermediaries. Section C.i considers applying intermediary liability law to app platforms for enabling the availability and sales of stalkerware apps in their stores. Section C.ii shifts the focus of intermediary liability to consider how Canadian law might respond if stalkerware developers themselves are held to be intermediaries, rather than the direct wrongdoers.

397 Office of the Privacy Commissioner of Canada, "In response to a case of a teen who was a victim of online impersonation, Facebook agrees to help non-users, on a case-by-case basis, reinstate their on-line reputation," PIPEDA Report of Findings #2013-010 (11 July 2013) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-010/>.

398 *Ibid* at para. 15.

i. Applying Intermediary Liability Law to Stalkerware Intermediaries

To date, Canada's approach to intermediary liability law has entailed crafting piecemeal approaches through the legislature and the judiciary within the confines of specific areas of law, such as copyright and defamation law.[399] Either Parliament or the courts could plausibly contribute to this piecemeal approach by applying a narrow intermediary liability framework specific to app stores and other intermediary platforms that make available intimate partner spyware or repurposed dual-use spyware.

In copyright law, for example, the Canadian government imposes responsibility on Internet intermediaries through the notice-and-notice regime, which requires Internet service providers to pass on notices of alleged infringement received from copyright owners to the accused subscribers, on pain of a fine rather than direct liability.[400] In contrast, the United States has established a notice-and-takedown regime, which requires notified intermediaries to remove user content that a copyright holder has alleged to be infringing, on pain of being exposed to liability themselves.[401] Concerns regarding due process, proportionality, and online freedom of expression led Canadian legislators to adopt notice-and-notice, to better balance the various interests at stake in copyright law.

The nature of stalkerware, its intended and unintended purposes and consequences, and the individualized abuse and broader societal harms that stalkerware encourages may justify a stronger intermediary liability approach, where such apps are found on intermediary platforms. However, the dual-nature facet of spyware requires a nuanced approach to take into account the different categories of stalkerware as defined in **Information Box 2: Classification of Stalkerware Technology**. For example, it may be appropriate to implement a notice-and-takedown approach in the case of "pure" stalkerware—spyware expressly designed or marketed for

399 See, e.g., Bradley J Freedman, "Canada's New Notice And Notice Regime For Internet Copyright Infringement," *Mondaq* (10 November 2014) <www.mondaq.com/canada/x/353028/Copyright/Canadas+New+Notice+And+Notice+Regime+For+Internet+Copyright+Infringement>; and Emily Laidlaw & Hilary Young, "Internet Intermediary Liability in Defamation: Proposals for Statutory Reform," commissioned by the Law Commission of Ontario (July 2017) <www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-Laidlaw-and-Young.pdf>. See, however, potential changes that may result from the *United States-Mexico-Canada Agreement*: Jordan Press, "USMCA writes new continental rules around online content, experts say," *Financial Post* (2 October 2018) <https://business.financialpost.com/pmn/business-pmn/usmca-writes-new-continental-rules-around-online-content-experts-say>; and United States-Mexico-Canada Agreement, Chapter 19: Digital Trade, Arts. 19.17(2)-19.17(4).

400 *Copyright Act*, R.S.C. 1985, c. C-42, s. 41.25-41.26.

401 *Digital Millennium Copyright Act*, 17 U.S.C. § 512.

the purpose of covert surveillance and monitoring of partners or ex-partners. In contrast, notice-and-notice may be more warranted in cases where spyware is ostensibly developed and sold to be used legally, such as parental or employee monitoring apps where covert surveillance is not a feature, but where evidence arises of the spyware having been repurposed for abuse.

Information Box 15: Legal and Policy Implications of Imposing Liability on Internet Intermediaries

Holding Internet intermediaries directly or indirectly liable for others' wrongdoing raises many legal and policy concerns, particularly with regard to issues of overreach, proportionality, due process, and curtailment or violation of human rights and civil liberties in online spaces, such as the right to freedom of expression or the right to privacy. Intermediary liability law has been a fraught concept since its emergence, and lawmakers should approach any expansion of such with the greatest caution and sensitivity to human rights and civil liberties implications, as recommended, for example, by the Manila Principles on Intermediary Liability.[402]

The particular harms from stalkerware, however, also implicate targeted persons' and marginalized communities' fundamental human rights and the ability to participate and thrive with equal rights and freedoms online and offline. A contextual and purposive approach to addressing technology's impacts on vulnerable groups and individuals thus requires nuanced analysis that may include various approaches to Internet intermediaries. Examining where Canada has already imposed liability on online intermediary platforms, such as to protect copyright, should prompt intersectional reflection on the values and priorities of Canadian law. Such reflection might inform analysis and decisions regarding how the law may most effectively intervene to protect vulnerable individuals' autonomy, dignity, and safety, including their ability to meaningfully exercise their fundamental human rights and freedoms.

ii. Stalkerware Developers and Vendors as Liable Intermediaries

This report has largely considered stalkerware app developers and vendors as the focus of direct liability for wrongdoing; however, vendors and developers of stalkerware apps and services may also be considered intermediaries, who facilitate the wrongdoing of their customers, the stalkerware operators. Here, we consider a possible legal route to hold stalkerware developers and vendors liable, as intermediaries, for harm that falls upon individuals targeted by their spyware.

402 "Manila Principles on Intermediary Liability," <https://www.manilaprinciples.org/>; Electronic Frontier Foundation, "The Manila Principles on Intermediary Liability Background Paper," (30 May 2015) <https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf>.

The analysis that follows is based on the "enabler" provision in the Canadian *Copyright Act*. The *Copyright Act* imposes direct liability on intermediaries for copyright infringement where the intermediary in question provides "a service primarily for the purpose of enabling acts of copyright infringement." This provision applies exclusively to cases where actual copyright infringement occurs.[403]A six-factor test determines whether or not the intermediary is liable and includes: (a) explicit or implicit marketing; (b) knowledge that the intermediary's service facilitated voluminous infringement; (c) the presence or absence of other significant uses of the service; (d) actions that the intermediary could have taken, or did take, to limit infringement; (e) any benefits received as a result of enabling infringement; and (f) the business's economic viability if it could not facilitate infringement.[404]

Without commenting on the merits of such a provision in the copyright context, such a law could serve as one potential model for addressing stalkerware. Specifically, the provisions would be adapted to hold stalkerware app developers and vendors liable for enabling operators to abusively monitor, track, and harass or intimidate their targets. **Table 1: Applying the "Enabler" Provision of the *Copyright Act* to Stalkerware** maps each element of the provision to the stalkerware context; the language in each factor has been edited to refer to stalkerware-facilitated abuse where the original text references copyright infringement.

403 *Copyright Act*, R.S.C. 1985, c. C-42, s. 27(2.3) and 27(2.4).

404 *Ibid*.

Table 1: Applying the "Enabler" Provision of the *Copyright Act* to Stalkerware	
Factors adapted from Section 27(2.4) of *Copyright Act*	**Application to Stalkerware Developers and Vendors to Determine Liability for Operator Abuses**
(a) whether the person **expressly or implicitly marketed or promoted the service as one that could be used to enable** [stalkerware-facilitated abuse];	Companies such as HelloSpy have explicitly marketed their software for the purpose of "catching cheating spouses," including using imagery of a man gripping the wrist of a woman whose face is bruised.[405] Depending on the circumstances, evidence that a stalkerware company has engaged in such marketing in the past may also be considered as part of the liability analysis.
(b) whether the person **had knowledge that the service was used to enable a significant number of acts** of [stalkerware-facilitated abuse];	Stalkerware companies are aware that their software is used in cases of abuse and surveillance without consent. Both informal tests of customer support responses[406] and customer reviews, such as those on the Google and Apple app stores, indicate that customers are purchasing spyware apps expressly to engage in covert surveillance of targeted persons.
(c) whether the service has **significant uses other than to enable acts** of [stalkerware-facilitated abuse];	Spyware that features the ability to remain invisible to the targeted person would likely have little to no significant use other than covertly monitoring and tracking someone without their consent. Child and employee monitoring apps need not remain hidden, invisible, or unknown to the targeted individuals for the monitoring to be effective. In fact, in the case of employees, some forms of surveillance must be disclosed to the monitored individuals if the surveillance is to be considered legal. This provision could assist in distinguishing between apps designed or sold to be used as stalkerware and apps genuinely designed or sold for ostensibly legitimate monitoring practices, such as find-my-phone apps.

405 Joseph Cox & Lorenzo Franceschi-Bicchierai, "PayPal Processes Payments for 'Stalkerware' Software Sold to Abusive Partners," *Motherboard* (20 February 2019) <https://motherboard.vice.com/en_us/article/7xnwa9/paypal-payments-stalkerware-software-abusive-partners>.

406 One informal test carried out by academics involved calling stalkerware companies' support centres: "In response to the question 'If I use your app to track my husband will he know that I am tracking him?', 8 out of 11 responded with affirmative explanations implicitly condoning IPS [intimate partner surveillance]. Only one (an off-store app) replied with an admonishment against use for IPS. Two apps did not respond: Rahul Chatterjee, et al, "The Spyware Used in Intimate Partner Violence," (2018) *IEEE Symposium on Security and Privacy* <https://www.ipvtechresearch.org/pubs/spyware.pdf> at p. 2. See also Nicki Dell, Karen Levy & Damon McCoy, "How domestic abusers use smartphones to spy on their partners," *Vox* (21 May 2018) <https://www.vox.com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spyware-domestic-abusers-apple-google>.

Table 1: Applying the "Enabler" Provision of the *Copyright Act* to Stalkerware	
(d) the person's **ability**, as part of providing the service, **to limit acts** of [stalkerware-facilitated abuse], and **any action taken** by the person to do so;	It is unknown what steps, if any, stalkerware companies have taken to prevent, limit, stop, or redress wrongdoing among their customers, beyond mere disclaimers. There are, however, ways to technologically limit or prevent covert surveillance within an app's design. Examples include implementing just-in-time or persistent notifications whenever a spyware app is actively tracking, logging, monitoring, exfiltrating, or recording a targeted individual's data; and ensuring the app icon or other indicators of its presence cannot be hidden (i.e., removing any "invisibility" features). Such control measures and design choices are within the ability of stalkerware companies to implement.
(e) any **benefits the person received** as a result of enabling the acts of [stalkerware-facilitated abuse]; and	Stalkerware app companies benefit directly from selling their apps. Their revenues are often derived from ongoing subscriptions to these apps and related services, such as company-maintained data portals and dashboards through which the stalkerware operator can access the targeted person's exfiltrated personal data.
(f) the **economic viability of the provision of the service if it were not used to enable** acts of [stalkerware-facilitated abuse]	Where a stalkerware app is a developer's or vendor's sole or core product and service, their business would likely no longer be economically viable if customers were predominantly purchasing their app to facilitate covert and abusive surveillance of targeted individuals and the app no longer enabled such surveillance. Should spyware app companies make changes that curtailed features that could be used for abuse, such as removing the hide-app feature and integrating mandatory just-in-time or persistent notifications, this may decrease or eliminate demand for the product.

The analysis in Table 1 is not presented to endorse this specific legal approach, necessarily, but to demonstrate how one form of existing intermediary liability law in Canada may be analogized from other legal contexts to address the problem of stalkerware, where spyware app vendors and developers are considered to be intermediaries rather than direct perpetrators of harm. As discussed in **Information Box 9: The Wassenaar Arrangement and Challenges of Regulating Dual-Use Technology**, however, legislators and policymakers must engage in any legal reforms in this area with an abundance of caution and informed sensitivity to the risk of unintended consequences, including jeopardizing beneficial activities that may be captured under overbroad definitions or by insufficiently considered drafting.

Part 5: Critical Discussion and Analysis

Parts 1-4 of this report analyze the existing criminal, civil, and regulatory laws in Canada, and relevant policy and international instruments, that relate to using, creating, selling, or facilitating the sale of stalkerware technology in Canada. In Part 5, we engage in more critical and holistic analysis of these kinds of technologies and their social and policy implications.

Section A addresses the dual-use nature of stalkerware and how legislators and policy-makers might respond to the issue of repurposed spyware apps. Specifically, we discuss the legality, regulation, and normative impacts of spyware used with children or employees. On the basis of children's and employee's constitutionally or otherwise protected privacy rights, we challenge the assumption that child monitoring and employee surveillance are legitimate uses of spyware. Given the well-documented association between intimate partner violence, abuse and harassment, and commercially available spyware applications, we set out a number of legal and policy considerations that should be involved in determining the legitimacy of such apps, even where they are ostensibly intended for monitoring children or employees exclusively.

Section B builds on the review of legal issues covered through Parts 1-4 to analyze the ability of Canadian law to adequately respond to the phenomenon of gender-based harm and intimate partner abuse that stalkerware operators perpetrate through stalkerware technology and that app developers, vendors, and distributors facilitate. We review two key barriers to the law's ability to provide remedy to those who have been victimized by stalkerware. The first barrier is lack of sociocultural and technical awareness, training, and resources among law enforcement. The second barrier is the tendency of responses to technology-facilitated gender-based abuse, including stalkerware abuse, to focus on victims of the abuse rather than offenders, who are the source of the abuse.

A. Challenges of Dual-Use Nature of Stalkerware: How Legitimate Are "Legitimate" Spyware Apps?

Stalkerware apps are heavily intertwined with adjacent and overlapping apps that offer similar or identical capabilities but which are ostensibly meant for activities such as increasing child safety or monitoring employees. As this report has documented, oftentimes many of these such apps are one and the same, with their ultimate functionality and purpose turning solely on how and against whom the operator deploys them.

Stalkerware applications are not always advertised for the express purpose of targeted intimate partner surveillance.[407] As described in the Introduction of this report, companies overwhelmingly tend to market their spyware software for purposes that appear—at least at face value—to be more beneficent or legitimate. Applications with stalkerware functionality are often advertised for child monitoring, family tracking, or child safety purposes or for employers to monitor and track their employees.[408]

Efforts to align a spyware company's products with legitimate social ends stand in stark juxtaposition with the capabilities of the spyware products sold to stalkerware operators, who use such apps to facilitate abusive and illegal behaviour.[409] Whether an app is advertised for child safety, anti-theft, or other purposes, there is nothing to prevent bad actors or abusers from exploiting an applications' functions for intimate partner surveillance or gender-based abuse.[410] For example, T-Mobile's "Family Allowances" program lets parents "block their children from texting and calling certain phone numbers, shut down their phones during school and homework hours, and monitor how much they are texting."[411] An abusive operator

407 Where stalkerware apps are advertised for intimate partner surveillance, the marketing can be explicit: for instance, the website of one stalkerware company includes a photograph that appears to depict a man threatening a bruised woman, with surrounding text that discusses the ability of the company's app to "catch cheating spouses": "Mobile Spy App for Personal Catch Cheating Spouses," HelloSpy (2012) <hellospy.com/hellospy-for-personal-catch-cheating-spouses.aspx?lang=en-US> (https://perma.cc/VEB8-7GLB).

408 Kristen Weir, "Parents Shouldn't Spy on Their Kids," *Nautilus* (14 April 2016) <http://nautil.us/issue/35/boundaries/parents-shouldnt-spy-on-their-kids> ("With tracking technologies such as mSpy, Teen Safe, Family Tracker, and others, parents can monitor calls, texts, chats, and social media posts. They can view maps of every location a child (and his phone) has traveled. An app called Mama Bear even sends parents speeding alerts if their kid is traveling too fast in a car."). See also Joseph Cox & Lorenzo Franceschi-Bicchierai, "'Stalkerware' Website Let Anyone Intercept Texts of Tens of Thousands of People," *Vice Motherboard* (31 October 2018), online: <https://www.vice.com/en_us/article/pa97g7/xnore-copy9-stalkerware-data-breach-thousands-victims> ("On its homepage, Xnore describes its 'cell phone tracker app' as the 'best parental & employee monitoring software.' But elsewhere the company also advertises its software to monitor spouses on the suspicion they may be cheating").

409 Diarmaid Harkin, Adam Molnar & Erica Vowles, "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," (2019) *Crime Media Culture* 1.

410 "[S]urvivors and professionals report that other seemingly benign apps, such as family tracking or 'Find My Friends' apps. . ., are being actively exploited by abusers to perform [intimate partner surveillance]. We call these dual-use apps: they are designed for some legitimate use case(s), but can also be repurposed by an abuser for IPS because their functionality enables another person remote access to a device's sensors or data, without the user of the device's knowledge. Both overt spyware and *dual-use* apps are dangerous in [intimate partner violence] contexts." Rahul Chatterjee, et al, "The Spyware Used in Intimate Partner Violence," (2018) *IEEE Symposium on Security and Privacy* 441 <https://www.ipvtechresearch.org/pubs/spyware.pdf> at p. 1 (emphasis in original).

411 Nick Wingfield, "Should You Spy on Your Kids?," *The New York Times* (9 November 2016) <https://www.nytimes.com/2016/11/10/style/family-digital-surveillance-tracking-smartphones.html>. See also "Family Allowances" (2019), online: *T-Mobile* <https://support.t-mobile.com/docs/DOC-

may use these same features to control a partner or ex-partner who is also on the "family plan."[412]

Even where spyware is used for ostensibly "legitimate" purposes, and not deployed in the service of abuse, child monitoring and employee surveillance raise potential legal and human rights concerns in their own right. Laws in Canada and other jurisdictions have generally affirmed that both children and workers possess legally, moreover constitutionally, recognized privacy rights, even in cases of good-faith actors. We discuss such rights and the attendant spyware-related concerns in the following sections on (i) child monitoring and (ii) worker surveillance.

i. Children's Privacy Rights under International and Canadian Law

Children and youth have privacy rights in common with those of adults under domestic and international law.[413] In some circumstances, those rights may be attenuated by the legal rights and obligations of guardians and custodians, such as parents and school authority figures. In other circumstances, the privacy rights of youth operate robustly in the context of the state's obligation to ensure that the best interests of the child are realized.[414] Children's privacy receives enhanced protection under the law, in recognition of the inherent vulnerability of children.[415]

1725> [https://perma.cc/L37Q-CFLW].

412 "Another complexity that came up frequently was that of cellular account ownership. Many clients reported sharing a cellular family plan, with their abuser as the account manager for the plan. In this situation, the abuser is in fact the legal owner of the client's account (and any children's accounts) and can track the devices using anti-theft software, activate or deactivate services, and view billing information containing details of any calls, texts, or charges made to the account. Furthermore, since many clients were financially dependent on the abuser, they often felt unable to cancel the family plan, particularly if doing so would mean purchasing new devices and cellular plans for themselves and their children." Diana Freed et al, "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders" (2017) *Proceedings of the ACM on Human-Computer Interaction - CSCW* <https://www.ipvtechresearch.org/pubs/a046-freed.pdf>.

413 *A.B. (Litigation Guardian of) v. Bragg Communications Inc.*, 2012 SCC 46 at para. 17; UNICEF, "Privacy, Protection of Personal Information, and Reputation Rights," Discussion Paper Series: Children's Rights and Business in a Digital World, UNICEF <https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> at p. 4 ("It is fair to say that children's rights to privacy and the protection of personal information and reputation must be considered, even attenuated, in the context of the need to protect children from harm and abuse and to preserve the role of parents as a source of guidance and support in the exercise of children's rights. However, these rights must not be neglected as children's privacy enjoys equal, albeit qualified, protection under international human rights law.").

414 *Ibid*.

415 As the Supreme Court of Canada stated in *A.B. (Litigation Guardian of) v. Bragg Communications Inc.*, "[r]ecognition of the inherent vulnerability of children has consistent and deep roots in Canadian law" (2012 SCC 46 at para. 17). See also Office of the Privacy Commissioner of Canada, "Draft OPC Position on Online Reputation," *Office of the Privacy Commissioner of Canada* (26 January 2018) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consulta-

The United Nations Convention on the Rights of the Child (UNCRC) (ratified by 192 countries, including Canada)[416] sets out in Article 16 that "[n]o child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation," and that the child "has the right to the protection of the law against such interference or attacks."[417] The UNCRC also provides that every child and youth[418] "who is capable of forming his or her own views [shall have] the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child."[419] The Supreme Court of Canada has recognized similarly in a case involving medical consent from a minor:

> It is a sliding scale of scrutiny, with the adolescent's views becoming increasingly determinative depending on his or her ability to exercise mature, independent judgment. The more serious the nature of the decision, and the more severe its potential impact on the life or health of the child, the greater the degree of scrutiny that will be required. [. . .]
>
> It is not only an option for the court to treat the child's views as an increasingly determinative factor as his or her maturity increases, it is, by definition, in a child's best interests to respect and promote his or her autonomy to the extent that his or her maturity dictates.[420]

Apps and other kinds of software that give parents and guardians full surveillance, monitoring, and controlling capabilities over every aspect of their children's and teenagers' online activities risks violating their rights and interests as provided for in international and Canadian law. Such risks are amplified should the surveillance occur covertly without the child's knowledge or consent, particularly in the case of older children. Intrusive surveillance implicates not only children's privacy rights, but also associated human and children's rights that the right to privacy

---

tion-on-online-reputation/pos_or_201801/> at section c.

416 Sonia Livingstone, John Carr, & Jasmina Byrne, "One in Three: Internet Governance and Children's Rights," *Global Commission on Internet Governance*, Paper Series: No. 22 (Centre for International Governance Innovation and the Royal Institute of International Affairs, 2015) <https://www.cigionline.org/sites/default/files/no22_2.pdf> at p. 9 ("As a normative and analytic framework with which to ensure that important dimensions of children's lives are properly addressed by policy actors, and to gain a holistic perspective on the manifold factors that affect their wellbeing, the UNCRC remains a remarkably resonant, even inspiring document — and a vigorous call to global action. It recognizes children as rights-holders, with full human rights and not a partial version thereof.").

417 Convention on the Rights of the Child, G.A. Res. 44/25 of 20 November 1989 (entry into force 2 September 1990) <https://www.ohchr.org/Documents/ProfessionalInterest/crc.pdf>.

418 UNCRC, Article 1: "For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier."

419 UNCRC, Article 12.

420 *A.C. v. Manitoba (Director of Child and Family Services),* 2009 SCC 30 at paras. 22 and 88.

enables. Such rights include the freedom of expression, including "freedom to seek, receive and impart information and ideas of all kinds … through any other media of the child's choice" (UNCRC, Art. 13); freedom of thought, conscience and religion (UNCRC, Art. 14); access to information "from a diversity of national and international sources" (UNCRC, Art. 17); and the right to "participate fully in cultural and artistic life" (UNCRC, Art 31).

In a report examining how Internet governance might best "translate the UNCRC into a clear set of standards and guidelines and a program of action that addresses children's rights in the digital age," Livingstone, Carr, and Byrne caution the following:

> [Much of Internet policy discourse concerning children] positions children solely as vulnerable victims, neglecting their agency and rights to access, information, privacy and participation. The problematic consequence is that highly protectionist or restrictive policies are advocated for children in ways that may undermine their freedom of expression or that trade children's particular needs off against adult freedoms online… [W]e urge the importance of considering children in relation to Internet governance because of their distinctive needs — as legal minors, not necessarily supported by caring and informed adults, often in the vanguard of online experimentation, and with generic human rights and particular rights regarding their best interests and development to their full potential.[421]

Further, a UNICEF discussion paper, "Children's Rights and Business in a Digital World: Privacy, Protection of Personal Information and Reputation Rights," states:

> Parental controls can similarly threaten children's free and confident use of technology, and applications installed to track children online may generate even more data about children's Internet use. Perhaps most concerning, parents who threaten their children's safety may use their power to cut off digital lifelines for seeking outside assistance. […]
>
> The tension between parental controls and children's right to privacy can best be viewed through the lens of children's evolving capacities. While parental controls may be appropriate for young children who are less able to direct and moderate their behaviour online, such controls are more difficult to justify for adolescents wishing to explore issues like sexuality, politics and religion. … Importantly, parental controls may also hamper children's ability to seek outside help or advice with problems at home.[422]

Numerous studies have noted the detrimental effect of constant surveillance

421 Sonia Livingstone, John Carr, and Jasmina Byrne, "One in Three: Internet Governance and Children's Rights," *Global Commission on Internet Governance*, Paper Series: No. 22 (Centre for International Governance Innovation and the Royal Institute of International Affairs, 2015) <https://www.cigionline.org/sites/default/files/no22_2.pdf> at p. 5 and 15 (footnotes omitted).

422 UNICEF, "Privacy, Protection of Personal Information, and Reputation Rights," Discussion Paper Series: Children's Rights and Business in a Digital World, UNICEF <https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> at p. 9 and 17 (footnotes omitted).

and digitally supercharged parental supervision on children's development. Documented consequences include: children learning to "direct behaviour through punishment and reward […] rather than as a reflection of their values and ethics" and being "denied opportunities to experiment with making critical and ethical choices, leading to lower ability to self-regulate and self-direct their behaviour;"[423] breaking trust between parents and teenage children and damaging the parent-child relationship overall;[424] monitored children becoming more secretive with their parents than children who were not monitored;[425] higher likelihood of mental health issues including anxiety, depression, and withdrawal;[426] and inhibiting children's ability to "learn how to negotiate an appropriate balance between trust and risk."[427] The nexus established in *A.C. v. Manitoba* between the maturity of children and youth as they age and the autonomy they require and that the law grants them as a necessary element of development into adulthood, makes it all the more critical to scrutinize the legitimacy of using stalkerware apps on youth, particularly those in their middle to late teens.

In view of children as future adult members of society, Judy Shulevitz writes, "There's another, possibly even more insidious, consequence of eavesdropping on our offspring. It sends the message that nothing and no one is to be trusted: not them, not us, and especially not the rest of the world. This is no way to live, but it is a way to destroy the bonds of mutual toleration that our children will need to keep our democracy limping along." Correspondingly, a report for the Office of the Privacy Commissioner of Canada noted that "[s]urveillance in childhood

423 Office of the Privacy Commissioner of Canada, "Surveillance Technologies and Children," *Office of the Privacy Commissioner of Canada* (October 2012) at p. 7.

424 Office of the Privacy Commissioner of Canada, "Surveillance Technologies and Children," *Office of the Privacy Commissioner of Canada* (October 2012) at p. 5 ("Trust is fundamental to promoting self-control and healthy development in children, and trust issues are commonly identified by research examining the effects of surveillance on children."). See also: Kristen Weir, "Parents Shouldn't Spy on Their Kids," *Nautilus* (14 April 2016) <http://nautil.us/issue/35/boundaries/parents-shouldnt-spy-on-their-kids>; Gary Marx & Valerie Steeves, "From the Beginning: Children as Subjects and Agents of Surveillance," 7 *Surveillance & Society* 192 (June 2010): ". . .constant monitoring can work against children's developmental needs, and can make it harder for them to become more resilient (Livingstone 2009). It may also work against creating the kinds of trusting relationships that encourage children to comply with adult rules. Kerr and Stattin (2000) report that monitoring children does not encourage pro-social behaviour; instead, children are more likely to behave in pro-social ways when they are able to voluntarily disclose information to adults with whom they share a bond of trust."

425 Skyler Hawk, et al, "'I Still Haven't Found What I'm Looking For': Parental Privacy Invasion Predicts Reduced Parental Knowledge," 49 *Developmental Psychology* 1286 (July 2013), cited in Office of the Privacy Commissioner of Canada, "Surveillance Technologies and Children," *Office of the Privacy Commissioner of Canada* (October 2012) at p. 6.

426 Kristen Weir, "Parents Shouldn't Spy on Their Kids," *Nautilus* (14 April 2016) <http://nautil.us/issue/35/boundaries/parents-shouldnt-spy-on-their-kids>.

427 Office of the Privacy Commissioner of Canada, "Surveillance Technologies and Children," *Office of the Privacy Commissioner of Canada* (October 2012) at p. 6.

can have a profound effect on understanding privacy later in life. Children learn through experience, and if they do not grow up in an environment where privacy is practiced, they may not learn how privacy works."[428] Furthermore, danah boyd has found that "privacy norms established by parents influenced their children's relationships with their peers. Teenagers share their passwords for social media and other accounts with boyfriends and girlfriends."[429] This type of behaviour and accustomization to lack of boundaries, learned from their parents, could potentially lead to gender-based violence, abuse, and harassment, particularly targeting young girls—precisely some of the fears that parental control apps leverage to sell their wares.

Further normalization of ubiquitous monitoring and spying may also make students more vulnerable to technology-facilitated abusive or predatory behaviour from other trusted adults in their lives and in the school environment, such as teachers or coaches.[430] In fact, schools are one of the key drivers of child surveillance tools[431] that are similar to those marketed for parental child monitoring; however, school surveillance applications are usually installed on school-issued laptops or devices.[432] Canadian courts have established that students have a diminished, yet persistent, expectation of privacy while at school, including with respect to searches that the school conducts in accordance with their role as custodians of their students.[433] Such searches, however, generally do not include pervasive and indiscriminate monitoring of students' activities, and authorities must balance students' privacy rights with the school's responsibilities in providing a "safe and secure learning

428 Office of the Privacy Commissioner of Canada, "Surveillance Technologies and Children," *Office of the Privacy Commissioner of Canada* (October 2012) at p. 7; Jason Nolan, et al, "The Stranger Danger: Exploring Surveillance, Autonomy , and Privacy in Children's use of Social Media," 36(2) *Canadian Children Journal* 24 at 27 (2011) ("If children are not afforded privacy in their home life or their daily lives, they will not know how to appropriately establish and advocate for their own boundaries and privacy or recognize those of others as they become adults").

429 Nick Wingfield, "Should You Spy on Your Kids?," *The New York Times* (9 November 2016) <https://www.nytimes.com/2016/11/10/style/family-digital-surveillance-tracking-smartphones.html>.

430 See, e.g. *R. v. Jarvis*, 2019 SCC 10.

431 See, e.g., Frida Alim, et al, "Spying on Students: School-Issued Devices and Student Privacy," *Electronic Frontier Foundation* (13 April 2107) <https://www.eff.org/files/2017/04/13/student-privacy-report.pdf>; Leslie Regan Shade and Rianka Singh, "'Honestly, We're Not Spying on Kids': School Surveillance of Young People's Social Media," 2(4) *Social Media + Society* 1 (2016); Simon Collins, "Birkenhead College requires parent-controlled 'spyware' as condition for students to access school Wi-Fi," *NZ Herald* (1 March 2019) <https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12207910>; and Simone Stolzoff, "Schools are using AI to track what students write on their computers," *Quartz* (19 August 2018) <https://qz.com/1318758/schools-are-using-ai-to-track-what-students-write-on-their-computers/>.

432 Ewen MacAskill, "US school accused of using laptops to spy on pupils," *The Guardian* (20 April 2010) <https://www.theguardian.com/world/2010/apr/20/us-school-accused-laptops-spying>.

433 *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393; *R. v. AM*, 2008 SCC 19.

environment."[434] With respect to digital privacy, "[s]tudents may expect some degree of privacy respecting the contents of their cell phones. As a general rule the vice-principal or teachers will not be scrolling through the contents of their cell phones," barring circumstances that give rise to a reasonable basis for concern and that warrant further search or incursion into a student's privacy.[435]

Further, multiple provincial privacy law regimes have considered that surveillance tools such as video monitoring "should only be used as a last resort after exhausting less privacy-invasive alternatives."[436] The Ontario Information and Privacy Commissioner, in a case concerning video surveillance of students, indicated that schools may implement such surveillance only after finding "less intrusive means … were ineffective or unworkable" and must install surveillance in a way that "minimizes privacy intrusion to that which is necessary, as opposed to simply helpful."[437] Similarly, the Nova Scotia Office of the Information and Privacy Commissioner issued guidelines that indicated that video surveillance should not be used unless it meets four criteria: (1) the surveillance is "demonstrably necessary to meet a specific need," with the need being "pressing and substantial;" (2) the institution has attempted and confirmed there are no less privacy-invasive methods available to achieve the same objective; (3) there is "clear evidence" the video surveillance will effectively meet the identified need; and (4) the loss of privacy from the surveillance is proportional to the need.[438] Extending these legal principles and requirements to electronic surveillance through children's digital devices would suggest that generalized monitoring of the kind that stalkerware apps promote is problematic at best, if not an outright unlawful violation of children's privacy.

Parental control and surveillance apps may also expose children to more online risks to third-party bad actors than they would be otherwise. Such exposure may result from security flaws in the apps, despite the apps ostensibly providing security

434 *R. v. Ermine*, 2014 SKPC 162 at para. 15. See also the reasonable expectation of privacy analysis for students in *R. v. Jarvis*, 2019 SCC 10.

435 *Ratt v. Tournier*, 2014 SKQB 353 at para. 33.

436 Office of the Information & Privacy Commissioner for British Columbia, "Guidance Document: Using Overt Video Surveillance," *Office of the Information & Privacy Commissioner for British Columbia* (October 2017) <https://www.oipc.bc.ca/guidance-documents/2006>.

437 Information and Privacy Commissioner of Ontario, Privacy Complaint MC13-46, Halton Catholic District School Board (11 March 2015) <https://decisions.ipc.on.ca/ipc-cipvp/privacy/en/134689/1/document.do> at p. 12.

438 Office of the Information and Privacy Commissioner of Nova Scotia, "Video Surveillance Guidelines," *Office of the Information and Privacy Commissioner of Nova Scotia* (16 March 2017) <https://oipc.novascotia.ca/sites/default/files/publications/Video%20Surveillance%20Guidelines%20(16%20March%202017).pdf>.

reassurance to parents. For example, Citizen Lab research over the course of 2015-2017 uncovered a number of significant security vulnerabilities across several parental monitoring and control applications. These apps were developed and marketed in response to a South Korean law that required all phones registered to minors come with monitoring and filtering apps installed. The Citizen Lab and its research partners concluded:

> In total we have released security audits of five Korean child monitoring apps (Smart Sheriff, Cyber Security Zone, Smart Dream, KT Olleh Kid Safe, Clean Mobile Plus). Across the audits we found that these apps were not designed with security or privacy in mind. The apps do not follow best security practices for data transmission, data storage, or user authentication. The results of our audits point to systemic security issues in child monitoring apps in Korea that are not isolated to a single developer or vendor.[439]

Spyware apps used in North America possess similar vulnerabilities. For example, the Citizen Lab assessed that FlexiSPY, mSpy, and Hoverwatch could potentially make a mobile device further susceptible to security vulnerabilities after the spyware app has been installed onto the device, through insecure software update models.[440]

Additionally, security flaws in Circle, a Disney device used to monitor and manage children's Internet use, meant that "a malicious attacker could gain various levels of access and privilege, including the ability to alter network traffic, execute arbitrary remote code, inject commands, install unsigned firmware, accept a different certificate than intended, bypass authentication, escalate privileges, reboot the device, install a persistent backdoor, overwrite files, or even completely brick the device."[441] Researchers found "critical security flaws" in children's smartwatches, "which could allow a potential attacker to take control of the apps, thus gaining access to children's real-time and historical location and personal details, as well

439 Fabian Faessler, et al, "Still Safer Without Another look at Korean Child Monitoring and Filtering Apps" *The Citizen Lab* (27 November 2017) <https://citizenlab.ca/2017/11/still-safer-without-kt-olleh-kidsafe-clean-mobile-plus/>; Ronald Deibert, "Korean Child Monitoring Applications: Insecure by Design," (11 September 2017) <https://deibert.citizenlab.ca/2017/09/insecure-by-design/> ("In short, what we found was — rather than protecting minor children — both applications actually put minor children, and their parents, at much greater risk than had they not used the applications in the first place."). See also the four-part series published by the Citizen Lab on Korean child monitoring and filtering apps: https://citizenlab.ca/2015/09/digital-risks-south-korea-smart-sheriff/.

440 For more details, see the assessment of security vulnerabilities of certain stalkerware apps in a report accompanying this one, published by the Citizen Lab, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry."

441 William Largent, "Vulnerability Spotlight: The Circle of a Bug's Life," *Talus Blog* (31 October 2017) <https://blog.talosintelligence.com/2017/10/vulnerability-spotlight-circle.html>.

as even enabling them to contact the children directly, all without the parents' knowledge."[442] Some transferred data overseas without encryption, and one of the watches also functioned as a covert listening device.[443]

Another child monitoring app, Family Orbit, "had an unsecured cloud server [potentially exposing] 281 GB worth of highly sensitive information affecting children potentially around the world."[444] Similarly, a spyware company named TeenSafe "leaked tens of thousands of accounts of both parents and children" by relying on an unprotected cloud server with no password, while also requiring users to turn off two-factor authentication (2FA) on their devices. Disabling 2FA thus made children's data particularly vulnerable to unauthorized access by someone who had obtained a child's Apple ID and password (stored in plaintext in TeenSafe's unsecured database).[445]

In short, international and Canadian law on children's privacy rights, the jurisprudence on monitoring children in schools, guidance from provincial privacy commissioners, the academic literature on the effects of parental surveillance on children, and documented repeated security leaks of children's data from monitoring software all suggest that even where stalkerware apps are genuinely confined to use with children, such usage raises a constellation of concerns, putting the legal and ethical legitimacy of these technologies into question. Moreover, the legal requirement to respect a child's privacy and autonomy increases in strength and overriding authority with the child's age and maturity. This recognition of children's rights and autonomy starkly highlights the degree to which it is even more so inappropriate to deploy the same spyware technologies and surveillance on targeted individuals who are adults.

442 ForbrukerRadet, "#WatchOut: Analysis of smartwatches for children," *ForbrukerRadet* (October 2017) <https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf>.

443 ForbrukerRadet, "#WatchOut: Analysis of smartwatches for children," *ForbrukerRadet* (October 2017) <https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf> at p. 3. See also, regarding a children's watch called Misafes "Kids Watcher": "These new attack vectors can not only be performed remotely (including capturing the IMEI remotely), but allow an operator to build up a global picture of the location of all the children. Combined with caller ID spoofing, this attack becomes really nasty." Alan Monie, "Tracking and snooping on a million kids", Pen Test Partners, Blog:Internet of Things (15 November 2018) <https://www.pentestpartners.com/security-blog/tracking-and-snooping- on-a-million-kids/>.

444 Beauceron Security Inc., "Hack highlights risks of spyware on children's devices," *Beauceron* (25 September 2018) <https://www.beauceronsecurity.com/blog/2018/9/19/spying-on-kids-back-fires>; Lorenzo Franceschi-Bicchierai, "Spyware Company Exposed '281 Gigabytes' of Children's Photos Online," *Motherboard* (30 August 2018) <https://motherboard.vice.com/en_us/article/ywk8gy/spyware-family-orbit-children-photos-data-breach>.

445 Zack Whittaker, "Teen phone monitoring app leaked thousands of user passwords," *ZDNet* (20 May 2018) <https://www.zdnet.com/article/teen-phone-monitoring-app-leaks-thousands-of-users-data/.

ii. Worker and Employee Privacy Rights in Canadian Law

Spyware that is intended to assist employers in tracking employee performance and enforcing company policies can also be repurposed to constitute stalkerware.[446] While limited employee monitoring is generally considered a legally and ethically permissible activity when compared to tracking and surveilling an intimate or former partner, the appropriateness of this practice may be more circumscribed than spyware companies generally assume or imply, in view of employees' privacy and related rights.

Focusing on employee privacy rights in the context of spyware is critical because employers or other individuals in the workplace can potentially abuse such tools. Numerous voyeurism cases in Canada, for example, involve inappropriate or illegal placement and usage of video surveillance in a workplace to record employees or customers in personal situations, such as using the restroom or changing clothes.[447] Managers have also made covert personal recordings of significantly younger female coworkers or subordinates at work, including of the individuals showering or using the bathroom.[448] It is not difficult to imagine that workplace-wide spyware, even if installed in good faith and in accordance with employee data protection laws, could be repurposed within the workplace for abusive purposes.

The general subject matter of employee and worker privacy constitutes its own significant body of law, which is beyond the scope of this report to comprehensively review. Instead, we simply note that employees do not leave their privacy rights at home or have them suspended while at their places of employment. While the particular context and circumstances surrounding employment and workplace-associated monitoring shapes the privacy analysis, the fact that someone is an employee does not mean they thereby forego their privacy rights or all expectations of privacy while at work or while completing activities outside of the workplace but in the course of their employment.

The Supreme Court of Canada has noted that, in the context of employees, "[a] reasonable though diminished expectation of privacy is nonetheless a reasonable expectation of privacy, protected by s. 8 of the *Charter*."[449] Employees retain

446 See, e.g., Rob Marvin, "The Best Employee Monitoring Software for 2019," *PC Mag* (11 October 2018) <https://www.pcmag.com/roundup/357211/the-best-employee-monitoring-software>.

447 See, e.g., *R. v. Bosomworth*, 2015 BCPC 7; *R. v. Payne*, 2014 BCPC 361; *R. v. Hamilton*, 2009 BCPC 381; and *R. v. Laskaris*, 2008 BCPC 130.

448 *R. v. Brandt*, 2013 MBPC 39; and *R. v. Muggridge*, 2015 NLPC 1314A00585.

449 *R. v. Cole*, 2012 SCC 53 at para. 9.

constitutional protection of their privacy even with respect to devices that belong to their employers, with the Court recognizing:

> Computers that are used for personal purposes, regardless of where they are found or to whom they belong, "contain the details of our financial, medical, and personal situations" (Morelli, at para. 105). This is particularly the case where, as here, the computer is used to browse the Web. Internet-connected devices "reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet" (*ibid*.).
>
> This sort of private information falls at the very heart of the "biographical core" protected by s. 8 of the *Charter*.[450]

The Court has further made clear that "[i]t is well settled that the search of cell phones, like the search of computers, implicates important privacy interests … [because they] may have immense storage capacity, may generate information about intimate details of the user's interests, habits and identity without the knowledge or intent of the user, [and] may retain information even after the user thinks that it has been destroyed [. . .]."[451]

Additionally, the Office of the Privacy Commissioner of Canada (OPC) provides guidelines to help employers balance their management needs with respect to employees' privacy rights. Most pertinent in the stalkerware context is that employers should collect, use, or disclose an employee's personal information with their knowledge and consent, and for appropriate purposes only. The employer is expected to disclose such surveillance and its rationale(s) to targeted employees. For example, multiple OPC decisions have established that employers must inform employees of video surveillance that occurs in the workplace, including its purpose.[452] In at least two cases, employers monitoring employees through web cameras and digital video surveillance contravened PIPEDA by lacking any appropriate purpose for the surveillance.[453]

450 *Ibid*. at paras. 47-48.

451 *R. v. Fearon*, 2014 SCC 77 at para. 51 (internal citations omitted).

452 Office of the Privacy Commissioner of Canada, "Bus terminal video surveillance is challenged by company employee," PIPEDA Case Summary #2009-001 (2009) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-001/>; *Office of the Privacy Commissioner of Canada*, "Employers subject to PIPEDA should inform employees about the existence of, and purpose for, video surveillance in the workplace," PIPEDA Case Summary #2015-001 (9 September 2015) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/ser/2015/s2015-001_0909/>.

453 Office of the Privacy Commissioner of Canada, "Surveillance of employees at work," PIPEDA Case Summary #2004-279 (2004) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-279/>; *Office of the Privacy Commis-*

At the provincial level, the British Columbia *Personal Information Protection Act* (PIPA), for instance, mandates that organizations must notify an employee—even if they are not required to obtain consent—if the employer is collecting or using the employee's personal information. The employer is only exempt from this requirement if the situation falls under a specific list of exceptions in sections 12 or 15 (such as if notifying the employee would compromise an investigation).[454]

In 2015, the District of Saanich, BC, was found to have installed spyware on employees' work computers without the employees' knowledge or consent.[455] The software carried out the following surveillance activities: captured automated screenshots every 30 seconds; monitored and logged all chat and instant messaging; logged all websites visited; retained a copy of every email; logged file transfer data; logged users' keystrokes; logged open and active program windows; and tracked the creation, deletion, renaming, or copying of every file. As a result, "the District collected all personal information that a user entered into their workstation."[456] The Office of the Information and Privacy Commissioner for BC (OIPC BC) launched an investigation and found the municipality noncompliant with the BC *Freedom of Information and Protection of Privacy Act* (FIPPA). The OIPC BC stated: "[E]mployees do not check their privacy rights at the office door. There is a right to privacy in the workplace, which has been upheld by Canadian courts and must be respected by public bodies as they consider what security controls are necessary to protect information in government networks."[457]

The right to privacy is intimately linked with the right to freedom of expression and the freedom of assembly and association. In his "Report on encryption, anonymity, and the human rights framework," the United Nations Special Rapporteur on freedom of expression, David Kaye, referred to privacy as a "gateway to the enjoyment of other rights, particularly the freedom of opinion and expression."[458]

---

sioner of Canada, "Employee objects to company's use of digital video surveillance cameras," PIPEDA Case Summary #2003-114(2003) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-114/>.

454 *Personal Information Protection Act*, SBC 2003, c 63, s. 13(3) and 16(3).

455 Elizabeth Denham, Information and Privacy Commissioner for BC, "Investigation Report F15-01: Use of Employee Monitoring Software by the District of Saanich," *Office of the Information & Privacy Commissioner of British Columbia* (30 March 2015) <https://www.oipc.bc.ca/investigation-reports/1775>.

456 *Ibid* at p. 5.

457 *Ibid* at p. 3. See also, Office of the Information & Privacy Commissioner for British Columbia, "Guidance Document: Employee Privacy Rights," *Office of the Information & Privacy Commissioner for British Columbia* (November 2017) <https://www.oipc.bc.ca/guidance-documents/2098>.

458 David Kaye, "Report on encryption, anonymity, and the human rights framework," *United*

In the employment context, privacy to express one's thoughts and opinions also can include a "zone of privacy" in which to associate and assemble with trusted others and where one has the freedom to engage in activities such as labour organizing or strategizing for collective rights. This nexus increases the importance to be placed on employees' privacy rights in the workplace, given the role such rights play as a precursor to meaningfully exercising other fundamental human rights.

Our brief review of Canadian employee privacy law offers one significant basis on which to distinguish spyware apps genuinely designed for employee monitoring from those implicitly or explicitly intended for intimate partner surveillance: whether or not the app makes it possible to engage in intrusive monitoring without the targeted person becoming aware of such monitoring. Relevant laws at the federal and provincial level suggest that employee surveillance and its rationale(s) generally must be disclosed to surveilled workers, in order to be legal. Based on our analysis, we conclude that there is little to no need for covert surveillance capabilities for employers to carry out employee monitoring that is effective for good-faith management purposes.

Information Box 16: Commercial Spyware and Nation-State Surveillance

The focus of this report is consumer spyware and stalkerware apps that private individuals use to surveil, monitor, and track other individuals. However, these apps constitute only one particular industry that is based on spyware, malware, and other forms of software that are designed and sold primarily for the purpose of surveilling and monitoring individuals. Separately, there exists an equally troubling commercial spyware industry that sells highly priced and highly sophisticated software to nation-states. This spyware is ostensibly meant to be used for legitimate aims of government; however, previous research by the Citizen Lab has revealed that spyware technology in this context has been deployed by autocratic governments against human rights activists, political dissidents, journalists, and lawyers representing victims of wrongful conduct by the state.[459]

Nations Office of the High Commissioner of Human Rights, A/HRC/29/32 (22 May 2015) <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx> at p. 7.

459 Companies such as NSO Group, Hacking Team, and Gamma International—based in Israel, Italy, and Germany / United Kingdom, respectively—sell such tools to governments, law enforcement, and intelligence agencies around the world, ostensibly for the purpose of electronic surveillance against threats to national security and criminal actors. See, e.g.: The Citizen Lab's series on the surveillance abuse linked to NSO Group's spyware in Mexico and elsewhere, including John Scott-Railton, et al, "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware," *The Citizen Lab* (20 March 2019) <https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/>; Bill Marczak, et al, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* (18 September 2018) <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>; and Bill Marczak, et al, "NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident," *The Citizen Lab* (31 July 2018) <https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/>.

For the most part, there is little overlap between the stalkerware app industry discussed in this report and the nation-state commercial spyware industry. The two industries and their respective products and services differ dramatically in many respects, including technical capabilities, software, operations, target market, infrastructure, resources, political positioning, and complexity. However, researchers and journalists have documented on at least two occasions spyware businesses that appear to have been involved in both industries.

For example, a research investigation by Amnesty International into StealthAgent—a spyware tool that was used to target a Pakistani human rights activist—concluded that StealthAgent shared technical features, code similarities, and employee and personnel connections with a stalkerware app of the kind studied in this report, known as TheOneSpy.[460] In another instance, Vice Motherboard reported that internal documents from the stalkerware company FlexiSPY indicated that the company may have contributed software, customer support, and staff to FinSpy, a nation-state spyware tool that the British-German spyware company Gamma subsequently sold to Bahrain.[461]

While in the above cases, governments may be purchasing spyware tools with a connection to particular stalkerware companies, journalists have also reported cases where state agents—specifically, in law enforcement and the military—appear to be using stalkerware apps in their own private lives.[462] Any such use would be deeply concerning, given the role of law enforcement actors in a justice system meant to serve victims and survivors of stalkerware abuse and related gender-based violence, abuse, and harassment, technology-facilitated or otherwise.

We do not draw further conclusions from these reports, but include them to highlight the reach of commercial spyware industries and wider range of associated issues, as part of the broader contextual background informing considerations of the stalkerware app industry that is the focus of this report.[463]

460 Amnesty International, "Human Rights Under Surveillance: Digital Threats Against Human Rights Defenders in Pakistan," *Amnesty International* (2018) <https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF> at p. 42-43.

461 Joseph Cox, "Meet FlexiSpy, The Company Getting Rich Selling 'Stalkerware' to Jealous Lovers," *Motherboard* (21 April 2017) <https://motherboard.vice.com/en_us/article/aemeae/meet-flexispy-the-company-getting-rich-selling-stalkerware-to-jealous-lovers> ("According to a 2011 document, FlexiSPY may have provided British-German company surveillance Gamma, known for its FinFisher spyware, with a piece of software called 'Cyclops', as part of Gamma's 'FinSpy' product. . . . The document also indicates that staff from the two companies may have physically worked on the same projects").

462 Joseph Cox, "Military, FBI, and ICE Are Customers of Controversial 'Stalkerware'" (23 February 2018), online: Vice *Motherboard* <https://motherboard.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware>. Intelligence officers reportedly perpetrate a similar form of technology-facilitated abuse by spying on individuals in their personal lives, not through stalkerware apps but through surveillance capabilities accessible at work. This practices appears to have been prevalent enough to have garnered its own term: "LOVEINT." Alina Selyukh, "NSA staff used spy tools on spouses, ex-lovers: watchdog," *Reuters* (27 September, 2013) <https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdogidUSBRE98Q14G20130927>; Letter from Dr. George Ellard (Inspector General, National Security Agency Central Security Service) to Senator Charles E. Grassley, 11 September 2013 <https://www.nsa.gov/news-features/press-room/statements/assets/files/grassley-letter.pdf>.

463 See also Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto), Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović (November 2017) <https://citizenlab.ca/wp-con-

B. Ability of Current Laws to Respond to Harms Arising from Stalkerware

Technology-enabled abuse often replicates the historic and traditional forms of intimate partner violence and abuse, including harassment, threatening, stalking, and control through fear-induced coercion. As a result, many Canadian laws that already criminalize domestic abuse, harassment, and serious invasions of privacy also already prohibit many forms of technology-facilitated abuses, including the use, sale, and/or distribution of spyware. And yet, available data about the prevalence of intimate partner surveillance and technology-facilitated abuse and harassment in Canada suggests there is a measurable gap between what the law dictates about such conduct and whether legal remedies are readily available to victims in practice. There are no reported criminal prosecutions in Canada for cases involving mobile phone spyware apps used for intimate partner surveillance. The analysis in this section focuses on two key impediments to the availability of legal remedies for victims of stalkerware: i) gaps in law enforcement and ii) victim-focused responses to stalkerware abuse.

i. Law Enforcement Gaps: The Need for Socio-Cultural and Technical Training and Resources

One of the principal obstacles to legal protection in Canada is lack of awareness, training, and resources for law enforcement authorities and regulators. Training around the lawfulness of using stalkerware and around the criminal and regulatory context that surrounding creating, selling, or facilitating the sale of spyware is absolutely necessary. Of course, the pace of technological change creates challenges for law enforcement, as police services and regulators must develop the investigative training and methods to effectively respond to phenomena of technology-facilitated harm. However, experience also suggests that law enforcement may often "lack the imagination or the training to extrapolate existing offences and see how they could work in an online or technology-enabled environment."[464]

tent/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf> at p. 17 ("[T]he commercial entities involved in tools used to target human rights defenders and those involved in developing stalkerware that jeopardizes the safety of women and girls are intimately interlinked—and in some cases, may even be one and the same").

464 David Fraser, quoted by Patrick Cain: "Is a stalker spying on you through your phone? Here's what to look for," *Global News* (29 September 2016) <https://globalnews.ca/news/2966238/is-a-stalker-spying-on-you-through-your-phone-heres-what-to-look-for/>. For example, legal tools that were available were not employed in the police response to the Rehtaeh Parsons case: Murray D Segal, "Independent Review of the Police and Prosecution Response to the Rehtaeh Parsons Case," (8 October 2015) <https://novascotia.ca/segalreport/Parsons-Independent-Review.pdf> at p. v ("The investigator had grounds to believe that at least some of the boys either had the photograph–child pornography–on their phones or had transmitted it. Search warrants

Criminal, civil, and regulatory laws already circumscribe stalkerware-related conduct in a number of respects. Once one maps the essential elements of those laws to the specific actions and actors involved in the use, development, and sale of stalkerware, the path is apparent, regardless of the technological landscape. The Internet and digital environments are not law-free zones. The analysis throughout this report described a range of criminal, civil, and preventative legal options that exist for individuals who are—or who fear they are—the targets of technology-facilitated harassment or stalking. It is the corresponding duty of law enforcement, regulators, and the justice system to protect individuals who are victimized by crime or experience serious harmful conduct, even where enforcing the law is challenging.

For many instances of technology-facilitated harassment and abuse, law enforcement agencies should recognize what has already been recognized under the traditional form of criminal harassment: an offender's isolated instances of conduct mustn't be an officer's sole focus to understand the gravity of the impact on the safety and security of the target of harassment. Intimate partner violence and gender-based abuse come in many forms, and multiple forms may operate in tandem to cumulatively erode the autonomy, dignity, and sense of safety of the targeted person. Technological manifestations of these patterns of abuse are no exception.

The normative framing offered by Dragiewicz, et al, is useful here, as the term "technology facilitated coercive control" encompasses "the technological and relational aspects of abuse in the specific context of coercive and controlling intimate relationships." Domestic violence, which is a "pattern of coercive and controlling behaviours, often backed by the threat of violence,"[465] contextualizes online misogyny and abuse. And yet, online manifestations of domestic violence are also unique, because technology can enable domestic violence perpetrators to "expand the reach of control and abuse, disrupting women's efforts to protect themselves."[466]

Those tasked with enforcing the law must have access to training and resources to equip them with the technological tools to identify and respond to stalkerware technology. However, such training must also enable officers with socio-cultural

could have been obtained to seize those devices at the earliest opportunity.").

465 Molly Dragiewicz, et al, "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms," (2018) 18(4) *Feminist Media Studies* 609 <https://www.tandfonline.com/doi/abs/10.1080/14680777.2018.1447341?journalCode=rfms20&> at p. 610

466 *Ibid* at p. 618.

training to ensure that they recognize and respond to technology-facilitated abuse as a dangerous form of wrongdoing in its own right.[467] In effect, training must not just be tool-focused but, instead, extend to education around the unique socio-cultural elements of intimate partner violence and abuse. Such training needs to be largely principle-based, so both offline and online harms can be registered, accounted for, and addressed.

Socio-cultural education is particularly important for law enforcement officers to receive because they play an important role in framing a case before it moves through the criminal courts. The police service responsible for investigating an offender performs this 'framing' role because the investigating officer chooses which criminal offences to lay against an offender. For example, in cases involving both stalkerware abuse and non-technological offences such as domestic assault, the officer could choose to lay only a charge of assault because assault may be easier to prosecute than offences involving technology. There is a risk, however, in treating those cases as purely "assault" cases (by charging the defendant with the offence of assault). Charging only traditional offences such as assault leaves individuals who are victimized by non-traditional forms of offences with a justice system that is less prepared to appropriately respond to the harm done. Put another way, if education does not empower officers to consider the full range of potential charges to a range of offences, then a significant number of offences—such as the use of stalkerware—might go uninvestigated and uncharged. Such a consequence would disenfranchise targeted persons from the full potential remediating capacity of law while letting a subset of serious criminal activities go without the disciplining power of law.

Information Box 17: What If Law Enforcement Authorities Do Not Pursue the Investigation or Complaint?

Complainants and victims of technology-facilitated harassment and stalking should reach out for support to women's shelters and community support organizations for help, and/or contact legal counsel if a complaint is not investigated or acted upon by their local police service. Independent police oversight bodies, such as Ontario's Office of the Independent Police Review Director (OIPRD), may also receive complaints from the public with regard to the conduct of the police.

467 Diana Freed, et al, "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders," (2017) 1 *CSCW ACM on Human-Computer Interaction* 46 <https://www.ipvtechresearch.org/pubs/a046-freed.pdf>.

ii. The Need for Offender-Focused Responses and Remedies

Persons targeted by technology-facilitated stalking, harassment, and abuse are often told to stop using their phones, close their social media accounts, or get off the Internet to "solve" technology-facilitated abuse. However, it is not the targeted person's engagement with technology that is the source of the abuse. Gender-based violence and harassment is an overarching, socially constructed ill that takes many forms, and while the seismic shift in the way that individuals interact with technology has created new areas where they are vulnerable to abuse, technology itself is not the problem.

The legal system in Canada renounces all forms of victim-blaming that amount to a contention, for example, that one's choice of clothes or participation in social activity imputes an acceptance of risk of sexual assault or sexual harassment. The construction of responsive social and legal policies to stalkerware technology must likewise reject solutions that implicitly or expressly engage in forms of victim-blaming. A decision to avoid using certain technologies will not guarantee the cessation of a pattern of violence, abuse, or harassment. Disengagement can also further isolate targets from networks of support or prevent them from accessing help. For many individuals, including persons in at-risk and disenfranchised groups such as those in the LGBTQ2+ context, access to technology is empowering and an important resource for supportive social networks.[468] Changing a phone number, replacing a phone, or creating a new email account may be appropriate security strategies in some contexts, but they do not constitute appropriate policy solutions to the issues associated with technology-facilitated abuse and harassment.

Having the freedom to participate in digital life in the modern age is a fundamental component of the freedoms of expression, autonomy, and liberty. The use of electronic mediums is increasingly an essential means of accessing equality-enhancing services and resources. Electronic apps and devices are now often designed to support mental health; improve the accessibility of cities; and support a range of motor, visual, speech, and auditory impairments.

As privacy, equality, and the freedom of expression are all designed to enable individual autonomy, dignity, and self-actualization, a solution to technology-facilitated violence and harassment should not require victims to abstain from

468 See Robert T. Cserni & Ilan Talmud, "To Know that you are Not Alone: The Effect of Internet Usage on LGBT Youth's Social Capital," in *Communication and Information Technologies Annual (Studies in Media and Communications), Volume 9* (Bringley, UK: Emerald Group Publishing Limited, 2015) at p.161 - 182.

electronic activities that otherwise serve to enhance their liberty and enable them to flourish and thrive in a free society. Policy and legal responses to such harassment should not therefore presuppose that it is appropriate to ask victims to choose between their physical and psychological safety, personal freedom, and autonomy.

Part 6: Recommendations

Based on our legal analysis in Parts 1 through 5, we conclude in Part 6 with proposed recommendations for how Canadian law and policy may more effectively address the problem of stalkerware and stalkerware-facilitated abuse. The proposed recommendations are aimed at a variety of actors across the Canadian legal system, including those who work in the criminal and family justice systems, federal and provincial legislators and policymakers, the Office of the Privacy Commissioner of Canada, and technology sector businesses, such as app intermediaries. Part 6 reiterates and presents together all of the recommendations that resulted from and are embedded in our analysis throughout earlier sections of the report.

A. Recommendations for Actors in Criminal and Family Justice Systems

Recommendation 1: Judicial, governmental, police, and institutional actors that have decision-making authority with respect to cases that involve stalkerware and related forms of technology-facilitated gender-based violence should ensure that legal and policy responses focus on the responsibility of stalkerware operators and companies, rather than disempowering victims by asking them to remove themselves from online environments as a solution.

Recommendation 2: Governmental and law enforcement institutions should develop public legal education materials on stalkerware and other forms of technology-facilitated violence, abuse, and harassment. Public legal education with respect to types of criminal and civil sanctions for technology-facilitated gender-based violence is an important part of developing legal and policy responses to these forms of abuse. Ignorance of the law is not a defence in the Canadian justice system. Stalkerware operators and stalkerware companies are presumed to be aware of the law and cannot avoid liability simply because they are not aware of them. Nevertheless, public legal education is an important preventative measure to ensure that perpetrators, potential perpetrators, and the general public understand the harms associated with stalkerware technology; the importance of human rights, including women's rights relating to autonomy, consent, equality, and privacy; and the criminal and legal consequences perpetrators risk for using stalkerware technology.

Recommendation 3: Police services across Canada should mandate regular, expert-led training for law enforcement on responding to reports of the use of stalkerware and related forms of technology-facilitated violence, harassment, and abuse. Major institutional barriers within law enforcement agencies often limit their ability to effectively respond to complaints of gender-based violence, abuse, and harassment more generally—whether online or offline. Though appeals for greater investigative powers are commonplace, it is unclear that police forces consistently make use of the full range of existing powers at their disposal to address threats to women and girls online.

Recommendation 4: Family law practitioners, family courts, support workers, child protection workers, and legal aid lawyers should receive education with regard to the availability and harms of consumer-level surveillance software in Canada. Family law courts should continue to presumptively rule illegally obtained evidence to be inadmissible. Referrals should also be made to law enforcement authorities in circumstances where the Court becomes aware of the fact that spyware has been deployed against another person.

B. Recommendations for Federal and Provincial Lawmakers and Government

Recommendation 5: Provincial and federal lawmakers should modernize existing legislation to ensure that it remains effective and inclusive in light of gender-based harm associated with technological change. For provincial governments in particular, law reform through the creation and/or modernization of statutory torts would provide greater clarity about the availability of remedies in the civil justice system for sexual harassment, harassment, stalking, and invasions of privacy. While this modernization effort would include law reform to provide meaningful access to remedies for traditional and non-technological forms of gender-based harm, lawmakers should pay particularly close attention to new and potential forms of technology-facilitated abuse, such as stalkerware, deep-fake sexual images, and the repurposing of GPS trackers or smart home devices to facilitate harassment and abuse.

Recommendation 6: Federal lawmakers should examine and clarify the criminal offences that directly relate to the use and sale of invasive spyware programs in Canada. In particular, lawmakers should clarify the computer-based offences under the *Criminal Code* (unauthorized use of a computer under section 342.1

and mischief in relation to computer data under section 430(1.1)), and the related offence under section 342.2 that criminalizes commercial activity in relation to the spyware programs that are designed or adapted primarily to commit the offences under sections 342.1 or 430. Amendments to these offences should be considered in order to provide more clarity regarding the legality of the purchase and sale of covert spyware apps (even those marketed for the purpose of covert monitoring of children), and to ensure that consumer-level spyware vendors do not have the financial incentive to provide false or misleading information to consumers about the (il)legality of spyware apps.

Recommendation 7: Provide the Office of the Privacy Commissioner of Canada and provincial counterparts with greater enforcement powers. The Office of the Privacy Commissioner of Canada and provincial counterparts must be given enforcement powers that are appropriate to address the sale of stalkerware apps in violation of PIPEDA. For example, the OPC should have the ability to impose administrative monetary penalties, including penalties that are high enough to act as effective deterrence. The OPC and provincial privacy commissioners, where they are not already able, should also be empowered to issue direct orders and enforce compliance against entities found to have violated PIPEDA or substantially similar legislation, including through the sale of stalkerware products and services. Such powers may be similar to those that data protection authorities can exercise under the GDPR.

Recommendation 8: Federal and provincial governments should fund further research and studies regarding the prevalence of intimate partner surveillance and technology-facilitated intimate partner violence, abuse, and harassment in Canada. Such data and further insights would help to advance critical discussion, improve evidence-based policy reform, and enable the law to respond more effectively to pre-existing and emerging issues in the area of stalkerware-enabled abuse, technology-facilitated intimate partner violence, abuse, and harassment, and technology-facilitated gender-based violence more broadly.

Recommendation 9: Federal and provincial governments should invest in greater resources, education, and support for front-line, anti-violence workers to develop greater technical literacy. The academic literature and experiences of community support workers are clear: lack of technological awareness, training, and literacy among front-line workers are a major barrier to providing more effective support to victims of technology-facilitated gender-based violence. The government should invest greater funding in this area to build front-line workers'

capacity to more effectively recognize and respond to signs of, and harms from, technology-facilitated gender-based violence.

C. Recommendations for the Office of the Privacy Commissioner of Canada

Recommendation 10: The Office of the Privacy Commissioner of Canada should open investigations into stalkerware companies that are known to operate and impact individuals in Canada. Our analysis of the data protection and privacy practices of stalkerware businesses concluded that such businesses, at least where intimate partner spyware and repurposed dual-use spyware is involved, almost certainly violate PIPEDA in one or more ways. The OPC should fulfill its mandate to uphold and enforce the Act, and should protect potential or future targets of stalkerware, by opening an investigation and bringing regulatory scrutiny to this industry.

Recommendation 11: The Office of the Privacy Commissioner of Canada should establish cross-jurisdiction agreements to pursue stalkerware businesses that are in a different country from their users and victims. The OPC should establish or work within pre-existing bilateral or multilateral agreements with foreign privacy regulators, such as the Global Privacy Enforcement Network, to pursue stalkerware businesses across borders where they have a real and substantial connection to Canada. Examples of prior successful joint efforts include the Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner[469] and investigation of a New Zealand company that reused millions of Canadian users' Facebook profiles.[470]

Recommendation 12: The Office of the Privacy Commissioner of Canada should issue a statement expressly establishing that commercial activity that facilitates the sale of stalkerware is considered a "No-Go Zone" under section 5(3) and the Guidance on Inappropriate Data Practices. Stalkerware businesses likely fall into at least three of the six No-Go Zones that the Commission has established at

469 Office of the Privacy Commissioner of Canada, "Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner," PIPEDA Report of Findings #2016-005 (22 August 2016) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/>.

470 Office of the Privacy Commissioner of Canada, "Company's re-use of millions of Canadian Facebook user profiles violated privacy law," PIPEDA Report of Findings #2018-002 (12 June 2018) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-002/>.

time of writing. The OPC should publicly confirm that selling stalkerware apps such as intimate partner spyware and repurposed dual-use spyware does constitute an inappropriate purpose under PIPEDA and violates section 5(3).

Recommendation 13: The Office of the Privacy Commissioner of Canada and provincial privacy commissioners should clarify that section 4(2)(b) of PIPEDA and the equivalent provision in substantially similar provincial legislation should be interpreted to exclude individuals alone acting for a "personal or domestic" purpose, and should not be interpreted to exclude entities acting under circumstances where an individual has retained them as businesses that provide commercial services in order to achieve that individual's personal purpose. Without such clarification, section 4(2)(b) may provide a loophole through which spyware businesses (and many other types of businesses) may claim to fall outside of PIPEDA's purview. This may be the case despite the fact that spyware apps collect, use, and disclose personal information in the course of commercial activities that are core to their business model, while moreover violating PIPEDA's fundamental requirements such as the need to obtain meaningful consent.

C. Recommendations for App Developers, Technology Companies, and App Intermediaries

Recommendation 14: Technology companies and the software development sector must take seriously their corporate social responsibility—as required by the United Nations *Guiding Principles on Business and Human Rights*—with respect to the harmful impacts and implications of stalkerware apps and similar types of technologies used to perpetuate gender-based and intimate partner violence, abuse, and harassment; app developers and technology companies must respond accordingly through self-regulation, education, training in ethics, human rights, and the needs and perspectives of marginalized communities and vulnerable individuals, or other meaningful initiatives. Our review of Canadian laws and regulations concerning the creation and development of stalkerware revealed that little stands in the way of creating harmful products and services such as intimate partner spyware. Legal responses such as a product liability, dangerous product, or class action lawsuit may serve as a deterrent, but could only address harm after the fact, and would not necessarily prevent it. The lack of binding laws and regulations in technology development to ensure ethical conduct or prioritize human rights places greater onus on app developers themselves, and increases reliance on the technology sector's corporate social responsibility, to

mitigate or prevent harmful technologies at the creation, design, and development stage. For example, employee monitoring apps genuinely intended to serve good-faith management purposes have no need for an "invisibility" feature, and should not be designed to offer such; excluding this feature and building in mandatory just-in-time and persistent notifications would reduce the chances of such an app being repurposed into stalkerware for covert intimate partner surveillance. App developers and technology companies should routinely take such considerations regarding human rights and historically marginalized groups into account in the course of their work and business activities, as stated in the UN Guiding Principles.

Recommendation 15: App stores and online intermediaries should proactively and systematically enforce their policies and developer agreements against stalkerware apps and their developers. App stores that have not already done so should explicitly ban apps with spyware functionalities from their platforms. Specifically, app stores should ban apps that are designed to be self-concealing and "undetectable," at the app review stage, and ban similar apps that are already on their platforms. Upon banning an abusive app, app store companies should engage in a public recall process, including pushing notifications to mobile devices that have the banned app installed. Moreover, all such intermediaries should more thoroughly and systematically enforce their own policies and developer agreements with respect to these apps, perhaps by regularly conducting a full app store sweep of the sort that Google and Apple engaged in prior to the GDPR enforcement deadline. These sweeps should include seeking out spyware apps that are available to download or purchase from an app store through a search on the open Internet, such as Chatterjee, et al, conducted. Where stalkerware apps overtly fall into the dual-use category, app stores should conduct regular audits to ensure that such apps are not being predominantly sold, marketed, or used for the purpose of stalkerware abuse.

Recommendation 16: App stores should make clear in all relevant policies and developer agreements that the protected "user" with respect to data protection, privacy, security, consent, and malicious behaviour means the *person whose data is collected*, even if that person was not the app purchaser. As many policies are currently written, the "user" may be interpreted to refer to the stalkerware operator rather than their targeted victim. The term "device owner" also may not appropriately protect the interests of the person whose data is being collected because in an abusive relationship, the operator can own the target's device as a means of financial or communications control. The most effective approach would be for app stores, online platforms, and third-party download

sites to expressly specify that their data protection, privacy, consent, malicious behaviour, and related policies and terms of developers' agreements meant to protect users apply to *any individual whose data, device, or activity is being tracked, monitored, collected, or disclosed by the app*, even if they are not the app purchaser, the primary app "user," or the owner of the device where the app is installed.

Conclusion

Despite the prevalence of technology-enabled intimate partner violence, abuse, and harassment, and despite increasing recognition of stalkerware apps and related issues by academics, security researchers, gender equality rights advocates, and journalists, the legality of the creation, sale, and use of consumer-level spyware apps has not yet been closely considered by Canadian courts, legislators, or regulators. Few reported cases involving spyware-enabled intimate-partner surveillance (IPS) have ever appeared in Canadian courts, and spyware companies that profit from the sale of these apps appear to operate in the Canadian marketplace more or less unhindered by criminal or regulatory law enforcement.

In this report, we canvassed a range of legal and policy issues that apply to the use, creation, sale, and third-party distribution of stalkerware apps, which also include certain types of spyware apps. We assessed the legality of stalkerware and spyware apps under Canadian criminal and civil law, tort law, product liability law, privacy and data protection law, consumer protection law, intermediary liability law, and intellectual property law. Our analysis found that the creation, use, and sale of spyware apps, which enable either covert or coerced surveillance of a targeted individual through their mobile device, have the potential to violate numerous criminal, civil, privacy, and regulatory laws in Canada.

We conclude, on the whole, that current Canadian law appears theoretically adequate to addressing stalkerware-facilitated violence and abuse. For example, the violence, abuse, and harassment perpetrated by a stalkerware operator would likely violate one or more criminal offences, such as criminal harassment and intimidation. Likewise, Canadian privacy and data protection legislation already outlaws the unethical practices in which stalkerware businesses engage. Select areas of legal uncertainty remain, however, and these areas of law, for the purpose of remedying and preventing the harms of stalkerware-facilitated abuse, would benefit from explicit clarification from regulators, the courts, or Parliament.

While the law may suffice in theory, we conclude from our analysis that there is a significant gap between what the law dictates about stalkerware-related conduct and whether legal remedies are available to victims in practice. This appears largely due to the lack of either, or both, socio-cultural and technological awareness, training, literacy, and resources regarding technology-facilitated gender-based violence, on the part of law enforcement officers, lawyers, front-line support workers, the courts, and policymakers. Given spyware technology's inherent dangers, invasive

capabilities, and the documented association between stalkerware apps and intimate partner violence, abuse, and harassment, as well as gender-based violence and abuse, more must be done to address stalkerware-facilitated abuse and provide genuine remedy to targeted individuals.

Stakeholders and decision-makers must ensure that any proposed responses to stalkerware-facilitated abuse are focused on the perpetrator, rather than the victim, of the abuse. Targets of technology-facilitated gender-based abuse are often told to remove themselves from technology and digital spaces, such as getting rid of their mobile devices and deleting online social media accounts. However, targeted individuals should not have to sacrifice their ability to participate equitably and fully in public and private life—online and offline, where the distinction is increasingly thin—in order to also enjoy physical and psychological safety and security.

A wide range of actors and stakeholders in Canada's various legal regimes have a role to play in creating a meaningful "web of constraints" that would prevent further harms and abuses from stalkerware. These measures must be available both in theory and in practice. Likewise, those in decision-making positions in the public and private sector must reinforce—in theory and in practice—laws, policies, and private sector agreements concerning privacy, consent, data protection, device security, malicious behaviour, and abuse. It is not enough to have laws and policies in place that outlaw stalkerware apps and their unethical uses or business practices. A constellation of proactive responses, which must also be socio-culturally and technologically informed, are required to implement and enforce those laws and policies in a manner that effectively prevents and mitigates harms arising from stalkerware, intimate partner surveillance, and related technology-facilitated gender-based violence, abuse, and harassment.

Appendix A: Digital Security Guides and Resources

Various non-governmental organizations or research institutions have created numerous publicly available resources to help individuals take steps to protect their digital security, and we provide a selection of these resources below. Please note that these resources might become outdated over time. Moreover, strategies to combat technology-facilitated abuse and to prevent individuals from being harmed by stalkerware must focus on the role and responsibilities of stalkerware operators, stalkerware companies, and stalkerware distributors. The onus must not be on victims or potential victims to avoid becoming targets of harm or to secure themselves from technology-facilitated violence, abuse, or harassment.

Access Now

- Digital Security Helpline: https://www.accessnow.org/help/
  This organization advises that it offers 24/7 services in the following nine languages: English, Spanish, French, German, Portuguese, Russian, Tagalog, Arabic, and Italian.

Chayn

- Do It Yourself Online Safety: https://chayn.co/safety/

Citizen Lab

- Security Planner: https://securityplanner.org/

Crash Override Resource Centre

- Account Security 101: http://www.crashoverridenetwork.com/accountsecurity.html
- Talking to Family and Police: www.crashoverridenetwork.com/familyandpolice.html

Electronic Frontier Foundation

- Surveillance Self-Defence: https://ssd.eff.org/

HACK*BLOSSOM

- DIY Cybersecurity for Domestic Violence: https://hackblossom.org/domestic-violence/
- DIY Guide to Feminist Cybersecurity: https://hackblossom.org/cybersecurity/

IPV Tech Research

- IPS App Mobile Device Scanner: https://www.ipvtechresearch.org/post/software/
  Researchers at Cornell Tech, Cornell University, and New York University, who are studying how to improve digital safety and privacy for victims of intimate partner violence, have made an open source phone scanner to detect spyware on Android or iOS mobile devices.

Tactical Technology Collective and Frontline Defenders: Security in a Box

- Keep Your Digital Communication Private: https://securityinabox.org/en/guide/secure-communication/
- Protect Your Device from Malware and Phishing: https://securityinabox.org/en/guide/malware/
- Use Your Smartphone as Securely as Possible: https://securityinabox.org/en/guide/smartphones/
- Create and Maintain Strong Passwords: https://securityinabox.org/en/guide/passwords/

Take Back the Tech

- Safety Toolkit: https://www.takebackthetech.net/be-safe/safety-toolkit
- Strategies against Cyberstalking: https://www.takebackthetech.net/be-safe/cyberstalking-strategies

Women's Services Network (WESNET)

- Mobile Spyware: Identification, Removal, and Prevention: https://techsafety.org.au/resources/resources-women/mobile-spyware-identification-removal-prevention/

Appendix B: Select Academic, Policy, and Investigative Literature and Resources Relating to Stalkerware

Academic Literature

Aghtaie, Nadia, et al, "Interpersonal Violence and Abuse in Young People's Relationships in Five European Countries: Online and Offline Normalisation of Heteronormativity," (2018) 2 *Journal of Gender Based Violence* 293 <https://research-information.bristol.ac.uk/en/publications/interpersonal-violence-and-abuse-in-young-peoples-relationships-in-five-european-countries(fbecb658-5e98-4dd1-abad-36f0de1a16bc).html>

Chatterjee, Rahul, et al, "The Spyware Used in Intimate Partner Violence," (2018) *IEEE Symposium on Security and Privacy* 441 <https://www.ipvtechresearch.org/pubs/spyware.pdf>

Citron, Danielle Keats, "Spying Inc.," (2015) 72 *Wash & Lee L Rev* 1243 <https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/7/>

Citron, Danielle Keats, "Sexual Privacy," forthcoming in *Yale LJ* (2019) on Digital Commons@UM Carey Law <https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2604&context=fac_pubs>

Clevenger, Katherine Fisher, "Spousal Abuse through Spyware: The Inadequacy of Legal Protection in the Modern Age," (2008) 21(1) *Journal of the American Academy of Matrimonial Lawyers* 653 <http://aaml.org/library/journal-of-the-american-academy-of-matrimonial-lawyers/volume-21-2008-number-1>

Cooligan, Katherine & Daniel Hohnstein, "'Intruding Upon the Seclusion of Personal Email' — What the Common Law Tort for the Invasion of Privacy Might Mean for Snooping Spouses and the Electronic Evidence that they Obtain," (2014) 34 *CFLQ* 135 <https://blg.com/en/News-And-Publications/Documents/The_Seclusion_of_Personal_Email_-_CFLQ_JUL2014.pdf>

Dimond, Jill, Casey Fiesler & Amy Bruckman, "Domestic Violence and Information Communication Technologies," (2011) 23 *Interacting with Computers* 413 <https://academic.oup.com/iwc/article-abstract/23/5/413/656474>

Dragiewicz, Molly, et al, "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms," (2018) 18(4) *Feminist Media Studies* 609-625 <https://www.tandfonline.com/doi/abs/10.1080/14680777.2018.1447341?journalCode=rfms20&>

Douglas, Heather & Mark Burdon, "Legal Responses to Non-Consensual Smartphone Recordings in the Context of Domestic and Family Violence," (2018) 41(1) *UNSW Law J* 157 <http://www.austlii.edu.au/au/journals/UNSWLJ/2018/7.html>

Douglas, Heather, Bridget Harris & Molly Dragiewicz, "Technology-Facilitated Domestic and Family Violence: Women's Experiences," (2019) 59 *The British Journal of Criminology* <https://academic.oup.com/bjc/advance-article-abstract/doi/10.1093/bjc/azy068/5281174?redirectedFrom=fulltext>

Freed, Diana, et al, "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology," (2018) *CHI 18* 67 <https://www.ipvtechresearch.org/pubs/stalkers-paradise-intimate.pdf>

Freed, Diana, et al, "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders," (2017) 1 *CSCW ACM on Human-Computer Interaction* 46 <https://www.ipvtechresearch.org/pubs/a046-freed.pdf>

Harkin, Diarmaid, Adam Molnar & Erica Vowles, "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," (2019) 00 *Crime Media Culture* 1 <https://journals.sagepub.com/doi/pdf/10.1177/1741659018820562>

Levy, Karen, "Intimate Surveillance," (2015) 51 *Idaho Law Review* 679 <https://www.uidaho.edu/-/media/UIdaho-Responsive/Files/law/law-review/articles/volume-51/51-3-levy-karen-ec.pdf?la=en&hash=E549D503BFE8222484A64883907F4AD27B4435E8>

Marganski, Alison & Lisa Melander, "Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression

Experiences and its Association with In-person Dating Violence," (2018) 33 *Journal of Interpersonal Violence* 1071 <https://journals.sagepub.com/doi/abs/10.1177/0886260515614283?journalCode=jiva>

Marques, Diogo, et al, "Non-Stranger Danger: Examining the Effectiveness of Smartphone Locks in Preventing Intrusions by Socially-Close Adversaries," (2018) *USENIX Symposium on Usable Privacy and Security (SOUPS)* <https://pdfs.semanticscholar.org/7356/56925902ac5109606979920f08787dc30ad4.pdf>

Southworth, Cynthia, et al, "Intimate Partner Violence, Technology, And Stalking," (2007) 13 *Violence Against Women* 842 <https://journals.sagepub.com/doi/10.1177/1077801207302045>

Vasiu, Ioana & Lucien Vasiu, "Light My Fire: A Roentgenogram of Cyberstalking Cases," (2016) 40 *American Journal of Trial Advocacy* 41 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2906170>

Woodlock, Delanie, "The Abuse of Technology in Domestic Violence and Stalking," (2016) 23(5) *Violence Against Women* 584

Resources, Guides, and Policy Reports

BC Society of Transition Houses, "Canadian Legal Remedies for Technology-Enabled Violence Against Women," *BC Society of Transition Houses* (2013) <https://bcsth.ca/publications/canadian-legal-remedies-technology-enabled-violence-women/>

Perry, Jennifer "Digital stalking: A guide to technology risks for victims," *Network for Surviving Stalking and Women's Aid Federation of England* (2012) <http://www.domesticviolence.co.uk/wp-content/uploads/2012/05/Digital_stalking_A_guide_to_technology_risks_for_victims_2012.pdf>

Carson, Angelique, "Where Domestic Violence and Technology Collide," *International Association of Privacy Professionals* (2013) <https://iapp.org/news/a/where-domestic-violence-and-technology-collide/#>

Electronic Privacy Information Center, "Domestic Violence and Privacy" <https://www.epic.org/privacy/dv/>

Cericola, Rachel & Kaitlyn Wells, "How to Keep Your Smart-Home Technology Secure From Domestic Abusers," *The Wirecutter* (October 23, 2018) <https://thewirecutter.com/blog/keep-your-smart-home-secure-from-domestic-abusers/>

Elliott, Ame, "Empowering Abuse Through UX," *Our Data Ourselves* <https://ourdataourselves.tacticaltech.org/posts/empowering-abuse/>

Government of Canada, Department of Justice, "Stalking is a crime called criminal harassment," <https://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/stalk-harc/har.html>

Privacy International, Gender and Privacy, "From Oppression to Liberation: Reclaiming the Right to Privacy," *Privacy International* (November 2018) <https://privacyinternational.org/sites/default/files/2018-11/From%20oppression%20to%20liberation-reclaiming%20the%20right%20to%20privacy.pdf>

Tanczer, Leonie, et al, "Gender and IoT Research Report: The rise of the Internet of Things and implications for technology-facilitated abuse," *PETRAS IoT Hub, Privacy International & London VAWG Consortium* (November 2018) <https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf>

Sample Media Coverage of Stalkerware

Motherboard, When Spies Come Home: A multi-part investigative series about the powerful surveillance software ordinary people use to spy on their loved ones (2017-2019) <https://motherboard.vice.com/en_us/topic/when-spies-come-home>

Nellie Bowles, "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse," *The New York Times* (23 June 2018) <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>

Takara Small, "How Smart Home Systems & Tech Have Created A New Form Of Abuse," *Refinery29* (9 January 2019) <https://www.refinery29.com/en-ca/2019/01/220847/domestic-abuse-violence-harassment-smart-home-monitoring>

Alan Feuer, “Drug Kingpin Used Spyware to Monitor His Wife and Mistress, Jurors Told,” *The New York Times* (9 January 2019) <https://www.nytimes.com/2019/01/09/nyregion/el-chapo-trial.html>

Keegan Hamilton, “El Chapo’s Lawyers Want to Suppress Evidence from Spyware Used to Catch Cheating Spouses,” *Vice News* (11 July 2018) <https://news.vice.com/en_us/article/zmkv3y/el-chapos-lawyers-want-to-suppress-evidence-from-spyware-used-to-catch-cheating-spouses>

Kate Knibbs, “How the Hell Are These Popular Spying Apps Not Illegal?,” *Gizmodo* (30 January 2015) <https://gizmodo.com/how-the-hell-are-these-popular-spying-apps-not-illegal-1682660414>

Iain Thomson, “HackerOne says ‘no’ to FlexiSPY stalkerware bug bounty program,” *The Register* (5 May 2017) <https://www.theregister.co.uk/2017/05/05/hackerone_not_hosting_flexispy_bug_bounty/>

David Gilbert, “mSpy hacker says company knew of data leak two months ago,” *International Business Times* (22 May 2015) <https://www.ibtimes.co.uk/exclusive-mspy-hacker-says-company-knew-data-leak-two-months-ago-1502473>

Joseph Cox and Lorenzo Franceschi-Bicchierai, “PayPal Processes Payments for ‘Stalkerware’ Software Sold to Abusive Partners,” *Motherboard* (20 February 2019) <https://motherboard.vice.com/en_us/article/7xnwa9/paypal-payments-stalkerware-software-abusive-partners>

Sample Security Research in Stalkerware

Cian Heasley, “diskurse”: https://github.com/diskurse/android-stalkerware

Krebs on Security: https://krebsonsecurity.com/2018/09/for-2nd-time-in-3-years-mobile-spyware-maker-mspy-leaks-millions-of-sensitive-records/

Let’s Talk About FlexiSPY, April 23, 2018: https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/