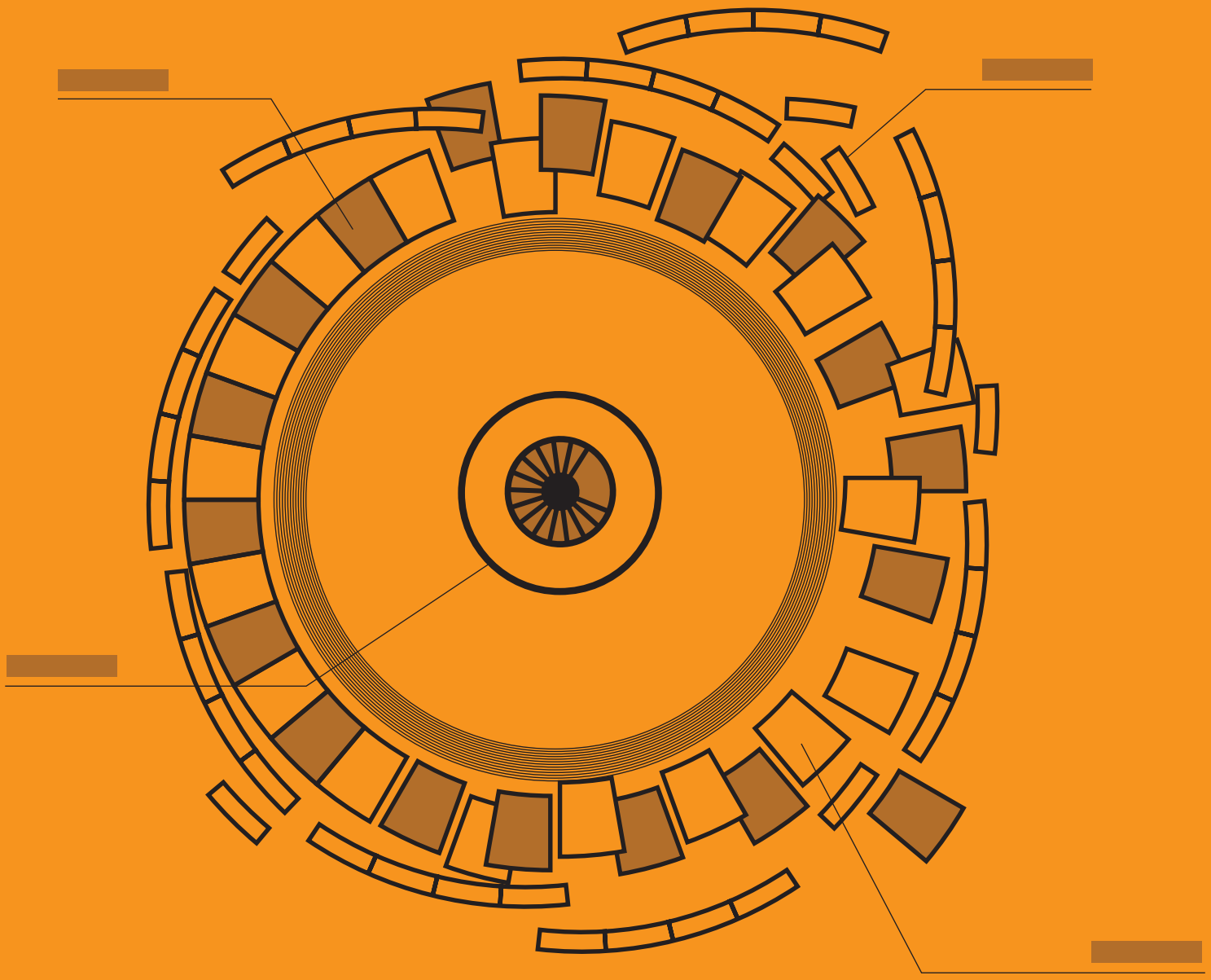


THE PREDATOR IN YOUR POCKET

A Multidisciplinary Assessment of the Stalkerware Application Industry

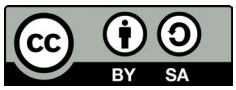
By Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, and Ronald Deibert

Research report #119
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 the 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: 1.2

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 B.

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.

The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & 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.

The Citizen Lab uses a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Its 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

Authors are listed in the order that their writing appears in the report.

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

Adam Molnar is currently a Lecturer at Deakin University (Australia) in the Department of Criminology and is a Visiting Professor at the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto. On 1 July, 2019, he will be Assistant Professor in the Department of Sociology and Legal Studies at the University of Waterloo. He received his Bachelor's from York University (Toronto), and his Master's and Ph.D from the University of Victoria.

Jakub Dalek is a Researcher at the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University Of Toronto. He received his Bachelor's from the University of Toronto.

Jeffrey Knockel is a Postdoctoral Fellow at the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto. He has used reverse engineering techniques to study how digital technologies affect people's freedom to communicate on the Internet in multiple peer-reviewed studies.

Miles Kenyon is a Communications Specialist at the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto. He received his Bachelor's from the University of Toronto and his Bachelor of Journalism from the University of King's College (Halifax).

Bennett Haselton is a contractor for the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto, and a developer for Psiphon, a maker of Internet anti-censorship software. He has been publishing research on Internet blocking and monitoring software since 1996. He also works as an Internet security researcher based in Seattle.

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 digital rights lawyer called to the Bar of Ontario, and completing the LL.M. (Concentration in Law and Technology) at the University of Ottawa, where she interned at the Canadian Internet Policy and Public Interest Clinic. She received her J.D. from the University of Victoria.

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, including (in alphabetical order): Siena Anstis, Suzie Dunn, Lara Fullenwieder, Maya Ganesh, Lex Gill, Diarmaid Harkin, Pam Hrick, Tamir Israel, Etienne Maynier, Petr Novak, Kate Robertson, Erica Vowles, and Rhiannon Wong. The design of this document is by Mari Zhou.

We are also grateful to the individuals who gave us the opportunity to share early versions of this of this research during the Citizen Lab Summer Institute on Monitoring Internet Openness and Rights (Munk School of Global Affairs & Public Policy, University of Toronto).

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, the Oak Foundation, the Australian Communications Consumer Action Network (ACCAN), 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:

chris@citizenlab.ca
adam.molnar@citizenlab.ca
cynthia@citizenlab.ca

Suggested Citation

Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, Ron Deibert. “The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry,” Citizen Lab Research Report No. 119, University of Toronto, June 2019.

Contents

Contents

Information Boxes

Table Of Acronyms

API	Application Programming Interface
APK	Android Application Package
ASN	Autonomous System Number
COPPA	Children's Online Privacy Protection Rule
DNS	Domain Name System
EU	European Union
EULA	End User License Agreement
FCC	Federal Communications Commission
GDPR	General Data Protection Regulation
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
OPC	Office of the Privacy Commissioner of Canada
PII	Personally Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act
PUA	Potentially Unwanted Application
PUP	Potentially Unwanted Program
RAM	Random Access Memory
SEO	Search Engine Optimization
SERP	Search Engine Results Pages
SMS	Short Message Service
SSL	Secure Socket Layer
TRJ	Trojan
URL	Uniform Resource Locator

Executive Summary

Persons who engage in technology-facilitated violence, abuse, and harassment sometimes install spyware on a targeted person's mobile phone. Spyware has a wide range of capabilities, including pervasive monitoring of text and chat messages, recording phone logs, tracking social media posts, logging website visits, activating a GPS system, registering keystrokes, and even activating phones' microphones and cameras, as well as sometimes blocking incoming phone calls. These capabilities can afford dramatic powers and control over an individual's everyday life. And when this software is used abusively, it can operate as a predator in a person's pocket, magnifying the pervasive surveillance of the spyware operator.

Intimate partner violence, abuse, and harassment is routinely linked with efforts to monitor and control a targeted person. As new technologies have seeped into everyday life, aggressors have adopted and repurposed them to terrorize, control, and manipulate their current and former partners. When National Public Radio conducted a survey of 72 domestic violence shelters in the United States, they found that 85% of domestic violence workers assisted victims whose abuser tracked them using GPS.[1] The US-based National Network to End Domestic Violence found that 71% of domestic abusers monitor survivors' computer activities, while 54% tracked survivors' cell phones with stalkerware.[2] In Australia, the Domestic Violence Resources Centre Victoria conducted a survey in 2013 that found that 82% of victims reported abuse via smartphones and 74% of practitioners reported tracking via applications as often occurring amongst their client base.[3] In Canada, a national survey of anti-violence support workers from 2012 found that 98% of perpetrators used technology to intimidate or threaten their victims, that 72% of perpetrators had hacked the email and social media accounts of the women and girls that they targeted, and that a further 61% had hacked into computers to monitor online activities and extract information.[4] An additional 31% installed computer monitoring software or hardware on their target's computer.[5]

---

1 Aarti Shahani (2014), "Smartphones Are Used To Stalk, Control Domestic Abuse Victims," NPR (September 15, 2014) <https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims>.

2 Danielle Keats Citron (2015), "Spying Inc.," *Washington and Lee L Rev* 72(3).

3 Delaine Woodlock (2013), "Technology-facilitated Stalking: Findings and Recommendations from the SmartSafe Project" In "Smartsafe," *Domestic Violence Resource Centre Victoria* <http://www.smartsafe.org.au/sites/default/files/SmartSafe-Findings-Booklet.pdf> at 15.

4 Safety Net Canada (2013), "Assessing Technology in the Context of Violence Against Women & Children: Examining Benefits & Risks," *British Columbia Society of Transition Houses* <https://bcsth.ca/publications/assessing-technology-context-violence-women-children-examining-benefits-risks/> at 6.

5 Safety Net Canada (2013), "Assessing Technology in the Context of Violence Against Women &

Spyware that possesses powerful surveillance capabilities are routinely marketed to consumer audiences to facilitate intimate partner surveillance, parent-child monitoring, or monitoring of employees. When these powerful capabilities are used to facilitate intimate partner violence, abuse, or harassment, we refer to such spyware as stalkerware.

Across a range of use-cases, spyware can easily transform into stalkerware. Perhaps most obviously, spyware that is explicitly sold or licenced to facilitate intimate partner violence, abuse, or harassment, including pernicious intrusions into the targeted person's life by way of physical or digital actions, constitutes stalkerware by definition. However, spyware can also operate as stalkerware when surveillance software that is sold for ostensibly legitimate purposes (e.g., monitoring young children or employees) is repurposed to facilitate intimate partner violence, abuse, or harassment. To be clear, this means that even application functions which are included in mobile operating systems, such as those which help to find one's friends and colleagues, can constitute stalkerware under certain circumstances.

"The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry" is a report that 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 stalkerware applications, stalkerware companies' marketing activities and public policies, and these companies' compliance with Canadian federal commercial privacy legislation.

Part 1 discusses the harms which are associated with a person being targeted by stalkerware, the full range of marketed capabilities associated with such malicious software, and lays out our justification for conducting research into a small handful of companies: in short, we found that the following companies appeared to be the most popular in the commercial markets in Canada, the United States, and Australia, and so we directed our resources on examining:

1) FlexiSPY;
2) Highster Mobile;

Children: Examining Benefits & Risks," British Columbia Society of Transition Houses <https://bcsth.ca/publications/assessing-technology-context-violence-women-children-examining-benefits-risks/> at 71.

3) Hoverwatch;
4) Mobistealth;
5) mSpy;
6) TeenSafe;
7) TheTruthSpy; and
8) Cerberus.

The rest of Part 1 provides a literature review for the subsequent Parts of the report, and makes clear where our research is meant to fill gaps in the published literature, or otherwise to reconfirm or retest results which have been published by other researchers. We posed a series of research questions based on assessments of relevant disciplinary literatures which are taken up in each of the following Parts of the report.

Part 2 undertakes a technical assessment of specific stalkerware applications. We focused on Android applications because Android-based stalkerware involves actually installing malware on a targeted person's devices. This process stands in contrast to stalkerware for iOS, which routinely depends on obtaining a targeted person's iCloud password to exfiltrate information for the person's iCloud backups. In the course of our research, we examined network activity, measured protection from commercial anti-virus products as well as Google's Play Protect system, and determined the extent to which stalkerware applications' self-update mechanisms might expose targeted persons to digital security risks in excess of those exclusively associated with the violence, abuse, and harassment from the operator of the stalkerware. Emergent from this research, we found that:

- Stalkerware we examined depends on intermediaries, principally located in the United States, Netherlands, and Hong Kong;
- Antivirus products generally identify stalkerware apps as being malicious;
- Google Play Protect can block stalkerware installation and remove installed stalkerware but it may not protect against the newest versions of stalkerware applications until a period of time after they are released; and
- Stalkerware developers insecurely implemented software update systems.

In **Part 3**, we evaluated how companies which sold stalkerware, and software which could be repurposed as stalkerware, marketed their products to prospective customers. We used marketing intelligence methods, as well as content analysis,

to conclude that many of the companies studied were actively promoting their software for the purposes of facilitating stalking and, by extension, intimate partner violence, abuse, and harassment. More specifically, we found that:

- Consumer spyware companies' blog and search engine optimization content revealed that most companies had extensive references to spousal monitoring;
- One company, mSpy, encoded concealed HTML text which advertised spousal spying on their website as a way to make their products more easily discoverable by people searching for ways to conduct intimate partner surveillance;
- Few companies significantly purchased Google Ads as part of their search engine optimization strategies, with the exception of mSpy;
- The substance of paid Google Ads tended to favour the use of the tools for general spying, hacking, or tracking, and did not include adwords that might help persons targeted by stalkerware to detect or remove the respective companies' software; and
- Individual organic searches that related to the spyware companies in our sample overwhelmingly favoured terms that identified the general use of the tools for spying, hacking, or tracking, and explicitly noted the circumvention of security features of products associated with the broader digital ecosystem.

Part 4 of the report undertook a content assessment of companies' user-facing public policies. We interrogated companies' respective privacy policies, terms of service documents, and End User Licence Agreements using a structured question set. This methodology let us better understand the policies which the companies adopted concerning the collection, processing, and storage of personal information associated with stalkerware operators as well as with the persons targeted by these operators. Emergent from this assessment, we concluded that the companies:

- Failed to make it clear how the victims of stalkerware can have their data deleted when they have not meaningfully consented to the collection;
- Failed to fully account for the personally identifiable information that can be captured when operating the software, thus circumventing the purpose and rationale of privacy policies to educate those affected by software to understand how it operates and collects such information; and
- Failed to adopt policies to notify persons targeted by stalkerware in the case of data breaches, or even individuals contracting for the services.

In **Part 5**, we conducted an assessment of stalkerware companies' business practices through the lens of Canada's federal commercial privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Our assessment examined the extent to which companies are accountable to PIPEDA and their corresponding obligations. We ultimately concluded that:

- Stalkerware companies should be found accountable under PIPEDA for the collection and processing of targeted persons' personal data on the basis that the companies collect personal information, engage in relevant commercial activities, and collect, use, or disclose targeted persons' data;
- Given the potential for stalkerware companies to argue that they are exempt from PIPEDA's obligations, the OPC should issue an interpretation bulletin or additional accompanying statement to the *Guidelines for obtaining meaningful consent or Guidance on inappropriate data practice*s that specifically address stalkerware, or the use of spyware in abusive contexts. Additionally, Parliament should consider reforming commercial sector data protection legislation to close loopholes that we have identified;
- Stalkerware companies ought to be obligated under PIPEDA to have extremely stringent data security practices based on the sensitivity of the data that they collect, process, disclose, and store; this pertains when these applications are used for ostensibly "legitimate" purposes and, as such, should apply to the collection of intimate data in the course of products being (re)purposed for stalkerware; and
- PIPEDA and the European Union's General Data Protection Regulation (GDPR) identify significant obligations that are imposed upon companies which sell products that have features enabling them to be used as stalkerware. The strength of the GDPR is ultimately found in the significant financial penalties which can be assigned to companies which fail to comply with the law. This is a strength that Parliament should add to PIPEDA by way of enabling the Privacy Commissioner of Canada to impose administrative monetary penalties and directly enforce its recommendations on companies.

Notably, PIPEDA only applies to the activities undertaken by business and organizations; as such, our assessment does not attend to the broader Canadian criminal law, tort law, privacy law, product liability, consumer protection, intellectual property, and intermediary liability law that are attached to the

legality of using, creating and developing, selling, or facilitating the distribution of stalkerware applications. A broader legal assessment of stalkerware, as well as a set of recommendations for legal and policy reform to address some of the harms that stalkerware engenders, can be found in a companion report entitled "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications."[6]

In Part 6 we collect our major findings from our multidisciplinary research and propose a range of recommendations that would mitigate some of the harms associated with stalkerware companies' practices and products. We focused on issues associated with consent, accountability and redress by jurisdiction, as well as data security and data protection. Specifically, our major findings included:

- There were significant and disturbing failures by the companies in this study to obtain meaningful and ongoing consent, which seriously increased the risks and threats faced by those who operators target with stalkerware. This omission was further marked by failures to ensure that targeted persons could exercise their data access and deletion rights under Canadian privacy law;
- While these companies were accountable under Canadian consumer privacy law, the limited 'bite' of that law may impede its ability—and, by extension, that of the Office of the Privacy Commissioner of Canada—to establish preemptive deterrence or ex post remedy and enforcement;
- Not all of the companies in this study indicated that data security was a meaningful element in their privacy policies, despite Canadian law imposing data security obligations; and
- Google's Play Protect service in tandem with antivirus applications appeared, in initial testing, to relatively reliably identify stalkerware. However, more long-term testing is required to further confirm these results.

Ultimately, the availability of stalkerware applications is the result of broader social conditions that either lead developers to believe it is appropriate to create software designed for stalking or, alternately, to create applications for ostensibly legitimate purposes that can be repurposed to facilitate surreptitious intimate partner surveillance. The recommendations that we propose in this report might,

6 "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications" is available at: https://citizenlab.ca/docs/stalkerware-legal.pdf

if adopted, rebalance stark information asymmetries between the operator and target(s) of stalkerware. This rebalancing would address a core aspect of how stalkerware works as a tool to facilitate intimate partner violence, abuse, and harassment: by mitigating the potential for operators to engage in pervasive and surreptitious surveillance. Adopting these recommendations would also ensure meaningful and ongoing consent to any individuals that might use these tools for ostensibly legitimate purposes.

These recommendations are, however, only part of a much broader series of technical and social transformations which are required to remedy the wider, and pervasive, issues that give rise to forms of gender-related violence, abuse, and harassment. While the technical and legal remedies outlined in this report might provide important relief in the context of consumer spyware, the ongoing struggle to transcend patriarchal gender inequalities, misogyny, and corrosive societal norms around controlling, abusive, and violent behaviour directed at women, girls, non-binary persons, and children is an undertaking that requires critical and supportive communities at its core. We hope that this report provides insight into some of the deleterious manifestations of these norms, and that the structural recommendations which we provide help to alleviate some of these long-standing social harms.

Introduction

Smartphones and personal laptops are used to communicate, seek information, access government services, build community, maintain relationships, participate in public discourse, conduct commerce, take photos, navigate to new places, and more; as a result, these devices give unique insights into one's personal life.[7] Unfortunately, current and former romantic partners, family members, acquaintances, or other personal associates sometimes purchase and use spyware or other tools to extract information from these devices for the purpose of facilitating violence, abuse, harassment, or other ills.[8] Intimate partner stalking has significant impacts on the psychological well-being and mental health of women,[9] including their employment[10] and relationships.[11] Increasingly, these abusive behaviours are facilitated through the use of digital technologies.[12] When National Public Radio conducted a survey of 72 domestic violence shelters in the United States they found that 85% of domestic violence workers assisted victims whose abuser tracked

---

7 The Citizen Lab (2015), "The Many Identifiers in Our Packets: A primer on mobile privacy and security," *The Citizen Lab* <https://citizenlab.ca/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/>; Christopher Parsons and Tamir Israel (2016), "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," *The Citizen Lab// CIPPIC* <https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>; OPC Blogger, "From APP-laudable to dis-APP-ointing, global mobile app privacy sweep yields mixed results," *Office of the Privacy Commissioner of Canada* (September 9, 2014) <https://www.priv.gc.ca/en/blog/20140909/>.

8 See: Lorenzo Franceschi-Bicchierai and Joseph Cox (2017), "Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones," *Mothberboard* (April 18 2017) <https://motherboard.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x>; BBC (2006), "Life term for stab death husband," BBC (July 10, 2006) <http://news.bbc.co.uk/2/hi/uk_news/england/5165154.stm>; Jason Koebler (2017), "'I See You': A Domestic Violence Survivor Talks About Being Surveilled By Her Ex," *Motherboard* (March 17 2017) <https://motherboard.vice.com/en_us/article/bmbpvv/i-see-you-a-domestic-violence-survivor-talks-about-being-surveilled-by-her-ex>; Aarti Shahani (2014), "Smartphones Are Used To Stalk, Control Domestic Abuse Victims," *NPR* (September 15, 2014) <https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims>; Michelle Cottle (2014), "The Adultery Arms Race," *The Atlantic* (November) <https://www.theatlantic.com/magazine/archive/2014/11/the-adultery-arms-race/380794/>.

9 Kuehner, Christine, Peter Gass, and Harald Dressing (2012), "Mediating Effects of Stalking Victimization on Gender Differences in Mental Health," Journal of Interpersonal Violence 27:2; Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, Sunny Consolvo (2017), "Stories from Survivors: Privacy and Security Practices when Coping with Intimate Partner Abuse," *Precautionary Behaviours* <https://dl.acm.org/citation.cfm?doid=3025453.3025875> .

10 TK Logan, Lisa Shannon, Jennifer Cole, and Jennifer Swanberg (2007), "Partner Stalking and Implications for Women's Employment," *Journal of Interpersonal Violence* 22(3).

11 Heather Melton (2007), "Stalking in the Context of Intimate Partner Abuse In the Victims' Words," Feminist Criminology 2(4); TK Logan, Lisa Shannon, Jennifer Cole & Robert Walker (2006), "The Impact of Differential Patterns of Physical Violence and Stalking on Mental Health and Help-Seeking among Women with Protective Orders," *Violence Against Women* 12(9).

12 Cynthia Fraser, Erica Olsen, Kaofeng Lee, Cindy Southworth (2010), "The New Age of Stalking: Technological Implications for Stalking," *Juvenile and Family Court Journal* 61.

them using GPS.[13] The US-based National Network to End Domestic Violence found that 71% of domestic abusers monitor survivors' computer activities, while 54% tracked survivors' cell phones with stalkerware.[14] In Australia, the Domestic Violence Resources Centre Victoria conducted a survey in 2013 that found that 82% of victims reported abuse via smartphones and 74% of practitioners reported tracking via applications as often occurring amongst their client base.[15] In Canada, a national survey of anti-violence support workers from 2012 found that 98% of perpetrators used technology to intimidate or threaten their victims, that 72% of perpetrators had hacked the email and social media accounts of the women and girls that they targeted, and that a further 61% had hacked into computers to monitor online activities and extract information.[16] An additional 31% installed computer monitoring software or hardware on their target's computer.[17]

The software that is used for intimate partner violence, abuse, and harassment is sometimes specially-crafted for this purpose, or companies clearly denote that their software can be used for these classes of abusive activities. However, there are times where developers also present their products for what they claim are more benevolent purposes, such as monitoring children or employees. As an example, software is sometimes sold as anti-theft software (e.g., Cerberus) but is documented as being used for abusive purposes by purchasers of the software.[18] In situations such as these, where applications are 'dual-use' and have ostensibly legitimate purposes as well as the capability to facilitate intimate partner violence, abuse, and harassment, we refer to the software as 'stalkerware' to delineate the latter kinds of uses and activities associated with the software. Throughout this report, we refer to the abusive operation of dual-use software as constituting 'stalkerware' and,

13 Aarti Shahani (2014), "Smartphones Are Used To Stalk, Control Domestic Abuse Victims," *NPR* (September 15, 2014) <https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims>.

14 Danielle Keats Citron (2015), "Spying Inc.," *Washington and Lee L Rev* 72(3).

15 Delaine Woodlock (2013), "Technology-facilitated Stalking: Findings and Recommendations from the SmartSafe Project" In "Smartsafe," *Domestic Violence Resource Centre Victoria* <http://www.smartsafe.org.au/sites/default/files/SmartSafe-Findings-Booklet.pdf> at 15.

16 Safety Net Canada (2013), "Assessing Technology in the Context of Violence Against Women & Children: Examining Benefits & Risks," *British Columbia Society of Transition Houses* <https://bcsth.ca/wp-content/uploads/2016/10/Assessing-Technology-in-the-Context-of-Violence-Against-Women-Children.-Examining-Benefits-Risks.pdf> at 6.

17 Safety Net Canada (2013), "Assessing Technology in the Context of Violence Against Women & Children: Examining Benefits & Risks," British Columbia Society of Transition Houses <https://bcsth.ca/publications/assessing-technology-context-violence-women-children-examining-benefits-risks/> at 71.

18 Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon Mccoy, and Thomas Ristenpart (2018), "The Spyware Used in Intimate Partner Violence" *2018 IEEE Symposium on Security and Privacy Proceedings* 1.

similarly, identify applications which are specifically designed to facilitate intimate partner abuse and harassment as 'stalkerware'; in doing so, we avoid making a claim about the broader legality or ethics associated with other uses of the spyware in this report.[19] Information Box 1: Report Terminology provides a summary of key terminology used throughout this report.

Information Box 1: Report Terminology

- **Dual-use technology:** technology that may be intended for, or may be used for, legitimate or benevolent ends, but which may be equally capable of being 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 both uses were intended.

- **Intimate partner spyware applications:** spyware applications that are intentionally designed and advertised for the purpose of facilitating surveillance of an intimate partner's mobile device.

- **Operator:** the person who installs or exploits stalkerware on another individual's device, and uses that technology to remotely monitor and surveil the user of the device.

- **Spyware:** 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 targeted device to another computer system. Because this code or software is deployed in the context of targeting a specific individual or group of individuals 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 application and spyware program.

- **Stalkerware:** consumer-level applications that exist or may be installed on a mobile device that let the operator of the application remotely monitor the activities of the device's user, or individuals routinely in the proximity of the user (e.g., parents and children). For the purpose of this report, this term includes intimate partner spyware applications and spyware applications which are repurposed to facilitate intimate partner violence, abuse, and harassment. We also use the terms stalkerware application and stalkerware program. A more detailed definition can be found in Part 1.1: What is Stalkerware?

- **Stalkerware developer:** a company or person(s) that creates a spyware application that is designed to operate as, or can be repurposed as, stalkerware. Such a company or person(s) design the program or write the code required for

19 See "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," a comprehensive legal analysis of stalkerware that the Citizen Lab has published separately, for further discussion concerning the ethics and legality of monitoring children and employees using spyware apps. The report is available at: https://citizenlab.ca/docs/stalkerware-legal.pdf.

a spyware application and its associated infrastructure (e.g., such as browser dashboards to view the collected data) to operate.

- **Stalkerware distributor**: an entity that distributes stalkerware and which may be either a stalkerware business or an intermediary.
- **Stalkerware intermediary:** 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., application stores).
- **Stalkerware vendor/business/company:** an entity that either: 1) offers its own spyware application for sale directly to private individuals; 2) owns the spyware software; or 3) whose business model primarily revolves around spyware.
- **Target:** a target or targeted individual or targeted person refers to the person who is subjected to surveillance through stalkerware technology installed on their device.
- **Victim-survivor:** a term used to describe a person, or persons, who are negatively impacted by intimate partner and family violence. The inclusion of the term 'survivor' references the potential for positive affirmations of agency and empowerment in the face of violence.

"The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry" explores how the companies which sell spyware that is used to facilitate intimate partner violence, abuse, and harassment technically design their products, how such companies promote their products using Search Engine Optimization (SEO) activities, and how such companies present their operations through their public policy documents. This report also examines the lawfulness of such software through the lens of consumer privacy law, as governed by Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA). In short, this project engages with the following questions:

- **Technical Infrastructure and Security:** Does software sold to facilitate intimate partner violence and harassment possess technical indicators that can be used to identify infrastructure that it communicates with? Are these products detectable by anti-virus programs? Do these applications leave targets of surveillance in heightened states of vulnerability insofar as the products introduce novel technical vulnerabilities?
- **Advertising Practices:** Do these companies' SEO practices reveal that they are knowingly marketing their products to persons who are seeking them out for the purposes of facilitating intimate partner violence or harassment? Do

SEO practices demonstrate that companies are attempting to assist persons who have been inappropriately or illegally targeted by the such companies' respective software products?

- **Terms of Use, Privacy Policies, and End User License Agreements (EULAs):** To what extent do companies selling these products have similar terms of service, privacy policies, or end user licence agreements? Do these policy documents clearly recognize and protect the rights of the targets of these companies' products?
- **Consumer Privacy and Data Protection Law:** In what ways do stalkerware applications contravene PIPEDA? What remedies might be available to those who are detrimentally affected by companies' products and services which are used to facilitate intimate partner violence and harassment?

Questions about how these companies operate, and how they treat the data of persons who are abusively targeted by spyware, is pertinent to a range of stakeholders. Beyond assisting the Office of the Privacy Commissioner of Canada in understanding the scope and nature of these products, answers to the aforementioned questions can assist civil society stakeholders in appreciating and more fully understanding the threats linked with this class of software and, prospectively, ascertain whether such applications are operating on their clients' devices or, alternately, be equipped to bring suit against companies who are selling unlawful products or are engaged in unlawful classes of commercial activity. Furthermore, "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," the legal report which accompanies "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry", provides a comprehensive assessment of the overall legality of these kinds of products under Canadian law and ultimately provides a range of legal theories that could be used in litigation against the companies selling these products, parties involved in operating these products, or parties involved in developing these products.

This report proceeds as follows:

- **Part 1** provides a background to stalkerware as a class of particularly abusive spyware and, also, offers a brief summation of academic and other literatures associated with these modes of abusive spyware as they pertain to the technical characteristics of the software, the marketing of them, the assessment of companies' publicly stated policies, and merits of assessing the legality of sold products and services and associated business practices.

- **Part 2** focuses on the technical research conducted, including the methodologies and results. We discuss characteristics of the network traffic associated with these products, including ways in which these products undermine device security, and the extent to which the researched stalkerware applications are detectable by anti-virus detection engines.
- **Part 3** principally focuses on the repurposing of marketing intelligence platforms as a means to learn more about how consumers as well as the spyware companies interpret and understand stalkerware as a commercial product and tool of surveillance. By examining how companies promote their products on their websites and social media accounts, investigating the paid Google Adwords that companies used to promote their products online, and the keywords that consumers used when searching for stalkerware products, we unpack how companies attract customers to their monitoring services and how customers may intend to use these services.
- **Part 4** examines public facing corporate policies to assess the extent to which stalkerware companies recognize the legal rights of individuals targeted by surveillance, as opposed to the legal rights of the operators of their stalkerware. We specifically examine whether these policies commit companies to assisting individuals targeted by stalkerware, such as by explaining how to have the application removed from their device, as well as having their data removed from a company's servers and from the custody of the operator.
- **Part 5** engages in a consumer privacy law-based legal analysis of stalkerware vendors, and focuses on stalkerware vendor accountability under PIPEDA (including developers who sell their own software), exceptions that potentially remove stalkerware companies from PIPEDA's ambit, the privacy rights and obligations companies must adhere to under PIPEDA, and a comparison between the European Union's General Data Protection Regulation and PIPEDA to understand the relative strengths and weaknesses of PIPEDA compared to the European law.
- **Part 6** highlights the most significant findings that emerged from evaluating stalkerware companies' technical products, marketing practices, corporate policies, and legal obligations under PIPEDA. This part also includes recommendations to government as well as to companies which sell and develop software which can be used abusively for facilitating intimate partner violence and harassment.

Part 1 - Background and Literature Review

Intimate partner violence, abuse, and harassment often involves abusers targeting and systematically and abusively intruding into the public and private lives of their current or former partners.[20] These kinds of stalking behaviours functionally entail "acts of pursuit of an individual over time that are threatening and potentially dangerous"[21] and, generally, are intended to exert control over the stalking victims.[22] Abusive partners tend to monitor the public and private lives of the targets in order to delimit who the targeted persons can communicate with, to unexpectedly show up in physical spaces proximate to the targeted persons, to understand how and where they are spending money and time, and more broadly to exert power and control over the targeted individual.[23] The focus for the stalker is to collect broad amounts of information about the target, often without their knowledge, and then use such information to facilitate either further abuse or harassment. Intimate partner stalking has significant impacts on the psychological well-being and mental health of women,[24] including their employment,[25] relationships,[26] and human rights,[27] and increasingly these abusive behaviours are facilitated through the use of digital technologies.[28]

---

20 Evan Stark (2009), *Coercive control: The entrapment of women in personal life.* (Oxford University Press: 2009).

21 J. Reid Meloy (1998), *The Psychology of Stalking: Clinical and Forensic Perspectives.* (Academic Press, Elsevier: 1998) at 2.

22 Delaine Woodlock (2017), "The abuse of technology in domestic violence and stalking," Violence against women 23(5); Heather Douglas, Bridget A Harris, Molly Dragiewicz (2019), "Technology-facilitated domestic and family violence: Women's experiences," *The British Journal of Criminology* 59(3).

23 Evan Stark (2013), "Coercive control," in *Violence against women: Current theory and practice in domestic abuse, sexual violence and exploitation*, Ed. Nancy Lambert and Leslie McMillan (2013: Jessica Kingsley Publishers); Jane Maree Maher, Jude McCulloch and Kate Fitz-Gibbon (2017), "New forms of gendered surveillance? Intersections of technology and family violence," In *Gender, Technology and Violence, Segrave and Vitis* (2017: Routledge).

24 Christine Kuehner, Peter Gass, and Harald Dressing (2012),"Mediating Effects of Stalking Victimization on Gender Differences in Mental Health," *Journal of Interpersonal Violence* 27:2; Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, Sunny Consolvo (2017), "Stories from Survivors: Privacy and Security Practices when Coping with Intimate Partner Abuse," *Precautionary Behaviours* <https://dl.acm.org/citation.cfm?doid=3025453.3025875>.

25 TK Logan, Lisa Shannon, Jennifer Cole, and Jennifer Swanberg (2007), "Partner Stalking and Implications for Women's Employment." *Journal of Interpersonal Violence* 22(3) (March 2007).

26 Heather Melton (2007), "Stalking in the Context of Intimate Partner Abuse In the Victims' Words," *Feminist Criminology* 2(4); TK Logan, Lisa Shannon, Jennifer Cole, and Robert Walker (2006), "The Impact of Differential Patterns of Physical Violence and Stalking on Mental Health and Help-Seeking among Women with Protective Orders," *Violence Against Women* 12(9).

27 "Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović," *The Citizen Lab* (November 2017) <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf>.

28 Nicola Henry and Anastasia Powell (2018), "Technology-facilitated sexual violence: A literature

Stalking behaviours are serious predictors of future violence[29] and such behaviours and associated practices assume many forms. Today, many stalkers and abusive partners are turning to collecting information from mobile phones since these devices aggregate and potentially disclose significant amounts of intimate information. The GPS tracking functionality of mobile phones is routinely used to track stalking victims, and a cross-Canada survey of programs that support women and children escaping or living in violent situations noted eighteen forms of technology-facilitated violence and abuse, including:

- breaking into and monitoring instant messaging accounts (46%);
- breaking into email, social media, and other online accounts (72%);
- impersonating the targeted individual or someone they know over email, another online platform, or other technology (69%);
- breaking into the victim's computer to monitor their 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%).[30]

In effect, digital surveillance technologies are increasingly being used by stalkers and abusive partners to exert control over their current or former intimate partners. We turn, now, to what constitutes 'stalkerware' and how applications

review of empirical research," *Trauma, violence, & abuse 19*(2); Cynthia Fraser, Erica Olsen, Kaofeng Lee, Cindy Southworth, and Sarah Tucker (2010), "The New Age of Stalking: Technological Implications for Stalking," *Juvenile and Family Court Journal* 61(4); Molly Dragiewicz, Delanie Woodlock, Bridget Harris, and Claire Reid (2018), "Technology-facilitated coercive control," In *The Routledge International Handbook of Violence Studies* Ed. Walter S. DeKeseredy, Callie Marie Rennison, and Amanda K. Hall-Sanchez (2018: Routledge).

29 See: Judith M. McFarlane, Jacquelyn C. Campbell, Susan Wilt, Carolyn J. Sachs, Yvonne Ulrich, and Xiao Xu (1999), "Stalking and Intimate Partner Femicide," *Homicide Studies* 3(4); Jacqulyn C Campbell, Daniel Webster, Jane Koziol-McLain, Carolyn Block, Doris Campbell, Mary Ann Curry, Faye Gary, Nancy Glass, Judith McFarlane, Carolyn Sachs, and others (2003), "Risk factors for femicide in abusive relationships: Results from a multisite case control study," *American Journal of Public Health* 93(7).

30 Cynthia Fraser, Rhiannon Wong, NNEDV Safety Net Project (2013), "Organizational Technology Practices For Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children," *Safety Net Canada* <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 19.

that are purpose-made for such surveillance as well as for ostensibly more legitimate purposes are being used by stalkers to exert control over the targets of their abusive behaviour.

1.1 What is Stalkerware

Companies sell spyware to help employers and parents keep track of employees and their children, respectively. Such spyware can also be used to abusively facilitate intimate partner violence and harassment; some companies even market their spyware with the explicit purpose of facilitating such intimate partner surveillance. TheTruthSpy, as an example, notes that its application enables an operator of the stalkerware to determine whether "your partner [sic] spending all his money on someone, where your partner is spending the most time … you need a spying device so that you can know with whom they are chatting or talking on the phone and you can also know what your partner is doing."[31]

Broadly, we adopt the definition from Harkin et al. concerning what constitutes 'spyware.' Specifically, such applications exhibit the following characteristics:

1) Data is gathered remotely from a target device that would otherwise not be shared unless foreign code or software were introduced or permitted access by an operator.
2) Data is gathered from the target device with the credible possibility that the user of the target device would not be aware of the exfiltrated information, the ongoing presence of the foreign code or software, or any permissions to disclose information. Even where the targeted user is aware of the app's presence on their device, however, they may not be aware of the ways in which the app is being used for monitoring and/or coercive control, or they may not be in a position to safely refuse to have the software deployed on their device.
3) The code or software is to be deployed in the context of targeting a specific individual or group of individuals for the purposes of monitoring, tracking, and surveillance. It therefore 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 (e.g., Facebook or other

31 TheTruthSpy (2018), "Download & Install TheTruthSpy on Android phones," *TheTruthSpy* <http://android.thetruthspy.com/>.

social networking services and platforms, as well as Internet-of-things devices).

4) The data being disclosed to operators about the target can be reasonably understood to include private, confidential, and otherwise intimate personal information (e.g., location data, private correspondence, personal photos, passwords, etc.).[32]

We define all spyware that is explicitly sold or licenced to facilitate intimate partner violence, abuse, or harassment, inclusive of deleteriously intruding into the abused partner's private life by way of physical or digital actions, as stalkerware by definition. We also stipulate that spyware operates as stalkerware when surveillance software sold for ostensibly legitimate purposes (e.g., monitoring young children or employees) is repurposed to facilitate intimate partner violence, abuse, or harassment. To be clear, this means that even application functions included in mobile operating systems, such as those which help to find one's friends and colleagues, can constitute stalkerware under certain circumstances.

Harms resulting from online and technology-facilitated violence, abuse, and harassment may include:

- Physical harm, such as stress-related illness, injury, and physical trauma;[33]
- Psychological or emotional harm, such as experiences of shame, stress, and 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 increasing needs for health care, judicial, and social services, impeding the exercise of free expression, the right to privacy, and other human rights central to one's autonomy and human dignity, and disturbing the sense of peace and security required to fully participate in social, economic, democratic life.[34]

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

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

34 "Submission to the United Nations Special Rapporteur on violence against women, its causes

Installing stalkerware on a targeted device often entails privileged access to it, meaning that the stalker either has physical access to the phone and knowledge of the phone's passcode (in the case of most Android-compatible and Apple-compatible stalkerware) or to the targeted person's iCloud password (in the case of most Apple-compatible stalkerware). Physical access to an Android-based mobile device combined with the relevant passcode(s) lets the operator bypass potential security notices as well as give all of the requested device permissions to the stalkerware application upon its installation. After being installed, some applications are designed so that the operator can conceal the presence of the stalkerware on the target's device. In such cases, the stalkerware does not appear in the device's applications menu or on the home screen, nor does it indicate when it is secretly tracking the target individual's activities or exfiltrating their data. In this way, the victim's device can become indefinitely infected and compromised without the victim necessarily knowing or suspecting that they are being subjected to device-based surveillance.

In the case of most iOS stalkerware, the stalker typically obtains the targeted persons' iCloud login and password and, where two-factor authentication has been enabled, physical access to an unlocked device associated with the iCloud Account. After presenting the login and password set to the stalkerware vendor's system, that system will subsequently exfiltrate information from the iCloud environment and make it available to the stalker. In relatively rare cases, iOS stalkerware may involve installing a specific application on an iOS device. However, such installations typically rely on exploiting security deficiencies in previous versions of iOS. In effect, iOS devices which have the most recent software patches installed tend not to be vulnerable to these kinds of iOS stalkerware, such as those sold by TheTruthSpy and FlexiSPY at the time of writing.

1.2 Case Selection

We employed general web searches in combination with searches of the Google Play store and the Apple App store to develop initial lists of stalkerware applications. Web searches included queries such as "spyware," "top spyware apps," and "track spouse." Emergent from these queries we found numerous curated lists that denoted the 'best' of these applications.[35] Based on these results we created a long-list of

and consequences, Ms. Dubravka Šimonović," *The Citizen Lab* (November 2017) <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf> at 2-3 (footnotes omitted).

35 See Figure 1. in Diarmaid Harkin, Adam Molnar, and Erica Vowles (2019), "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," Crime Media Culture for the results of some of these queries.

available spyware that could be deployed for stalkerware purposes. Our searches of the Google and Apple mobile application stores included queries such as "spyware," "surveillance," "tracking," "spouse monitoring," and "employee tracking." Many of the returned applications constitute 'dual-use' applications, or those which might be used for ostensibly legitimate, as well as abusive, purposes. The queries to the app stores also produced longlists of potentially abusive applications.

In part due to the challenges associated with determining the efficacy of the dual-use nature of many applications in the mobile application stores, and given the significant number of applications branded as 'spyware' in these stores, we narrowed our sample to applications that were both functional and in broad circulation. After reviewing 'best of' lists when searching the open web, we directed our focus on the applications identified in our open web queries. We subsequently used 'Google Trends' to narrow down our sample based on the companies that individuals searched for the most frequently. Many of these applications were included in 'best of' lists despite not appearing in application store searches. The most popular applications that emerged from this process included:

1) FlexiSPY;
2) Highster Mobile;
3) Hoverwatch;
4) Mobistealth;
5) mSpy;
6) TeenSafe; and
7) TheTruthSpy.

We also included Cerberus, which was available in the Google Play Store at the time of writing, based on academic articles which noted that the application is occasionally used as stalkerware.[36] **Parts 2 to 5** of this report focus almost exclusively on the aforementioned eight applications; the exception is the addition of Trackerview in Part 3, which was included in that section of the report to determine if applications which sold their products primarily as a geo-location tracking tool would adopt marketing strategies which differed from the other companies in our sample.

36 As example, see: Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon Mccoy, and Thomas Ristenpart (2018), "The Spyware Used in Intimate Partner Violence" *2018 IEEE Symposium on Security and Privacy Proceedings* 1.

1.3 Stalkerware Capabilities

Not all stalkerware has identical capabilities, though this class of abusive software does tend to share a range of common characteristics. Almost all of the applications included in this report are capable of monitoring SMS messages, a range of chat applications (e.g., WhatsApp, LINE), phone call logs, stored media such as photos and videos, web traffic, and GPS information. In contrast, some but not all stalkerware applications can monitor email, social media activity, contacts in an address book, calendar entries, keystrokes, or surreptitiously activate either the microphone or take photographs.

All of the applications we studied could be installed on Android devices. In all cases except those of FlexiSPY and mSpy, applications which targeted iOS devices depended on the stalker obtaining the iCloud login and password of the targeted person. Services would then use this login and password set to automatically extract data from iCloud, which includes contacts, calendar information, photos, notes, geolocation, and potentially even files stored in iCloud drive—and make the data available to the stalker. It should be noted, however, that other stalkerware apps are available to install on iPhones and operate similarly to Android-based apps as described in this report, provided that the targeted phone has been 'jailbroken'.

Tables 1 and 2 more specifically denote the classes of capabilities that are associated with the selected applications (excluding Trackerview) that were studied over the course of this report. Capabilities were assessed based on companies' marketing materials as well as testing with some of the companies' applications.

	Record/Access/Monitor											
	Phone Calls	SMS	Chat Apps	Phone Logs	Social Media	Stored Media	Web Traffic	Email	GPS	Contacts	Calendar	Keystrokes
Cerberus				X					X			
FlexiSPY	X	X	X	X	X	X	X	X	X			X
Highster Mobile		X	X	X	X	X	X		X	X	X	
Hoverwatch	X	X	X	X			X		X	X	X	
Mobistealth	X	X	X		X	X	X	X	X			X
mSpy		X	X	X		X	X	X	X	X	X	X
TeenSafe		X	X	X			X		X	X		
TheTruthSpy	X	X	X	X	X	X	X	X	X			

Table 1: Recording, Access, and Monitoring Capabilities of Stalkerware Applications

	Activate Microphone	Take Photos	Remote Access/ Update	Block Phone Calls	Backup Data	iOS	Android
Cerberus		X	X		X		X
FlexiSPY	X	X	X			X**	X
Highster Mobile		X				X*	X
Hoverwatch		X					X
Mobistealth	X				X*	X*	X
mSpy				X	X*	X*	X
TeenSafe					X*	X*	X
TheTruthSpy	X					X**	X

Table 2: Extended Capabilities of Stalkerware Applications and Operating System Compatibility
* Applications access iOS-based data by collecting information from iOS backups, which require acquiring a target's iCloud login/password as opposed to exfiltrating data directly from a targeted mobile device
** Applications access iOS-based data by installing applications on older or deprecated versions of iOS that have security vulnerabilities which can be exploited to install the application

1.4 Domestic Violence, Gendered Surveillance, and Privacy

Instances of family violence and intimate partner violence and abuse in Canada constitute a widespread and serious socio-political problem. Family or intimate partner violence affects nearly one out of three women and one out of four men at some point in their lives.[37] Among all police-reported instances of violent crime in Canada, more than 26% resulted from family violence.[38] Such violence is significantly gendered, with almost 67% of family violence victims in Canada being women and girls.[39] Among all child and youth victims of violent crime, approximately 30% of victims suffered at the hands of a parent, sibling, spouse, or other family member; 59% of these police-reported cases involved a parent as the abuser. Such parental violence is also gendered, with female children and youth more likely being victims of family violence that is reported to authorities as compared to young males.[40] The Government of Canada noted in 2014 that fewer than one in five of all people

37 National Coalition Against Domestic Violence (2019), "Statistics," <https://ncadv.org/statistics>.

38 According to Canadian Centre for Justice, Statistics 2016, it is worth noting further that in 2014 fewer than 19% who had been abused by their spouse reported abuse to police (Canadian Centre for Justice, Statistics, 2016).

39 Canadian Centre for Justice, Statistics 2016.

40 Shana Conroy (2018), "Section 4: Police-reported family violence against children and youth," *Statistics Canada* <https://www150.statcan.gc.ca/n1/pub/85-002-x/2018001/article/54893/04-eng.htm>.

abused by their spouse reported the violence to police.[41] Given the extent to which family and intimate partner violence is notoriously under-reported, the actual scope and impact of the problem is certainly greater than these statistics suggest.

The extent to which digital technologies exacerbate existing phenomena of intimate partner and family violence are being recognised by a range of scholars and anti-domestic violence advocates. Following the recognition that online and offline behaviours are increasingly inseparable in nearly all aspects of private and public life,[42] researchers are examining how technologies and digital media are inseparable from instances of intimate partner and family violence. Echoing Langdon Winner,[43] these abusive uses of technology are in part based on the internal characteristics of how specific technologies (and technological systems) function as well as being shaped through social and cultural norms that influence how, and to what ends, technologies are used. In other words, socio-cultural norms are deeply inculcated into the material design of technologies and, as such, technologies themselves implicitly express particular norms of power and control. Even in instances where developers do not deliberately design products for problematic uses, design decisions are invariably linked with particular use cases, or affordances, for humans. These decisions, and their corresponding affordances, are always informed by the socio-cultural conditions of its users and, consequently, routinely have the effect of reproducing historical power structures.

Forms of bullying, sexual harassment on social media and dating apps,[44] online fraud,[45] non-consensual sharing of personally identifying details online (doxing),[46]

41 Government of Canada (2016), "Family Violence: how big is the problem in Canada?" Canada.ca,<https://www.canada.ca/en/public-health/services/health-promotion/stop-family-violence/problem-canada.html>; Canadian Centre for Justice Statistics (2016); Stats Canada (2014),"Family violence in Canada: A statistical profile, 2014." *Juristat, Statistics Canada Catalogue* 85-002-X; J Boyce (2016), "Victimisation Aboriginal People in Canada, 2014." *Juristat, Statistics Canada Catalogue* 85-002-X.

42 Nancy Baym (2015), *Personal Connections in the Digital Age.* (2015: Polity Press).

43 Langdon Winner (1986), *The Whale and the Reactor: a search for limits in an age of high technology.*(1986: University of Chicago Press).

44 Nicola Henry and Anatasia Powell (2015), "Embodied harms: Gender, shame, and technology-facilitated sexual violence." *Violence against women* 21(6); Nicola Henry and Anastasia Powell (2018), "Technology-facilitated sexual violence: A literature review of empirical research," *Trauma, violence, & abuse* 19(2).

45 Bert-Jaap Koops and Ronald Leenes(2006), "Identity theft, identity fraud and/or identity-related crime," *Datenschutz und Datensicherheit-DuD* 30(9).

46 Clare McGlynn and Erika Rackley (2017), "Image-based sexual abuse," *Oxford Journal of Legal Studies* 37(3).

non-consensual distribution of intimate images and image-based sexual abuse,[47] and monitoring of behaviours through Internet of Thing sensors in the home[48] or through social media activities[49] are all specific areas where technologies are regarded as having a distinct influence on forms of gendered violence. In each of the aforementioned instances, technologies provide novel affordances to engage familiar forms of gendered surveillance, discrimination, misogyny, harassment, and the perpetration of violence in intimate relations.

Technology-facilitated violence and abuse is often defined as the use of digital media technologies to facilitate coercive and controlling relationships, which some scholars refer to as technology-facilitated coercive control. Existing research regarding the shape and impact of technology-facilitated violence and abuse is spread across a range of discrete technologies and methodological approaches. Standardised self-report surveys are often used to measure the prevalence of certain behaviours or actions linked with technology-facilitated violence, abuse and harassment.[50] Self-report and victim surveys were developed in response to the limits of relying exclusively on official crime statistics and are used to register a broader range of harms that are associated with abusive behaviours and which don't necessarily translate into official police or criminal reports. However, scholars such as Douglas et al. have noted that self-report surveys are divorced from the lived experiences of women and children who are most impacted by technology-facilitated violence and abuse. As such, self-report surveys can overlook important findings about the situated "context, meaning, or outcomes" of certain forms of technology-facilitated harassment and control. This gap can lead to an underappreciation of the scale and detail involved in how different types of abuse occur, and, most notably, which can occur in the context of an intimate relationship.[51]

47 Anastasia Powell, Nicola Henry, and Asher Flynn (2018), "Image-based sexual abuse" in *Routledge Handbook of Critical Criminology*, Eds.Walter S. DeKeseredy, Molly Dragiewicz (2018: Routledge).

48 Isobel Lopez-Neira, Trupi Patel, Simon Parkin, George Danezis and Leonie Tanczer (2019), "'Internet of Things': How abuse is getting smarter," *Safe–The Domestic Abuse Quarterly* 63; Leonie Tanczer, Isobel Lopez-Neira, Simon Parkin, Trupi Patel and George Danezis (2018), "Gender and IoT Research Report," <https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf>.

49 Molly Dragiewicz, Jean Burgess, Ariadna Matamoros-Fernandez, Michael Salter, Nicolas P. Suzor, Delanie Woodlock, and Bridget Harris (2018), "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms," *Feminist Media Studies* 18(4).

50 Cynthia Brown and Kelsea Hegarty (2018), "Digital dating abuse measures: A critical review," *Aggression and violent behavior* 40; Holly Johnson (1998), "Rethinking survey research on violence against women," in *On Violence Against Women 9: Rethinking violence against women* Eds. Dobash and Dobash (Thousand Oaks: 1998); Jude McCulloch, Jane Maree Maher, Kate Fitz-Gibbon, Marie Segrave and James Roffee(2016), "Review of the Common Risk Assessment and Management Framework (CRAF): Final Report" *Department of Health and Human Services, Victoria* <https://apo.org.au/node/68283>.

51 Heather Douglas, Bridget A Harris, Molly Dragiewicz (2019), "Technology-facilitated domestic and family violence: Women's experiences," *The British Journal of Criminology* 59(3) at 4.

Academic scholars also conduct extensive qualitative interviews that focus on women's experiences to learn about how technologies are used in the context of domestic family violence.[52] Researchers who adopt this methodology document how abusers utilise technologies to control the everyday activities of victim-survivors; such modes of control pertain to how victim-survivors talk with friends on social media, pay bills, shop, obtain services, seek information, and engage in other forms of digital participation.[53] Such a level of control can present a reality where the perpetrator is omnipresent and deepen the victim's sense of isolation, fear, and anxiety in everyday activities. Notably, this control can also severely undermine prospects for victim-survivors to seek outside help or support without additional fear of repercussion, often which includes threats and physical violence.

The authors of this report acknowledge the enormous value of the aforementioned modes of studying and researching the experiences of victim-survivors of technology-facilitated surveillance. These situated knowledges are essential for comprehensively understanding, and developing responses to, the issue of technology-facilitated violence and abuse. But, as Maher, McCulloch and Fitz-Gibbon incisively note, "how we understand and respond to the differing and shifting implications of privacy in technology-facilitated family violence abuse, as well as how we assign responsibility in relation to this type of violence, will have significant impacts on the safety of women and children."[54]

For this reason our report, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry," builds on the work that registers the lived experiences of victim-survivors who encounter specific forms of technology-facilitated violence and abuse. Given that both the forms and responses to technology-facilitated violence and abuse are conditioned through existing technological systems, legal environments, and digital media environments, we look to these social and technical structures to better understand how they (re) inscribe forms of technology-facilitated violence, discrimination, and exclusion.

52 Heather Douglas, Bridget A Harris, Molly Dragiewicz (2019), "Technology-facilitated domestic and family violence: Women's experiences," *The British Journal of Criminology* 59(3); JaneMaree Maher, Jude McCulloch and Kate Fitz-Gibbon(2017), "New forms of gendered surveillance? Intersections of technology and family violence," In *Gender, Technology and Violence, Segrave and Vitis* (2017: Routledge).

53 Heather Douglas, Bridget A Harris, Molly Dragiewicz (2019), "Technology-facilitated domestic and family violence: Women's experiences," *The British Journal of Criminology* 59(3) at 8.

54 Jane Maree Maher, Jude McCulloch and Kate Fitz-Gibbon (2017), "New forms of gendered surveillance? Intersections of technology and family violence," In *Gender, Technology and Violence, Segrave and Vitis* (2017: Routledge).

We pause, briefly, to make a few comments about some of the terms used in this report. Scholars tend to adopt a range of definitions when advancing specific theoretical or methodological approaches, and practitioners in the constabulary, legal, and support services sectors tend to also adopt uniquely inflected terms and definitions. We acknowledge that each of the many descriptors used to describe 'domestic violence,'[55] 'family violence',[56] 'intimate partner violence,' and 'technology-facilitated coercive control'[57] can each reflect distinct qualitative aspects of the types and impacts of harm, control, and violence that are perpetrated in intimate partner relationships, and that the distinctive qualities of these terms can be amplified when digital media is involved.

We do not attempt to resolve these debates but do, however, believe it is important that we elaborate on our own choices in terminology. Following Dragiewicz et al (2019), we sometimes use the term "technology-facilitated coercive control" to reflect the broad range of harms and violence that arises in the context of abusive and controlling relationships. Within this broader terminological context, we also routinely use the terms 'targeted individual' and 'targeted persons,' particularly in the legal and technical parts of this report. We use these terms to denote both how devices and persons are the subject (target) of malicious uses of stalkerware. In many instances, the uses of these tools are part of a pattern of controlling and abusive behaviour that is often backed by the threat of physical violence. Our use of these terms is not intended to suggest a deprivation of agency, identity, or community from those who are affected by such behaviours and harms. For this reason, we will at times also use the terms 'victim' and 'victim-survivors,' the former to refer to the real human impacts on those affected, and the latter to also register the productive force of survival and community in the face of systemic oppression.

In what follows through the rest of **Part 1**, we identify further key literature that is associated with each major component of this report as set out in the Introduction, namely, the technical assessment of stalkerware (*Part 1.5*, overviewing **Part 2** of the report), findings regarding advertising practices (*Part 1.6*, overviewing **Part 3** of the report), evaluation of corporate policies (*Part 1.7*, overviewing **Part 4**), and

55 The use of the term 'domestic' may imply that violence is occurring only inside a home.

56 The term 'family' might be more broadly inclusive to register the range of harms that are experienced through 'primary' victimisation as well as 'secondary' victimisation.

57 The term 'violence' might artificially constrain description to forms of physical abuse, while 'coercive control' can register a broader range of harms that includes manipulation, deprivation of liberty, coercion, and isolation. See: Evan Stark (2013), "Coercive control," in *Violence against women: Current theory and practice in domestic abuse, sexual violence and exploitation*, Ed. Nancy Lambert and Leslie McMillan (2013: Jessica Kingsley Publishers).

a legal analysis based in consumer privacy law (*Part 1.8*, overviewing **Part 5**). For each of these parts, we highlight where our research either responds to gaps in, or supplements existing elements of, the literature pertaining to the use of stalkerware to facilitate intimate partner violence, abuse, and harassment.

1.5 Technical Assessments of Software Products

Surveys of the technologies associated with intimate partner violence have shown that there are both 'best-of-class' lists which identify potential stalkerware applications to acquire[58] as well as those which canvass the kinds of products which are available to mitigate harms associated with stalking and intimate partner violence.[59] The academic literature has tended to focus on the functionalities of mobile phones, with particular attention paid to GPS capabilities given that location information is often used to escalate remote surveillance activities to physical violence, harassment, or abuse. Such locational information is sometime derived from third-party software, from functionality built into operating systems of phones and motor vehicles, or from freestanding GPS devices.[60]

There are relatively few substantive technical interrogations of stalkerware itself in the academic literature, with Chatterjee et al. perhaps most significantly exploring the intimate partner surveillance ecosystem. Specifically, they built an analysis pipeline from which they determined that the majority of the most problematic spyware applications are dual-use, insofar as they have ostensibly legitimate uses that can also be repurposed for abusive practices.[61] Moreover, similar to Harkin et al., they found that many dual-use developers encourage abusive uses of the application by way of advertisements, blog posts, and customer support services.[62] Of note in Chatterjee, along the rest of the literature, are assertions that stalkerware is relatively rarely detected by anti-virus applications; per Chatterjee, who most extensively examined anti-virus detection rates:

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

59 Lauren F. Cardoso, Susan B. Sorenson, Olivia Webb, Sara Landers (2019), "Recent and emerging technologies: Implications for women's safety," *Technology in Society*.

60 Brenda Baddam (2017), "Technology and Its Danger to Domestic Violence Victims: How Did He Find Me," *Albany Law Journal of Science & Technology* 28(1).

61 Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon Mccoy, and Thomas Ristenpart (2018), "The Spyware Used in Intimate Partner Violence" *2018 IEEE Symposium on Security and Privacy Proceedings* 1.

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

> [o]f the 40 anti-spyware apps, 37 are completely ineffective against dual-use apps, flagging at most 3% of them. Most of the anti-spyware apps flag more than 70% of the off-store spyware apps...All but the one of the top-brand anti-virus providers (e.g., Avast, AVG, Avira, ESET, McAfee, and Kaspersky) detect less than 3% of dual-use apps. **Presumably this reflects their design goals, which do not necessarily include detecting IPS spyware, let alone dual-use apps.**[63]

This is not to say that technical assessments of stalkerware haven't been undertaken more broadly in the public and hacker communities. Vice's *Motherboard* has aggressively reported on the abusive software, collecting stories about payment processors associated with the ecosystem,[64] failures of stalkerware companies to undertake even basic security of the data they harvest from the devices of targeted individuals,[65] and regular hacking of stalkerware companies' infrastructures and technical surfaces.[66] Each of these stories has tended to be based on hackers either accessing the infrastructure used by the stalkerware vendors, reverse engineering stalkerware, or adversarially attempting to penetrate the systems or infrastructure of stalkerware companies.

Stalkerware inhabits a category of abusive software that bears resemblance to that used in the course of criminal and, in some cases, nation-state activities.[67]

---

63 Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon Mccoy, and Thomas Ristenpart (2018), "The Spyware Used in Intimate Partner Violence" *2018 IEEE Symposium on Security and Privacy Proceedings* 1, at 12. Boldface not in original.

64 Joseph Cox and Lorenzo Franceschi-Bicchierai (2019), "PayPal Processes Payments for 'Stalkerware' Software Sold to Abusive Partners," *Motherboard* (February 20 2019) <https://motherboard.vice.com/en_us/article/7xnwa9/paypal-payments-stalkerware-software-abusive-partner>.

65 Joseph Cox and Lorenzo Franceschi-Bicchierai (2018), "'Stalkerware' Website Let Anyone Intercept Texts of Tens of Thousands of People," *Motherboard* (Oct 31 2018) <https://motherboard.vice.com/en_us/article/pa97g7/xnore-copy9-stalkerware-data-breach-thousands-victims>; Lorenzo Franceschi-Bicchierai (2018), "Spyware Company Leaves 'Terabytes' of Selfies, Text Messages, and Location Data Exposed Online," *Motherboard*, (August 23 2018) <https://motherboard.vice.com/en_us/article/9kmj4v/spyware-company-spyfone-terabytes-data-exposed-online-leak>.

66 Lorenzo Franceschi-Bicchierai (2018), "A Hacker Has Wiped a Spyware Company's Servers—Again," *Motherboard* (February 16 2018) <https://motherboard.vice.com/en_us/article/3k7a5k/hacker-wipes-spyware-retina-x-FlexiSPY>; Lorenzo Franceschi-Bicchierai (2017), "Stalkerware Company FlexiSPY Calls Catastrophic Hack 'Just Some False News'," *Motherboard* (April 19 2017) <https://motherboard.vice.com/en_us/article/xyjwpw/FlexiSPY-calls-catastrophic-hack-just-some-false-news>.

67 Diarmaid Harkin, Adam Molnar, and Erica Vowles (2019), "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," *Crime Media Culture*. See also"Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović," *The Citizen Lab* (November 2017) <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf>; Privacy International (2018), "Pay No Attention to the Man Behind the Curtain" (June 2018) <https://privacyinternational.org/sites/default/files/2018-06/Pay%20No%20Attention%20to%20That%20Man%20Behind%20the%20Curtain%20-%20Exposing%20and%20Challenging%20Government%20Hacking%20

The Citizen Lab has a background in technical analyses of such forms of malware, having conducted assessments of sophisticated software used to target politicians, journalists, human rights defenders, and academics,[68] reverse engineered South Korean child monitoring applications,[69] and examined the technical characteristics and security of fitness tracking applications,[70] amongst a wide range of additional malware research. Experience has shown us that engaging in infrastructure mapping—that is, identifying the characteristics and components of the Internet that software relies upon to carry out an actor's nefarious activities—can reveal information about how an application collects, transmits, or secures data.[71] Such information can be helpful in broadening our assessment of how particular software operates and, in some cases, how to recommend that abusive software

for%20Surveillance.pdf>; Joseph Cox (2017), "Military FBI and ICE are Customers of Controversial Stalkerware," *Motherboard* (February 23 2018) <https://motherboard.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware>; Jennifer Valentino-DeVries (2018), "Hundreds of Apps Can Empower Stalkers to Track Their Victims," *The New York Times* (May 19, 2018) <https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html>.

68 John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2017), "Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware (Research Report No.94)," *The Citizen Lab* (June 2017) <https://citizenlab.ca/2017/06/more-mexican-nso-targets/>; John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2019), "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware (Research Report No.117)," *The Citizen Lab* (March 2019) <https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/>; John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2018), "Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague (Research Report No.116)," *The Citizen Lab* (November 2018) <https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/>; John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata (2017), "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links (Research Report No.89)," *The Citizen Lab* (February 2017) <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/>.

69 Fabian Faessler, Geoffrey Alexander, Masashi Crete-Nishihata, Andrew Hilts, and Kelly Kim (2017), "Safer Without: Korean Child Monitoring and Filtering Apps (Research Report No. 100)," *The Citizen Lab* (September 2017) <https://citizenlab.ca/2017/09/safer-without-korean-child-monitoring-filtering-apps/>; Colin Anderson, Masashi Crete-Nishihata, Chris Dehghanpoor, Ron Deibert, Sarah McKune, Davi Ottenheimer, and John Scott-Railton (2015), "Are the Kids Alright? Digital Risks to Minors from South Korea's Smart Sheriff Application (Research Report No. 62)," *The Citizen Lab* (September 2015) <https://citizenlab.ca/2015/09/digital-risks-south-korea-smart-sheriff/>.

70 Andrew Hilts, Christopher Parsons, and Jeffrey Knockel (2016), "Every Step you Fake: A Comparative Analysis of Fitness Tracker Privacy and Security (Research Report No. 69)," *The Citizen Lab* (February 2016) <https://citizenlab.ca/2016/02/fitness-tracker-privacy-and-security/>.

71 Andrew Hilts, Christopher Parsons, and Jeffrey Knockel (2016), "Every Step you Fake: A Comparative Analysis of Fitness Tracker Privacy and Security (Research Report No. 69)," *The Citizen Lab* (February 2016) <https://citizenlab.ca/2016/02/fitness-tracker-privacy-and-security/>; Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune (2015), "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation (Research Brief No. 64)," *The Citizen Lab* (October 2015) <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/>.

be disabled by notifying infrastructure operators.[72] This report leverages all of the aforementioned methods to better answer the technical questions associated with this project. Specifically, emergent from the literature and the Citizen Lab's past experiences, in **Part 2** we asked:

- What are the technical characteristics of stalkerware applications' network traffic?
- What do these characteristics reveal about the stalkerware applications, or the affiliated companies, in question?
- Do anti-virus applications successfully detect stalkerware applications?
- How do stalkerware applications undermine device security?

1.6 Assessments of Corporate Marketing

Spyware companies are heavily invested in selectively marketing their products and services to a broad consumer audience. A closer look at these materials reveals that vendors take a concerted effort to represent their products to prospective consumers through messages of caring for surveillance targets and ensuring their safety. At the same time, these products are well known for their potential to facilitate violence and abuse, and there is a documented history of them facilitating such harms. Furthermore, software sold by these companies tend to introduce or exacerbate risks to personal safety and digital security.[73]

In their systematic empirical study, Harkin et al. (2019) examined images and textual content found on spyware companies' websites and in their marketing materials. The researchers revealed the recurring message that children, intimate partners, employees, and potential thieves are all depicted as legitimate targets of spyware. Applications such as Hoverwatch tell consumers they can "catch a cheating spouse" and The TruthSpy suggests monitoring "your lovers" or "your husband/wife," while FlexiSPY relies on more coded language, stating that the app can "protect your

72 Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ronald Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>; Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune (2014), "Hacking Team's US Nexus," *The Citizen Lab* <https://citizenlab.ca/2014/02/hacking-teams-us-nexus/>.

73 Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon Mccoy, and Thomas Ristenpart (2018), "The Spyware Used in Intimate Partner Violence" *2018 IEEE Symposium on Security and Privacy Proceedings* 1.

relationships."[74] Vendors also took explicit steps to legitimize their product by advertising third-party endorsements from recognisable media outlets, parenting associations, or technology companies.[75] These endorsements were accompanied by customer testimonials that remarked on how using the products could be a parent's "moral duty" or how useful spyware could be for solving relationship problems. Overall, many of the companies suggested, or even encouraged, non-consensual surreptitious surveillance in intimate relations while *simultaneously* attempting to shift any burden of criminal or civil liability away from their own business and onto users.

To date, academic literature that has discussed marketing intelligence platforms has largely focused on how these platforms let businesses utilize business intelligence analytics.[76] More specifically, a marketing intelligence platform is a subscriber-based business analytics tool that provides access to structured data about a company and its competitors' online behaviours. Subscribers to one of these platforms can view items such as the paid Google Adwords that companies purchase, popularly used search terms which are associated with companies' products, social media analytics, and other market related information. Businesses tend to use this information to gain an advantage over competitors. While a burgeoning academic literature on "digital methods" is investigating how to repurpose digital media to study collective phenomena,[77] our reviews of the privacy and surveillance studies literatures have indicated that scholars in these fields have yet to repurpose marketing intelligence platforms when conducting their research. We use marketing intelligence platforms to better understand companies' practices insofar as these platforms offer novel insights into how spyware and stalkerware are marketed and discovered by mass consumer audiences through the medium of search engine intermediaries.

"The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry" examines how vendors selectively represent (and, by extension, legitimize) their own products and services. Specifically, in **Part 3**, we investigated:

74 Diarmaid Harkin, Adam Molnar, and Erica Vowles (2019), "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," *Crime Media Culture*, at 12.

75 Diarmaid Harkin, Adam Molnar, and Erica Vowles (2019), "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," *Crime Media Culture*, at 16.

76 Ee Peng Lim, Hsinchun Chen, and Guoqing Chen (2013), "Business intelligence and analytics: Research directions," *ACM Transactions on Management Information Systems (TMIS)* 3(4), at 17.

77 Tommaso Venturini, Liliana Bounegru, Jonathan Gray, and Richard Rogers (2013), "A Reality Check(List) for Digital Methods," *New Media & Society* 20 (11); Richard Rogers (2013), *Digital methods* (2013: MIT Press).

- What kinds of content are present on stalkerware companies' websites, and does such content reveal a deliberate effort to sell products to facilitate intimate partner surveillance, abuse, or harassment?
- What can we learn about stalkerware companies' practices based on the search keywords they have purchased?
- What can we learn from the organic search terms used to bring individuals to the companies' respective websites?
- To what extent do these methods help researchers gauge the relative interest in stalkerware companies' products and services?

1.7 Corporate Policy Assessments

Companies that want to enter into contractual relationships with customers develop public facing policies and legal documents to ensure that the contracting parties understand the nature of the relationship being developed and services being acquired. Companies selling dual-use products, where the products can be used for ostensibly legitimate as well as abusive functions, are particularly likely to develop such policy documentation to enjoy normalized commercial relationships within the jurisdictions where they do business. Past research examining privacy policies and terms of service have showcased how social media companies as well as fitness tracking companies often differently express how their services, policies, and technologies operate when contrasted against technical assessments of the companies' products or evaluations of internal guidance to law enforcement agencies.[78] Similarly, a range of academics and non-profit organizations have examined the contractual terms of privacy policies to the effect of showcasing the range of activities that companies can take with the data they collect from the persons and devices associated with the respective companies' services or products.[79]

78 See Colin Bennett, Christopher Parsons and Adam Molnar (2014), "Real and Substantial Connections: Enforcing Canadian Privacy Laws Against American Social Networking Companies," *Journal of Law, Information & Science* http://www.jlisjournal.org/abstracts/bennett_etAl.23.1.html; Christopher Parsons, Andrew Hilts, and Masashi Crete-Nishihata (2018), "Approaching Access: A comparative analysis of company responses to data access requests in Canada," *The Citizen Lab* <https://citizenlab.ca/wp-content/uploads/2018/02/approaching_access.pdf>; Andrew Hilts, Christopher Parsons, and Jeffrey Knockel (2016), "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," *The Citizen Lab* < https://citizenlab.ca/2016/02/fitness-tracker-privacy-and-security/>.

79 Aleecia M McDonald and Lorrie Faith Cranor (2008), "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*3; Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle (1999), "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," *E-Commerce* 99; Janice Y. Tsai, Serge Egelman, Lorrie Cranor, Alessandro Acquisti (2010), "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* 22(2); Serge Egelman, Janice Tsai, Lorrie Faith Cranor,

To date, no party has comprehensively examined stalkerware companies' public-facing corporate policy documents. A series of papers have recognized how companies have attempted to indemnify themselves by imposing liability onto the purchaser or user of their applications, where the latter have used their software abusively.[80] The literature has also examined how public-facing materials (e.g., websites) are used to sell mobile apps for ostensibly legitimate as well as abusive reasons.[81] However, none to our knowledge have comprehensively examined the privacy policy and terms of service documents of the companies selling stalkerware.

The Citizen Lab routinely employs corporate policy document assessments in its research reports, and had adopted a common series of questions to streamline assessment processes. This methodology enables us to systematically evaluate how companies present themselves through public legal documentation and, subsequently, to assess where there are commonalities or variances in that legal presentation versus how software technically operates, companies market themselves, or the actual laws and regulations of the countries the companies operate within. Emergent from this line of assessment, in Part 4, we specifically asked:

- Do any policies establish conditions which assert that operators should not surreptitiously install software on the device of any other individual without the latter's explicit and meaningful consent?
- Can the victims of stalkerware-facilitated intimate partner violence, abuse, or harassment contact the relevant companies to learn about the companies' practices and have their information removed or made inaccessible to the offending partner?
- Do policies clearly establish conditions which would prevent offending partners from surreptitiously installing stalkerware on the device of a child who is part of a shared custody situation without the explicit and meaningful consent of the other partner?
- Do the policies recognize the right for the targets of stalkerware to be notified

Alessandro Acquisti (2009), "Timing is everything?: the effects of timing and placement of online privacy indicators," *CHI '09 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

80 Diarmaid Harkin, Adam Molnar, and Erica Vowles (2019), "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," *Crime Media Culture*; Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon Mccoy, and Thomas Ristenpart (2018), "The Spyware Used in Intimate Partner Violence" *2018 IEEE Symposium on Security and Privacy Proceedings* 1.

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

in the case of data breaches, changes to companies' privacy policies, or other ways in which companies might lose control of, or modify terms of accessing, the targeted persons' data?

- Do the policies identify which jurisdictions the companies operate out of and, as such, which country's laws they claim to respect? If so, do any make mention of Canadian law?[82]

1.8 Legal Evaluation of Products

Information Box 2: Accompanying Legal Report

The Citizen Lab has published a legal report, "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," to accompany this report's holistic assessment of stalkerware applications. "Installing Fear" comprehensively canvasses Canada's criminal and civil laws to assess the legality of stalkerware applications and outlines a litany of criminal offenses and causes of action in tort that might be brought against companies which sell stalkerware or individuals who operate the software. "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications" additionally provides a more expansive privacy law analysis and evaluates the potential application of product liability, consumer protection, intellectual property, and intermediary liability law and policy to the development, sale, and operation of stalkerware products and services.

Various actors in the legal system, including legal scholars, practitioners, and the courts, have considered the different kinds of technologies which stalkers might use to facilitate intimate partner violence, abuse, and harassment. Legal scholarship has often focused on ways in which the law inadequately accounts for contemporary modes of digitally-facilitated stalking; for instance, close readings of U.S. law have raised concerns about that jurisdiction's ability to adequately identify the harmful activities associated with technology-facilitated stalking.[83] Even when such forms of stalking are definitely shown to have occurred, or to be occurring, it can be challenging to obtain criminal redress, with Fraser et al. writing:

> … [w]hile law enforcement officers often feel that their hands are tied until the stalker commits an action that is clearly a chargeable offense, they can ensure that the victim knows that she is not to blame for the stalker's behaviour or actions and they are taking the stalking seriously. Additionally, law enforcement might work with the victim and the victim's advocate to identify the evidence that is needed and to help document the necessary information.[84]

We recognize that the legal scholarship continues to broadly investigate how

82 For a comprehensive listing of the questions posed against companies' public policies, see Appendix A.

83 Katherine Fisher Clevenger (2008), "Spousal Abuse through Spyware: The Inadequacy of Legal Protection in the Modern Age," *American Academy of Matrimonial Law* 21(1).

84 Cynthia Fraser, Erica Olsen, Kaofeng Lee, Cindy Southworth (2010), "The New Age of Stalking: Technological Implications for Stalking," *Juvenile and Family Court Journal* 61.

countries' respective criminal and civil codes can (or, in some cases, cannot) be brought to bear against stalkers and abusers. However, in our survey there has been little assessment of how the stalkerware ecosystem intersects with obligations under Canadian privacy legislation. In this report, we evaluated the practices of vendors of stalkerware (including developers where they sell their own apps), and whether these practices were coherent with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).[85] Specifically, in Part 5, we asked:

- Are stalkerware companies accountable under PIPEDA for collecting personal information, engaging in relevant commercial activities, and collecting, using, or disclosing targets' data?
- Do exemptions within PIPEDA or relevant case law mean that stalkerware companies could be removed from the ambit of PIPEDA's reach?
- What does PIPEDA require from stalkerware companies in terms of their privacy obligations and people's privacy rights, and what corresponding activities and practices do those obligations entail? Is it possible for the studied companies to meet such obligations as their apps currently operate, and if so, are they in fact adhering to those obligations?
- To what extent is PIPEDA superior or inferior to the European Union's General Data Protection Regulation, and what lessons might be drawn from the European law?

85 Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Section 2: Technical Assessment of Stalkerware

Academic literature and materials produced by non-profit organizations have tended to focus broadly on the capabilities of stalkerware applications but generally not explored the specific technical operations of the malicious software itself. Technical analysis, however, can be productively employed to gain insights into the operation of software, to the effect of revealing that additional data elements might be exfiltrated in excess of publicly stated data collection practices, that data is poorly secured, or that the software itself exposes an individual's personal information to risk of unauthorized exfiltration or manipulation. Further, such analysis can sometimes reveal insights into a software developer's business associations.

In this section of the report, we analyze a series of technical characteristics of specific pieces of stalkerware in order to gain insights into the products sold by stalkerware vendors. We ultimately conclude that:

- Stalkerware we examined depends on intermediaries, principally located in the United States, Netherlands, and Hong Kong;
- Antivirus products generally identify stalkerware apps as being malicious;
- Google Play Protect can block stalkerware installation and remove installed stalkerware but it may not protect against the newest versions of stalkerware applications until a period of time after they are released; and
- Stalkerware developers insecurely implemented software update systems which exposed targeted persons to risks in excess of those associated exclusively with the abusive surveillance itself.

This section begins by identifying the binaries[86] which are used in our analysis and the justification for focusing exclusively on Android-based stalkerware. Next, we conduct a series of technical analyses which include assessing the network activity associated with some stalkerware, the extent to which stalkerware applications are detected by Android antivirus products, and the effectiveness of the Google's Play Protect system in blocking the applications' functioning. We then evaluate how these applications update themselves and prospectively open targets to greater risks and then discuss the significance of our findings.

86 A binary here refers to a file that contains executable code which can be run on a computer or mobile operating system.

2.1 Case Study Selection

Throughout this report we look at the binaries denoted in Table 3:

Product	Downloaded Filename	SHA1 Hash	Date APK Obtained
Cerberus	Cerberus_disguised.apk	120e8faebcaed49cc1e8c6d4481837c2de1f4557	January 22, 2018
FlexiSPY	flexispy_5002_3.0.1.apk	c0feffbfa7bb7898091e749520f14ea0d7cf6b8b	August 12, 2018
Hoverwatch	hoverwatch-setup-fovmf.apk	58db76c503527432f8d3c4c4bddf1ed3160eb2f7	January 22, 2019
MSpy	mspy_android.apk	123eec42e4632d88f3b8844e4221ba6e853a5cb3	July 20, 2018
TheTruthSpy	TheTruthSpy.apk	46fe77c63a069a83f8dc77c852be458919e7700d	January 25, 2018
TheTruthSpy	TheTruthSpy-2.apk[87]	c8ba88fab5801d3ba3376bef592a91331c454d93	January 18, 2019

Table 3: Binaries Used for Technical Analysis

All of these files were downloaded directly from the official websites of the developers.

As noted in Part 1.2 and 1.3, we focused on Android-based stalkerware over the course of this research study; this focus is reflected in the files chosen for our analysis. In all cases within our sample, except that of FlexiSPY and TheTruthSpy, applications which targeted iOS devices depended on the stalkererware operator obtaining the iCloud login and password of the targeted person. Services would then use this login and password set to automatically extract data from iCloud—which includes contacts, calendar information, photos, notes, geolocation, and potentially even files stored in iCloud drive—and make it available to the stalker.

In contrast to most iOS-based stalkerware activities, stalkerware designed for Android-devices involves actually installing the malware on the device. Furthermore, we know based on academic and non-profit organizations' literature that surveillance of mobile devices raise significant risks because operators can use the data from such devices to engage in particularly serious and threatening intimate partner violence, abuse, and harassment. For these reasons, this section of our report exclusively focuses on Android-based stalkerware, and to the exclusion of that which relies on iCloud passwords or which might be installed on desktops of laptops or other personal computing devices.

87 We are adding the -2 to the filename throughout this report even though the original filename was "TheTruthSpy.apk" we do this to differentiate from the first version which is also named "TheTruthSpy.apk".

2.2 Technical Assessments

2.2.1 Network Activity

We initially examined the network activity of each of the applications so as to generate a list of network indicators that could potentially be used by users or network administrators to determine whether these applications are running on their networks. We were also interested in looking at the hosting environments of the different applications and the jurisdictions through which the data transits during regular usage of the applications. Specifically, such assessment can be useful because the legal protections, regulations, and exposures may vary as data crosses legal jurisdictions.

We ran each of the applications and kept a record of which domains were being requested to determine network activity.[88] We then resolved each of the domains to an IP address; in cases where there was more than one response, we noted each resolution as a separate entry. For each unique IP address, we obtained network information using the GeoIP ASN database provided by MaxMind API[89]. Where it is noted, we obtained additional historical DNS data from the SecurityTrails DNS service. Table 4 summarizes the geolocation information that was associated with the IP addresses we observed while the stalkerware applications were running:

App	Domain	IP	Country	ASN Name	ASN #
Cerberus	www.cerberusapp.com	66.228.35.203	United States	Linode, LLC	63949
FlexiSPY	admin.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
FlexiSPY	admin.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
FlexiSPY	api.flexispy.com	180.150.144.84	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
FlexiSPY	blog.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
FlexiSPY	blog.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
FlexiSPY	client.mobilefonex.com	180.150.156.198	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
FlexiSPY	community.flexispy.com	104.25.91.115[90]	United States	Cloudflare, Inc.	13335
FlexiSPY	community.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335

88 We accessed all of these domains on September 7, 2018, with the only exception being Cerberus on May 3, 2018.

89 The two databases used were using definitions named “GeoLite2-ASN-1543969259” and “GeoLite2-Country-1543969259” provided by the Maxmind API.

90 “Historical DNS data: flexispy.com” *SecurityTrails.com* (Accessed May 14, 2019) <https://securitytrails.com/domain/www.flexispy.com/history/a>.

App	Domain	IP	Country	ASN Name	ASN #
FlexiSPY	ecom.flexispy.com	180.150.144.85	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
FlexiSPY	portal.flexispy.com	180.150.144.87	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
FlexiSPY	push.mobilefonex.com	180.150.156.193	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
FlexiSPY	www.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
FlexiSPY	www.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
mSpy	a.thd.cc	46.166.133.55[91]	Netherlands	NForce Entertainment B.V.	43350
mSpy	cp.mspyonline.com	104.25.84.24	United States	Cloudflare, Inc.	13335
mSpy	cp.mspyonline.com	104.25.85.24	United States	Cloudflare, Inc.	13335
mSpy	pipe.thd.cc	104.31.95.14	United States	Cloudflare, Inc.	13335
mSpy	pipe.thd.cc	104.31.94.14	United States	Cloudflare, Inc.	13335
mSpy	repo.mspyonline.com	104.25.85.24	United States	Cloudflare, Inc.	13335
mSpy	repo.mspyonline.com	104.25.84.24	United States	Cloudflare, Inc.	13335
mSpy	thd.cc	104.31.94.14[92]	United States	Cloudflare, Inc.	13335
mSpy	thd.cc	104.31.95.14	United States	Cloudflare, Inc.	13335
mSpy	www.mspyonline.com	104.25.85.24	United States	Cloudflare, Inc.	13335
mSpy	www.myspy.com	104.20.20.58	United States	Cloudflare, Inc.	13335
mSpy	www.myspy.com	104.20.21.58	United States	Cloudflare, Inc.	13335
TheTruthSpy	my.thetruthspy.com	69.64.74.242	United States	Codero[93]	18501
TheTruthSpy	protocol-a735.thetruthspy.com	69.64.91.29	United States	Codero	18501
TheTruthSpy	protocol-a739.thetruthspy.com	69.64.91.29	United States	Codero	18501
TheTruthSpy	setupmail-a739.icloudappe.com	69.64.91.29	United States	Codero	18501
TheTruthSpy	thetruthspy.com	66.226.73.96	United States	Codero	18501
TheTruthSpy	www.thetruthspy.com	66.226.73.96	United States	Codero	18501

Table 4: Table of Geolocation Information Associated with Stalkerware Applications

91 "Historical DNS data: 'a.thd.cc'" *SecurityTrails.com* (Accessed May 14, 2019) <https://securitytrails.com/domain/a.thd.cc/history/a>.

92 "Historical DNS data: 'a.thd.cc'" *SecurityTrails.com* (Accessed May 14, 2019) <https://securitytrails.com/domain/a.thd.cc/history/a>.

93 As of March 26, 2019, Codero has asked and subsequently taken the content relating to TheTruthSpy down from their servers. See Lorenzo Franceschi-Bicchierai (2019), "Hosting Provider Finally Takes Down Spyware Leak of Thousands of Photos and Phone Calls"*Motherboard* (March 26, 2019) <https://motherboard.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy>.

For all the unique IPs observed during runtime, the country distribution for the products are summarized in Table 5:

App Name	Infrastructure Location Distribution
Cerberus	100% United States (Linode)
FlexiSPY	60% United States (CloudFlare) and 38% Hong Kong (Rackspace)
mSpy	92% United States (CloudFlare) and 8% Netherlands (NForce)
TheTruthSpy	100% United States (Codero)

Table 5: Geographic Distribution of Unique IPs when running Stalkerware

The only three countries that we saw hosting the infrastructure used by these applications were located in the United States (81.3%), Hong Kong (15.6%), and the Netherlands (3.1%). The specific networks used were CloudFlare (59.4%), Codero (18.8%), and Rackspace (15.6%); Linode and NForce each had a single IP and each accounted for 3.1% of the used infrastructure.

2.2.2 Measuring Protection from Commercial Anti-Virus Products

We examined the extent to which antivirus software and network security products detected the binaries listed in **Part 2.1** as malicious. This examination involved using results from the VirusTotal API.[94] VirusTotal describes itself as a "service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content."[95] The service conducts these analyses by aggregating information from up to "70 antivirus scanners and URL/domain blacklisting services."[96]

VirusTotal lacks a commercial incentive to prefer one vendor over another, and the company has written that "[t]hough we work with engines belonging to many different organizations, VirusTotal does not distribute or promote any of those third-party engines. We simply act as an aggregator of information. This allows us to offer an objective and unbiased service to our users."[97] Although VirusTotal exposes the virus definition information for a wide variety of files, the service does not constitute a good measure of the relative quality of one antivirus engine over another.

94 "Getting Started" *Virus Total* (Accessed May 14, 2019) <https://developers.virustotal.com/v2.0/reference#getting-started>.

95 "About Us" *Virus Total* (Accessed May 14, 2019) <https://support.virustotal.com/hc/en-us/sections/115000720829-About-us>.

96 "How it works" *Virus Total* (Accessed May 14, 2019) <https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works>.

97 "How it works" *Virus Total* (Accessed May 14, 2019) <https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works>.

In this section, we relied on VirusTotal to determine whether stalkerware companies' Android APK files would be detected by security products. We hasten to note we did not carry out this assessment to evaluate the quality of one security product over another. As an extreme hypothetical example, if an antivirus product tagged every file as suspicious regardless of content, it likely would not be a useful product to a user but would reflect quite positively when looking solely at VirusTotal results. VirusTotal itself recognizes this possible situation and, thus, states on their website that it is not a tool to compare the quality of security products.[98]

We used the APK files we possessed to determine the version number from the contained AndroidManifest.xml file.[99] We then checked all of the hashes on VirusTotal's website. We did not submit the files themselves directly to VirusTotal because we were only interested in determining whether the files we possessed would likely be detected by security products aggregated in VirusTotal. Since we did not submit the files, but only referred to previously submitted scans done by VirusTotal, the scans could have been performed during different times. As a result of this, the number of antivirus engines consulted can vary from one scan to another. We noted all of the cases in which the web interface of VirusTotal indicated a positive (malicious) value. The summary of the overall detections across all engines is presented in Table 6:

Product	Filename	APK Version	Positive Count	Engines Used	% Positives
Cerberus	Cerberus_disguised.apk	3.5.2	6	63	9.5%
FlexiSPY	flexispy_5002_3.0.1.apk	3.0.1	34	63	54.0%
Hoverwatch	hoverwatch-setup-fovmf.apk	6.3.260	22	59	37.3%
mSpy	mspy_android.apk	5.3.0	20	63	31.7%
TheTruthSpy	TheTruthSpy.apk	N/A	0	0	0.0%
TheTruthSpy	TheTruthSpy-2.apk	N/A	0	0	0.0%
				MEAN	***22.1%***

Table 6: Overall Antivirus Detection of Stalkerware Applications

98 "Support: Why do not you include statistics comparing antivirus performance?"*Virus Total* (Accessed May 14, 2019) <https://support.virustotal.com/hc/en-us/articles/115002094589-Why-do-not-you-include-statistics-comparing-antivirus-performance->.

99 The AndroidManifest.xml file is a file in an Android APK that contains information such as the application's name, version, and required permissions.

Overall, these files seemed to be well known by security product vendors. Only files that were associated with TheTruthSpy were never detected by any engine. All other products were detected as malicious by six to 34 security products. FlexiSPY was the most frequently detected with 34/63 (54%) detection rate. Overall in our sample, we see a mean of 22.1% chance of detection. As the aim and detection techniques used in antivirus products differ greatly, a detection rate of 100% is neither likely nor expected. Generally, when five or more antivirus engines detect an apk as a malware, we presume that the engines are not registering a false positive; the greater number of detections which identify a given file increases the overall confidence that the file is malicious.[100]

A more detailed breakdown of the security products that detected one or more of the stalkerware applications as malicious is presented in Table 6.

Security Product	Cerberus	FlexiSPY	Hoverwatch	MSpy	TheTruthSpy
AegisLab	X	X			
AhnLab-V3		X	X	X	
Alibaba		X		X	
Avast		X			
Avast-Mobile		X	X		
AVG		X			
Avira (no cloud)		X	X	X	
Babable	X	X	X	X	
Baidu		X			
BitDefender		X			
CAT-QuickHeal		X	X	X	
Comodo			X		
Cyren	X	X	X	X	
DrWeb		X	X	X	
Emsisoft		X			
eScan		X			
ESET-NOD32		X	X	X	
F-Secure		X	X		
Fortinet		X	X	X	
GData		X			
Ikarus		X	X	X	
Jiangmin		X			

100 Sophos (2019), "How to investigate and resolve a potential False Positive or Incorrect Detection" *Sophos Community Beta* (Accessed May 14, 2019) <https://community.sophos.com/kb/en-us/128136>.

Security Product	Cerberus	FlexiSPY	Hoverwatch	MSpy	TheTruthSpy
K7GW		X	X		
Kaspersky		X	X	X	
MAX		X	X	X	
McAfee		X	X	X	
NANO-Antivirus		X	X	X	
Qihoo-360		X	X	X	
Sophos AV	X	X		X	
Symantec		X	X	X	
Symantec Mobile Insight	X	X	X	X	
Tencent		X			
TrendMicro-HouseCall		X		X	
Trustlook	X		X		
ZoneAlarm by Check Point		X	X	X	
Zoner		X			

Table 7: Positive (Malicious) Detections by Antivirus Engines

Since we looked at Android APKs, we also had to determine which of the antivirus engines listed in Table 7 had Android versions of the engines. To determine this, we first looked at reporting done by AV Tests GmbH,[101] an organization that describes itself as an "independent research institute for IT security from Germany." The organization has produced comparative reports on security products for over 15 years[102] and lists Android-based antivirus products. We mapped these products to the VirusTotal engine names. For those that did not appear on the most recent Android AV Tests list,[103] we used Google and searched for "{engine name} antivirus android" to see if any official sources provided Android versions. We found that most of the engines which returned positive detections appeared to have an Android version; the only exceptions were for Babable, Jiangmin, and NANO-Antivirus. In these latter three instances, we were unable to find a version that was advertised for Android.

Among all the antivirus products, the only ones which detected four out of the five examined stalkerware apps were: Babable, Cyren, and Symantec Mobile Insight.

101 "The best antivirus software for Android," *AV Test* (Accessed May 14, 2019) <https://www.av-test.org/en/antivirus/mobile-devices/>.

102 "About the Institute," *AV Test* (Accessed May 14, 2019) <https://www.av-test.org/en/about-the-institute/>.

103 "The best antivirus software for Android," *AV Test* (Accessed May 14, 2019) <https://www.av-test.org/en/antivirus/mobile-devices/>.

We were also interested in whether the antivirus engines detected these applications explicitly or whether a more generic detection was being performed. Specifically, we were interested in determining whether a detection was based on heuristics or if a particular signature was generated for a given product. To determine this, we looked at the name given by the antivirus engine to see if the name of the product was used in the detection. Table 8 denotes the detection names assigned to the different spyware by the antivirus products which detected the spyware as malicious.

Product	Antivirus	Detection Name	Update
Cerberus	Sophos AV	Android Cerberus Disguised (PUA)	20180618
FlexiSPY	Avast	Android:KillerMob-P [Trj]	20180608
FlexiSPY	Avast-Mobile	Android:KillerMob-P [Trj]	20180607
FlexiSPY	AVG	Android:KillerMob-P [Trj]	20180608
FlexiSPY	BitDefender	Android.Monitor.Killermob.C	20180608
FlexiSPY	CAT-QuickHeal	Android.Killermob.GEN7590 (PUP)	20180608
FlexiSPY	Emsisoft	Android.Monitor.Killermob.C (B)	20180608
FlexiSPY	F-Secure	Android.Monitor.Killermob.C	20180608
FlexiSPY	Ikarus	PUA.AndroidOS.Killermob	20180608
FlexiSPY	eScan	Android.Monitor.Killermob.C	20180608
Hoverwatch	Avira (no cloud)	SPR/ANDR.Hoverwatch.rwsil	20190320
Hoverwatch	ESET-NOD32	a variant of Android/Monitor. Hoverwatch.F potentially unsafe	20190320
Hoverwatch	F-Secure	PrivacyRisk.SPR/ANDR.Hoverwatch	20190320
Hoverwatch	Fortinet	Adware/Hoverwatch!Android	20190320
MSpy	AhnLab-V3	Android-Spyware/MSpy.7a40d	20180602
MSpy	Avira (no cloud)	SPR/ANDR.Mspy.ofgui	20180602
MSpy	CAT-QuickHeal	Android.Mspy.A (PUP)	20180602
MSpy	DrWeb	Program.MSpy.7.origin	20180603
MSpy	ESET-NOD32	a variant of Android/Monitor.Mspy.J potentially unsafe	20180603
MSpy	Fortinet	Adware/Mspy!Android	20180603
MSpy	Kaspersky	not-a-virus:HEUR:Monitor. AndroidOS.Mspy.a	20180603
MSpy	NANO-Antivirus	Riskware.Android.Mspy.fdihek	20180603
MSpy	ZoneAlarm by Check Point	not-a-virus:HEUR:Monitor. AndroidOS.Mspy.a	20180603

Table 8: Positive (Malicious) Detections by Antivirus Where the Product is Referenced in the Detection Name

We found that 23/82 (28.05%) of positive detections mentioned the name of the product in the detection. This result may indicate that there had been at least some

determination by those antivirus vendors that the specific application would be unwanted by customers and not a generic detection based on risky behaviours or heuristics. Within this list, detection names also vary in how strongly the names identify something as malicious from potentially (e.g., "a variant of Android/Monitor. Mspy.J potentially unsafe" and "PUA.AndroidOS.Killermob") to more firm (e.g., "Riskware.Android.Mspy.fdihek" and "Android:KillerMob-P [Trj]"). The names given to the detections provide some visibility into how antivirus companies perceive these products: either as something outright malicious or something only potentially unwanted by a user. Specifically, PUA and PUP are terms meaning "Potentially Unwanted Application" and "Potentially Unwanted Program," respectively, and are commonly used by antivirus and security industry vendors. In contrast, TRJ likely refers to Trojan in this detection name. For FlexiSPY, we often see it detected as "killermob" though we are unsure why. This may be a reference to Killer Mobile, which is another manufacturer of similar software.[104]

2.2.3 Measuring the Protection Provided by Google Play Protect

Android phones with the Google Play Store installed are protected against malicious applications using a system called Google Play Protect. It is an antivirus-like service that scans applications that have been sideloaded (i.e., installed onto the phone from outside of the Google Play Store). Google Play Protect scans sideloaded applications before they are installed and, if they are identified as malicious, prevents their installation. However, Google Play Protect can be disabled from the Google Play Store, allowing someone with access to the phone to bypass Play Protect's restrictions. Many of the applications that we analyzed included instructions to disable Play Protect, suggesting to us that Play Protect may identify the applications as malicious. However, Play Protect can be re-enabled to trigger it to manually scan installed applications and prompt the user to uninstall any applications that are identified as malicious.

We performed the following experiment to determine whether, and with what consistency, Google Play Protect provides protection from stalkerware applications. Specifically, we attempted to sideload the following applications on a non-rooted Motorola G5 phone with Android 7.1 installed:

- (Disguised) Cerberus 3.5.3 (downloaded 2018-01-21)

104 Thomas Brewster (2017), "Meet The 'Cowboys Of Creepware' – Selling Government-Grade Surveillance To Spy On Your Spouse," *Forbes.com* (February 16, 2017) <https://www.forbes.com/sites/thomasbrewster/2017/02/16/government-iphone-android-spyware-is-the-same-as-seedy-spouseware>.

- TheTruthSpy (2018-01-23)
- mSpy 5.3.0 (2018-04-03)
- FlexiSPY 3.0.1 (2018-04-18)
- TheTruthSpy (downloaded 2019-01-18)

Versions were determined by examining each application's version string in AndroidManifest.xml. Dates were determined as self-reported in the zip header of each application's APK. Some applications did not report a version string; in such cases, we reported the date that the APK was downloaded.

There was a version of Cerberus available through the Play Store which Play Protect did not identify as malicious. However, we tested a "disguised" version of the application that is available through Cerberus's website. This disguised version features a name and icon which were designed to mislead a user into thinking that the application was an Android OS service. This sort of deception of appearance was consistent with the other applications analyzed in this section, insofar as they also sought to conceal their presence on the device on which they were installed.

We attempted installations on January 18, 2019 and January 22, 2019. We found that all but Cerberus and TheTruthSpy (downloaded 2019-01-18) were blocked from installation by Play Protect on January 18, 2019. The older version of TheTruthSpy (January 23, 2018) was blocked at this time. When testing on January 22, 2019, we found that the newer version of TheTruthSpy (downloaded January 18, 2019) was also blocked, but Cerberus was still not. We postulate that Cerberus may not have been blocked because a non-disguised version was available in the Google Play Store. These installation periods and results are denoted in Table 9:

Application	Date	Blocked January 18 2019	Blocked January 22 2019
(Disguised) Cerberus 3.5.3	Downloaded 2018-01-21	N	N
TheTruthSpy	2018-01-23	Y	Y
mSpy 5.3.0	2018-04-03	Y	Y
FlexiSPY 3.0.1	2018-04-18	Y	Y
TheTruthSpy	Downloaded 2019-01-18	N	Y

Table 9: Google Play Protect Results

Given that the most recent version of TheTruthSpy was not blocked on January 18, 2019, this suggests to us that Google Play Protect may only block newer versions of

stalkerware apps after a period of days. Further evidence to support this position comes from the FlexiSPY support team. On their support forums, in expressing their frustration with attempting to defeat Play Protect, which had reportedly also begun deleting FlexiSPY without prompting, FlexiSPY reported the following:

> "Please be informed that we just released the new version (3.5.7) yesterday. You may try this version, but unfortunately it might be detected again within a day or two. Please understand that the software might be detected by Play Protect again."[105]

We analyzed the differences between FlexiSPY versions 3.5.6 and 3.5.7 and found only minimal differences. These consisted only of changes to the version code and number in the AndroidManifest.xml file and changes to the version number referenced by the compiled Java code. These observably small differences to the code suggest that only minimal changes are required for stalkerware developers to evade Play Protect but that this evasion may only last days. However, future work is required to systematically measure how often stalkerware developers release new versions of their software, to measure which versions evade Play Protect protection, and to measure how much time Play Protect requires before detecting the new versions.

For all applications that were blocked from being installed by Google Play Protect, we also tested whether they were removed if Google Play Protect were disabled, the application installed and run, and then Google Play Protect were re-enabled. We found that in each case, Google Play Protect would prompt the user to remove each application after Play Protect was enabled by presenting a prompt with an uninstall option. This suggests that enabling Google Play Protect on phones where it has been disabled may be an effective approach to identifying and removing stalkerware in cases where the stalkerware has been installed on non-rooted mobile devices.[106] However, a rigorous investigation of this is still required to test this hypothesis.

2.2.4 Vulnerabilities in Stalkerware Update Processes

Android applications generally receive updates securely via the Google Play Store. However, stalkerware applications are often excluded from the Google Play Store due to their malicious nature. As a result, stalkerware developers cannot utilize the Play Store's secure update system, meaning that stalkerware developers are responsible for developing updates to their applications and, also, for the security

105 "Google Play Protect Issue" *Flexispy.com* (Accessed May 14, 2019) <https://community.flexispy.com/index.php?/topic/2048-google-play-protect-issue/&do=findComment&comment=9385>.

106 On rooted devices, malicious applications can hide themselves in the file system in arbitrarily complex ways such that they are no longer uninstalled when the application is uninstalled.

of their update processes. An insecure update process does not authenticate downloaded code, which could enable a third-party adversary in a man-in-the-middle position to inject and install an arbitrary application instead of the intended update. Such an adversary could include anyone in a position in between the stalkerware victim and the stalkerware control servers, and who has the ability to selectively modify data communication. This would allow the adversary to run arbitrary software on the targeted person's device, thus enabling both the operator of the stalkerware and the additional third-party to maliciously surveil or operate the targeted person's mobile device.

In a stock Android system and on a non-rooted phone, the only way for an application to update itself involves the application requesting that the operating system install an APK using the Android Intents API.[107] Using this API, the application is responsible for ensuring the authenticity of the APK, such as whether the APK is in fact an updated version of itself as opposed to malicious code injected by an adversary. When invoked, this API presents the same prompt to the user as if they had downloaded an APK from the browser. In fact, this is one way an application can update itself using this API: it can open a browser page and instruct the user to download and install the application. In such cases, the browser downloads the APK and invokes the Intents API to install the APK. An application can ensure the authenticity of the update by using technologies such as HTTPS.

Another, less roundabout, way for the application to update itself is to download the APK itself and then directly invoke the Intents API to install it. This method eliminates the need to use a browser but requires more code and, thus, puts a greater onus on the application developer to ensure the authenticity of the update. However, an application can be designed to ensure the authenticity of the update with the use of HTTPS or by checking the version and digital signature of the downloaded file.

Since the Intents API prompts the user to install the application update, the use of the API risks revealing the installation of the application. In the case of stalkerware, this side effect may be undesirable by the stalkerware developers who routinely design their software to hide itself from the target. To work around this, on a rooted phone, application developers have additional options. The typical work around is to use an in-built executable utility called "pm" to install the application. From a shell, an example invocation of the utility to install an application that is not currently installed would appear as follows:

107 "Intent," *Android Developers* (Accessed May 16, 2019) <https://developer.android.com/reference/android/content/Intent>.

```
$ pm install myapp.apk
```

To replace an installed application with a later version, one would add the “-r” option as follows:

```
$ pm install -r myapp.apk
```

Using the “pm” utility may be preferred by stalkerware developers because it does not display a prompt to the target and, thus, reduces the likelihood that the application’s installation will be detected. If an application is updated by first being uninstalled and then installed without the “-r” option, then no authentication is performed. However, if the application is updated in place with the “-r” option, then the replacement APK is verified to have both a larger version code than that of the one being replaced and it is verified to be signed with the same digital signature. This verification would restrict a third-party attacker to injecting and installing any APK which had a higher version code than the installed stalkerware and the same digital signature as any other installed application on the phone.

A final way for an application to update itself is not to update the application on the operating system level at all. Instead, modular updates to the application may be downloaded as Java *.jar files or native shared object libraries and then loaded dynamically. This approach to updating the application enables selective updating of parts of its code in a similar fashion as that of a web browser updating its extensions. This functionality does not require root permissions and can be performed without any prompt to the user. However, this approach generally requires greater implementation complexity than utilizing the operating system to perform updates. Although this sort of functionality is not permitted by the Google Play Store, most stalkerware applications are already excluded from the Play Store due to their malicious nature. With this update approach, the onus of ensuring the authenticity of the downloaded updates is on the application developer.

To determine if stalkerware apps excluded from the Play Store include code to update themselves and, if so, whether that code is vulnerable to malicious attack via lack of sufficient authentication, we performed the following analysis. To ascertain whether an application used the Intents API to install updates we used the search tool “grep” to search the given application’s code for the pattern ‘setDataAndType.’ This pattern is an API call that is required to install an APK using Intents. To determine whether an application updates itself on a rooted phone using the pm

utility, we searched its code for '\<pm\>.' To determine if the application used a dynamic approach to update itself modularly, we searched its code for '\.jar\>' and '\.so\>.' Finally, as a broader measure, we also searched for 'update' and 'upgrade' (case insensitively). For each match in the code, we manually analyzed the code to determine if it was being used for installing updates. If so, we examined whether the code was being used and if it was vulnerable to attack. We applied this analysis to the following apps:

- (Disguised) Cerberus 3.5.3 (downloaded 2018-01-21)
- TheTruthSpy (2018-01-23) and TheTruthSpy (downloaded 2019-01-18)
- mSpy 5.3.0 (2018-04-03)
- FlexiSPY 3.0.1 (2018-04-18)
- Hoverwatch 6.3.260 (downloaded 2019-01-22)

We describe the result of this analysis for each of these applications in the following sections.

2.2.4.1 Cerberus

The disguised version of Cerberus that we analyzed was available from the company's website and not through the Google Play Store. We found that this disguised version had the functionality to self-update through the application. The application contains code to obtain the latest version from the following URL:

```
hxxp://www.cerberusapp[.]com/download/version
```

At the time of this writing (April 8, 2019), the resource at this URL was a string that contained the latest version code ("283620"). If the latest version was more recent than the installed version, the user was redirected to download an update from the following URL in a Web browser:

```
hxxps://www.cerberusapp[.]com/get
```

Since checking for the latest version was performed without cryptographic protection, a malicious actor in a man-in-the-middle position could trick the application into not downloading an available update, despite the existence of one. However, since updates were provided by a fixed SSL-encrypted Web page there was no room for a malicious actor to inject arbitrary code. This matters because such arbitrary code could enable an adversary to run malicious code in excess of

the surveillance capabilities integrated into the stalkerware, or could run similar malicious code but exfiltrate the information to the adversary who injected the malicious code.

2.2.4.2 TheTruthSpy

We did not find self-updating functionality in either version of TheTruthSpy that we analyzed.

2.2.4.3 mSpy

We found code in the version of mSpy that we analyzed that implemented self-updates. Two methods were implemented: the Intents API on a non-rooted phone and the pm utility on a rooted phone. The code snippet, below, shows both code branches, the first showing when the phone is rooted and the second when it is not.

```
if (this.d || com.droid.mob.display2.application.e.a.aD()) {
    PackageUpdateService.a.b(“Installing update with root”);
    g.a(packageUpdateService$PackageDownloadResult.b);
    this.c(packageUpdateService$PackageDownloadResult);
} else {
    PackageUpdateService.a.b(“Prompt install update”);
    final Intent intent = new Intent(“android.intent.action.
VIEW”);
    intent.setFlags(0x10000000);
    intent.setDataAndType(Uri.fromFile(new
File(packageUpdateService$PackageDownloadResult.b)),
“application/vnd.android.package-archive”);
    this.getApplicationContext().startActivity(intent);
}
```

In the rooted branch of the above code, the following function is called to install the downloaded update:

```
public static void a(final String s) {
    a(new String[] { “chmod 755 “ + s, “pm install -r “ + s });
}
```

Unlike the Intents API branch of the code, the rooted branch would provide version code and digital signature verification as it uses the “-r” option. However, neither of these branches appeared to be actively used; we draw this conclusions because checks for updates always failed. The URL to check for updates was generated by

the following Java code, which dynamically built the URL from a given hostname:

```
String.format("%s/update.
php?passkey=aXDKqBfPNd3kGpoTRrVa&package=%s", com.droid.
mob.display2.application.e.a.a().j(), MApplication.a().
getPackageName());
```

However, the hostname for updates was blank. As a result the check for updates would always fail due to the generated URL being malformed:

```
h.ai = this.a(this.c(e, "autoupdate_url"), "host", "");
```

Thus, self-updating might not have been activated in the version of mSpy that we analyzed.

Since the branch used by non-rooted phones which invoked the Intents API did not provide any authentication and the branch used by rooted phones only provides partial verification, we investigated whether any authentication such as SSL was provided by the network when updating. We found that both the check for updates and the download of the new APK was done using the Java "HttpURLConnection" API. This Java interface does not provide SSL authentication. Moreover, we found no other authentication in the code; as such, we conclude that if the self-updating code in mSpy were used on a non-rooted phone then it would be vulnerable to man-in-the-middle attacks such that an adversary in a man-in-the-middle position could install arbitrary software onto the targeted person's mobile device. On a rooted phone, the victim would be vulnerable to a third-party adversary only installing any APK which had a higher version code than the installed stalkerware application and the same digital signature as any other application currently installed on the phone.

2.2.4.4 FlexiSPY

FlexiSPY advertised its ability to update remotely[108] and, specifically, that they "are one of the only spy apps on the market to offer this feature." Previous analysis[109] and proof of concept exploit code[110] has shown that FlexiSPY performs insufficient authentication of downloaded updates and that it is vulnerable to attacks that enable an adversary to install arbitrary applications onto the targeted person's

108 "Update Flexispy Remotely" *Flexispy.com* (Accessed May 14, 2019) <https://www.flexispy.com/en/features/update-flexispy-remotely.htm>.

109 "Flexispy for Android Backdoor" *Flexispy.com* (Accessed May 14, 2019) <https://web.archive.org/web/20170801132528/https://ht-sec.org/flexispy-for-android-backdoor/>.

110 "Flexispy POC," *Github.com* (Accessed May 14, 2019) <https://github.com/fatal0/FlexiSpyPOC>.

mobile device. These attacks include man-in-the-middle attacks on the update process, but, since the application on a rooted phone also listens for commands on an open port, it is also vulnerable to attack by anyone who can connect to that port, such as by someone on the same Wifi network as the victim's mobile device or Internet users in general if the victim's mobile device is connected to the Internet and not protected by a firewall.

We have confirmed that these vulnerabilities still existed in the version of FlexiSPY that we analyzed and that the application could still be exploited by a third-party adversary to install arbitrary applications on a victim's phone.

We found that FlexiSPY only supported updates on a rooted phone and that updates are triggered via a remote update command. Although the application used the "pm" utility to install the replacement APK, it did not update in place using the "-r" option. Rather, it first used a separate daemon running beside the main application to uninstall the main application:

```
Object[] a4 = new Object[1];
a4[0] = s;
a0.a(String.format("pm uninstall %s", a4));
android.os.SystemClock.sleep(1000L);
Object[] a5 = new Object[1];
a5[0] = s;
a0.a(String.format("am force-stop %s", a5));
Object[] a6 = new Object[1];
a6[0] = s;
a0.a(String.format("pm disable %s", a6));
```

As a result, when the new application APK was installed, the "pm" utility performed no verification of the APK's digital signature or version code.

We found no other cryptography protecting the update process either. The remote update command that instructs the FlexiSPY application to download and install an APK included the link of the replacement APK and its CRC32 checksum. However, as the command itself is sent without any cryptographic protection, the download link and the checksum could be arbitrarily chosen by a third-party adversary. As a result, rooted phones running this version of FlexiSPY are at high risk to third-party exploitation.

2.2.4.5 Hoverwatch

We found code that implemented self-updates using two methods in the version of Hoverwatch that we analyzed. Hoverwatch included code to update via the Intents API:

```
ac.a(“CrFn”, “Inf: install “.concat(String.valueOf(d)));
Intent intent = new Intent(“android.intent.action.VIEW”);
intent.setFlags(0x10000000);
intent.setDataAndType(Uri.fromFile(new File(d)), “application/
vnd.android.package-archive”);
CoreApplication.a.startActivity(intent);
```

Hoverwatch also included code using the pm utility to self-update on a rooted phone:

```
if (file != null && file.exists() && file.isFile() && file.length()
> 0) {
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append(o);
    stringBuilder.append(“\n”);
    String stringBuilder2 = stringBuilder.toString();
    StringBuilder stringBuilder3 = new StringBuilder();
    stringBuilder3.append(stringBuilder2);
    stringBuilder3.append(“pm install -r “);
    stringBuilder3.append(file.getAbsolutePath());
    stringBuilder3.append(“ \n”);
    stringBuilder2 = stringBuilder3.toString();
    stringBuilder3 = new StringBuilder();
    stringBuilder3.append(stringBuilder2);
    stringBuilder3.append(a(file.getAbsolutePath(), true));
    String stringBuilder4 = stringBuilder3.toString();
   ac.b(“CrRt”, “cmd: “.concat(String.valueOf(stringBuilder4)));
    a(stringBuilder4, 300000, true, null);
}
```

Since Hoverwatch updates using the “-r” option, version code and digital signature verification is performed on the downloaded APK to ensure that the version code is higher than that of the installed application and that the digital signature is the same as whichever application the downloaded APK replaces.

As with mSpy, this update code did not appear to be active. Before installing an update, the code checked for the existence of an update from the following URL:

```
hxxps://i.hoverwatch[.]com/api/online/programversion/HWA/
```

At the time of this writing (April 8, 2019), this resource included information on the date of the latest version ("2018-12-31"), the product name ("Hoverwatch for Android"), and the version ("6.3.260"). However, the download link of the latest version was blank (an empty string), which short-circuited the self-update process. The update check was secure when analyzed because it was protected with SSL. If, in the future, updates were enabled on the server and a download link were provided, then the ultimate security of the update check would hinge on whether the download link were HTTP or HTTPS, as the actual APK download is performed using the "java.net.URL" API. This API can either use SSL encryption or not depending on the URL passed. Thus, assuming that the download link provided by the update check was HTTPS, then the update process would be sufficiently authenticated. However, if it is not, then the update process would be vulnerable to attack in the case of a non-rooted phone and partially vulnerable in the case of a rooted phone.

2.3 Discussion

Our technical assessments revealed a number of findings that merit discussion and pertain to the topics of infrastructure mapping, malware engines' detection of stalkerware, and the secondary risks that stalkerware developers' software inflict on the targets of such software. We discuss each of these points in order.

In the course of identifying the infrastructure that was used to host stalkerware, the only network that we saw which was used for more than one stalkerware application was Cloudflare. Cloudflare is not a traditional cloud provider; it does not offer hosting directly to customers but, instead, is a content delivery network that sits as an intermediary between the actual web server and the end user. Due to Cloudflare's intermediary status, the actual web server that was being used to host those aspects of the respective companies' infrastructure was obscured. In other words, where Cloudflare infrastructure was used, we could not determine the geographic region wherein the respective companies' servers were actually located. While many companies self-identify the countries in which legal proceedings must be brought, it is possible that they may actually host their content in jurisdictions dissimilar from where such proceedings must be brought. In such cases, there is the potential that the companies would be subject to the legal jurisdictions of both countries where they host data as well as where they assert litigation must take

place, not to mention the jurisdiction where the harm is actually occuring, if the stalkerware operator and targeted person live in yet a third jurisdiction. However, the significant adoption of Cloudflare services blunts an assessment of exactly what, and how many, legal jurisdictions the companies included in their study may be subject to.

With regards to how well stalkerware was detected by anti-malware engines, we draw two conclusions. The first pertained to our synthetic evaluation of how well antivirus engines generally detected stalkerware and the second is linked to our specific assessment of Google Play Protect. As previously discussed, 23/82 (28.05%) of positive detections mentioned the name of the product itself in the detection. Within the list, detection names varied in how strongly the names identified something as malicious, from potentially (for example: "a variant of Android/Monitor.Mspy.J potentially unsafe" and "PUA.AndroidOS.Killermob") to more a more firm evaluation (example: "Riskware.Android.Mspy.fdihek" and "Android:KillerMob-P [Trj]").

The names given to the detections lend some visibility into how antivirus companies perceive these products: either as something outright malicious or something only potentially unwanted by a user. Specifically, PUA and PUP are terms meaning "Potentially Unwanted Application" and "Potentially Unwanted Program," respectively, and are commonly used by antivirus and security industry vendors. In contrast, TRJ likely refers to Trojan in this detection name. For FlexiSPY, we often see it detected as "killermob" though we are unsure why. This may be a reference to Killer Mobile, another manufacturer of similar software.[111] Emergent from the data we can see that antivirus companies do not uniformly label stalkerware as explicitly malicious, potentially suggesting that assessments done by antivirus companies do not register the stalkerware as rising to the same level of harm as more outwardly malicious code or, alternately, as recognizing the potential dual-use nature of the software based on its feature set.

Turning to Google Play Protect, based on our limited assessments it appeared that the detection engine could identify at least some malicious stalkerware applications within days of being updated by developers. Further, when reactivating Play Protect on non-rooted Android devices we found that Play Protect was able to reliably remove the stalkerware in all cases where Play Protect would have otherwise

111 Thomas Brewster (2017), "Meet The 'Cowboys Of Creepware' -- Selling Government-Grade Surveillance To Spy On Your Spouse," *Forbes.com* (February 16, 2017) <https://www.forbes.com/sites/thomasbrewster/2017/02/16/government-iphone-android-spyware-is-the-same-as-seedy-spouseware>.

identified the stalkerware upon installation. Significantly, when Play Protect was reactivated, the user was often explicitly asked if they wanted to uninstall the stalkerware as opposed to immediately quarantining or deleting it. This behaviour is positive, insofar as it ensures that the agency for the decision to delete the malware is placed in the user who will likely often be the person being targeted by the stalkerware. Removing surveillance tools is often associated with heightened risks of violence in cases of intimate partner violence, abuse, and harassment, and so Google's decision to not unilaterally remove the malware may reflect both the potential that the malware is actually desired (i.e., it may be a case of ostensibly legitimate child or employee monitoring) or, if not desired, that its removal could worsen a targeted person's life in potentially fatal ways.

However, comments left on FlexiSPY's website suggest that the malware may be automatically uninstalled or deleted by Play Protect, even when the Play Protect has been disabled. While we did not conduct sufficient research to confirm that this is a now-common practice, if it is, then the inability to install the malware would seem to be a potentially positive result insofar as it would reduce the ability of stalkerware operators to use this malware in their surveillance of other persons. However, there may also be risks associated with these behaviours: specifically, if the stalkerware is automatically removed, then the operator may escalate their mode(s) of violence or assume that the removal is linked to an activity carried out by the person targeted by the surveillance. In either of these cases, the automatic deletion of the stalkerware might seem to, on the one hand, yield technically positive results while, on the other, constitute a socially risky technical behaviour that could further endanger the person who is the target of the operator's malign interests.

Finally, in assessing the ways that stalkerware developers can potentially update their applications, we found that developers could further endanger a targeted person's security by relying on insecure software update methods. Specifically, when developers do not use encrypted update channels, there is the potential for malicious third-parties to arbitrarily engage in a man-in-the-middle attack. FlexiSPY was clearly susceptible to this kind of attack, as might be mSpy and Hoverwatch depending on if and how they actually implement self-updating. These insecure development practices amplify the risks facing individuals being targeted by the operators of spyware: not only are such individuals threatened by the operators, they are also prospectively at risk of being harmed by additional unknown malicious parties. Such parties might install malware onto the targeted person's device to exfiltrate personal information, use the device as part of a botnet or other

malicious distributed computing activity, or otherwise violate the targeted persons' autonomy.

2.4 Conclusion

Conducting technical analyses of several pieces of stalkerware enabled us to test the hypothesis posed through the academic and non-profit organizational literatures: that antivirus systems are largely unable to detect stalkerware. Furthermore, and in excess of most other researchers, we evaluated the extent to which Google Play Protect served as a legitimate means of keeping targets safe from having their data inappropriately collected by stalkerware applications. Finally, we found that stalkerware applications can increase the threats faced by targeted persons, in excess of the efforts of coercive control being exercised by the operator of the stalkerware: the software, itself, may expose the targeted person to an increased potential of being targeted by other kinds of malware should a third-party exploit an insecure software update channel. Each of these mainline conclusions will be taken up later, and in depth, in **Part 6**.

Part 3: Search Engine Optimization Analysis

Spyware companies compete in a global online marketplace and, like most commercial businesses, they are invested in promoting their products online to lure prospective consumers. One way of reaching these customers is through online search results. To raise the likelihood that companies will connect with consumers, companies engage in strategies to optimise their visibility on search engines. Scrutinising these practices is important because they indicate how companies selectively represent their products to prospective purchasers. But perhaps more important, the framing of these products also shape realities and expectations about the acceptable uses of spyware products as they relate to intimate relationships, parenting, and even employee monitoring. Building on research into the selective advertising of consumer spyware companies conducted by Harkin et al.,[112] this part of the report evaluates how spyware companies are engaged in promoting the visibility of their products through search engine optimisation (SEO) practices.

In this section of the report, we analyzed the SEO practices of the stalkerware companies selected for our study. Our analysis leveraged subscription-based services for businesses to gather search engine intelligence. We also analyzed HTML text on spyware companies' own websites; such text is often carefully curated to enhance the profile of a company's own products on search engines to prospective consumer audiences. Emergent from our analysis, we found that:

- Consumer spyware companies' blog and SEO content revealed that most companies had extensive references to spousal monitoring;
- Only one company, mSpy, encoded concealed HTML text which advertised spousal spying on their website;
- Few companies significantly purchased Google Ads as part of their SEO strategies, with the exception of mSpy;
- The substance of paid Google Ads tended to favour the use of the tools for general spying, hacking, or tracking, and did not include ads that might help persons targeted by stalkerware to detect or remove the respective companies' software; and
- Individual organic searches that related to the spyware companies in our

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

sample overwhelmingly favoured terms that identified the general use of the tools for spying, hacking, or tracking, and explicitly noted the circumvention of security features of products associated with the broader digital ecosystem.

This part begins by describing the methods we adopted to conduct SEO and marketing analyses, followed by a presentation of the data collected and then a discussion of the major findings that emerged from our analyses. We conclude with a brief review of our main findings and a discussion about the value and limitations of using marketing intelligence platforms for research inquiry.

3.1 Methodology

We adopted a pair of methodologies for this section of the report. First, we used a marketing intelligence platform to understand if, and how, the stalkerware companies in our sample purchased Google Ads to attract people to their websites as well as the kinds of search queries that individuals used to arrive at the websites of each spyware company, whether the individuals were potential stalkerware operators seeking to surveil a partner, or whether they were someone concerned about being a victim of spyware abuse. Second, we analyzed the HTML code on the companies' websites to determine if they had text which might be seen by search algorithms but hidden from an individual when they browsed the site, as well as whether the companies' blogs or other public materials referenced spousal or other targeted surveillance, tracking, or monitoring. These methods complement the empirical analysis of website material undertaken by Harkin et al. in their assessment of the content of stalkerware companies' websites.[113]

The sample of studied companies included FlexiSPY, mSpy, Highster Mobile, Hoverwatch, Mobistealth, Cerberus, Teensafe, and TheTruthSpy. We included Trackview, in addition to the other applications studied throughout this report, to determine if applications which sold their products primarily as a geo-location tracking tool would adopt market strategies that differed from the other companies in our sample.

3.1.1 Marketing Intelligence Methods

Private companies' use of business intelligence analytics are commonplace in today's information-based economy. Businesses value these analytics because they provide insights about industry sectors and consumers' traits and habits, as well as competitors' products, services, and behaviours. Organizations often

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

rely on this information to make timely and informed decisions about how they promote their services.[114] In response to market demand for business analytics, a number of emerging commercial enterprises have emerged that specialise in recognising patterns in consumer traits (e.g., via social media or browser activities) and the networked relationships between domains, with some insights specifically provided through Search Engine Optimisation' (SEO) tools. By using SEO tools, such as AhRefs, to understand stalkerware companies' self-presentation to customers, as well as how companies understand how prospective customers discover these companies' websites, we can better understand how companies might curate their digital practices—and what kinds of norms and audiences they find it valuable to communicate with—to yield higher rankings in search results and a relative growth in website traffic, and an associated upswing in revenue.

Information Box 3: Google Ads 101

Google Ads (formerly Google Adwords) is an online advertising platform. Businesses and individuals use the platform to purchase advertisements which are based on specific keywords, such as "how to spy on someone's phone without touching their phone." When these keywords are searched for using Google's search engine, the advertisers' products and services will appear at the top of the returned search results.

We purchased a subscription to AhRefs,[115] one of the most well recognised marketing intelligence platforms. We then collected information from a number of metrics that the company provided, including, but not limited to:

- **Paid Adwords:** These are keywords that organisations purchase to boost the visibility of their products on search engine platforms such as Google to gain the attention of consumers via search engine results. Our intend behind gathering data on the types of paid Google Ads was to learn whether, and/or to what extent, stalkerware companies selectively interpret and present their products and services to a consumer audience. For example, did a company that primarily marketed itself as a parental control app purchase Google Ads related to intimate partner spying?
- **Organic Keywords:** These are keywords that individuals enter into search engines to receive lists of search results, from which individuals may arrive at a company's website. We gathered data on search engine keywords to obtain a window into how individuals (which potentially includes prospective

114 Chen, Hsinchun, Roger HL Chiang, and Veda C. Storey (2012), "Business intelligence and analytics: From big data to big impact." *MIS quarterly* 36(4) at 1166

115 *Ahrefs.com* (Accessed May 14, 2019) <https://ahrefs.com/>.

stalkerware operators) who might click through the search results to visit a consumer spyware company website could self-interpret and understand their activities.

- **Organic Keyword Search Volume:** This metric indicates how many times per month, on average, people searched for a given keyword and were served a particular URL. This figure gives us an indication of the relative popularity of certain keywords over others.

Using AhRefs, we downloaded all of the organic keywords and keyword search volume specific to each spyware company's domain across three jurisdictions: Canada, the United States, and Australia. These jurisdictions were chosen as part of a representative sample between two ongoing studies into stalkerware including Citizen Lab (Canada) and Deakin University (Australia). The United States, as a large jurisdiction with a prospectively significant number of potential customers of these products, was added to complement both the Canadian and Australian jurisdictions as a similarly representative sample. The United States is also important as a jurisdiction given that the United States' Federal Communications Commission (FCC) has previously taken an interest in spyware products and services, and the U.S. has also been a jurisdiction where a resident plead guilty to advertising and selling spyware online.[116]

AhRefs operates by linking an organic search term to a specific URL on a 'search engine results page' (SERP), its ranking position relative to other results using the same organic search term, and the estimated monthly search volume of that particular search term/URL combination.

When looking up AhRefs results for the root domain <http://www.mspy.com>, the data might look something like the information presented in Table 10:

Keyword	Position	Volume	URL
how to put parental controls on tablet	5	350	https://blog.mspy.com/how-to-put-parental-controls-on-a-tablet/
how to put parental controls on tablet	7	150	https://blog.mspy.com/set-parental-controls-samsung-tablet/
how to protect kids online	12	50	https://blog.mspy.com/set-parental-controls-samsung-tablet/

Table 10: Ahrefs Examples

116 Charlie Osborne (2014), "StealthGenie spyware seller fined $500,000 in landmark conviction" *Zero Day* (December 1, 2014) <https://www.zdnet.com/article/stealthgenie-spyware-seller-fined-500000-in-landmark-conviction/>.

In this example, we see three AhRefs results: two results for the organic search term “how to put parental controls on tablet” and one for “how to protect kids online.”The first shows that a monthly average of 350 users searched using the term “how to put parental controls on tablet,” were served a search engine result that led to the URL <https://blog.mspy.com/how-to-put-parental-controls-on-a-tablet/>, and that this result appeared in the fifth position on a SERP. In the second example, 150 monthly users searched for that same keyword combination but were served a search engine result for <https://blog.mspy.com/set-parental-controls-samsung-tablet/>, and this appeared as the seventh search result. In the third example, 50 monthly users searched for the term ‘how to protect kids online,’ were served a search result for <https://blog.mspy.com/set-parental-controls-samsung-tablet/>, and this URL appeared as the twelfth search result. In aggregate, these examples showcase how the same keyword search can lead to different URLs and that different keyword searches can lead to the same URL.

Based on the limitations of our subscription licence, we restricted our analysis to a maximum of 1,000 of these organic keyword searches-URL pairs and only those that would be listed in the top 20 positions of a SERP. After obtaining our data set, we structured and analysed it pursuant to a grounded-theory approach.[117] A number of dominant themes emerged from the data set, which we disaggregated as specific categories. The following list includes the categories, their terminological definitions, and explanatory value with respect to the purpose of this study:

- **General:** Searches that contain generic queries for spying/hacking/tracking and that did not explicitly mention a brand by name (e.g., a product such as iPhone, an application such as SnapChat, or a service provider such as T-Mobile) or a specific target of spying/hacking/tracking such as “spouse,” “wife,” “teenager”.
- **Intermediary:** Searches that explicitly mentioned a brand name (e.g., product, app, or service provider) but which excluded the name of a given spyware vendor.
- **Parental:** Searches that explicitly mentioned a parent-child dynamic in relation to spying/hacking/tracking.
- **Spousal:** Searches that explicitly mentioned a spousal or romantic relationship in relation to spying/hacking/tracking.

117 Grounded theory is a systematic methodological approach in the social sciences that draws together both inductive data collection and analysis and deductive theory-building. See Kathy Charmaz (2006), *Constructing grounded theory: A practical guide through qualitative analysis,* (2006: Sage).

- **Employee:** Searches that explicitly mentioned an employment dynamic in relation to spying/hacking/tracking.

We then coded each organic keyword search and allocated them per our aforementioned categories. The allocations were based on the presence or absence of a set of keywords:

- A search was classified as **general** if it did not explicitly reference another relationship (e.g., "spouse," "wife," "teenager," "employee"), or an intermediary (such as "Android," "iPhone," or "WhatsApp") (e.g., "how to spy on someone through their phone camera").
- A search was classified as **intermediary** if it included a brand name (e.g., product, app, or service provider), including popular abbreviations (e.g., "snap" for Snapchat, "messenger" for Facebook Messenger, "fb" for Facebook) (e.g., "spy app for android undetectable").
- A search was classified as **parental** if it included any of the following keywords: "parent(al)," "teen," "child," "son," "daughter," "kid," or "family" (e.g., "how to track my daughters phone without her knowing").
- A search was classified as **spousal** if it included any of the following keywords: "partner," "spouse," "husband," "wife," "girlfriend," "boyfriend," or "cheating" (e.g., "spy apps for cheating spouses").
- A search was classified as **employee** if it included any of the following keywords: "employee," "employer," "worker," "boss," "supervisor," or "corporate" (e.g., "corporate mobile phone tracking").
- A search was classified as cross-indexed (i.e., **intermediary/spousal**) if it included relevant keywords from more than one of the above categories (e.g., "how to hack my girlfriends snapchat").

An initial review of the data was conducted in June 2018 and revisited and revised in March 2019.

3.1.2 Examination of HTML on Companies' Websites

We conducted manual searches of the HTML code found on the websites of the spyware companies in our sample and looked for whether there was code which was readable by web search robots but concealed from humans who visited the websites and read their contents. Companies sometimes engage in these activities to influence their relative ranking in a search query list; a company with concealed HTML for, say, spousal monitoring may rank higher than a website that lacks such

concealed HTML. We principally examined companies' websites on September 1, 2018-November 25, 2018, and re-examined websites in May 2019.

In addition to looking for concealed HTML, we also examined the HTML which was publicly presented to persons who visited the websites. Specifically, we looked to see whether there was text on blogs or other associated elements of the companies' websites or social media accounts which promoted their products for spousal surveillance, tracking, or monitoring, as well as for potentially employee or child monitoring. We principally examined companies' websites on September 1, 2018-November 25, 2018, and re-examined websites in May 2019.

In both cases, we ran Google queries on specific websites, and searched for specific content on those websites such as "spouse" or "girlfriend." A query might appear as "+site:mspy.com spouse girlfriend." If we found matching visible text then we examined the text to determine if the webpage explicitly encouraged spying on spouses, girlfriends, or partners. If we did not, however, see those terms on the page as presented to a regular viewer, we examined the webpage's source to see whether, and where, the queried text was located. The text might, as an example, be configured to principally be visible to search engine bots and not to website visitors. When we encountered such situations, we concluded the the company was surreptitiously encouraging intimate partner surveillance.

3.2 Data

In this section, we present the findings of each of the nine companies whose paid Adwords and organic keywords we analyzed from Ahrefs results. We present an overview of the total keywords analyzed, a keyword breakdown by category, and key examples and takeaways. Where noteworthy, we also break data down as specific to either Australia, Canada, or the United States of America. We also subsequently present our findings of the HTML analysis.

3.2.1 Paid Google Ads

Of the nine companies that we analysed, only mSpy purchased paid Google Ads in Canada (n=14), Australia (n=13), and the United States (n=372). Hoverwatch was found to purchase just one adword in Australia, which was for its own name ("Hoverwatch"). When mSpy paid adwords (n=399) and Hoverwatch paid adwords (n=1) data were aggregated across all jurisdictions (see Table 11), we found that the most prevalent categories included 'General,' followed by 'Intermediary,' 'Parental,' 'Parental/Intermediary,' and Spousal/Intermediary.' In Table 11 and Table 12 we present our results of mSpy paid adwords.

Keyword Category	Number of keywords (volume)	Examples
General	223 (68,770)	"how to spy on someone phone without touching their phone"
Intermediary	139 (7510)	"how to hack an instagram account on iphone"
Parental	19 (1630)	"what app can i use to monitor my childs phone"
Parental/ Intermediary	16 (810)	"tracking your childs iphone"
Spousal/ Intermediary	1 (10)	"cheating spouse snapchat"

Table 11: Aggregated mSpy Paid Google Adword Information

In Canada, paid Ads included 14 unique terms, totalling a combined monthly search volume of 4,380 across all of the keyword searches. As Table 12 shows, the most prevalent mSpy adwords were 'General,' followed by 'Parental' and 'Intermediary.' There were no keywords related to 'spousal' in our assessment of keywords.

Keyword Category	Number of keywords (volume)	Examples
General	12 (4,290)	"spy tracking devices"
Parental	1 (70)	"parental control software free"
Intermediary	1 (20)	"how to hack an instagram account on iphone"
Spousal	0	

Table 12: mSpy Google Ads in Canada

3.2.2 Organic Keywords

Our analysis of organic keywords (n=13,878) provided by AhRefs for all nine stalkerware vendors in the three geographic regions we surveyed revealed that the overwhelming majority of keyword search data that served users with stalkerware results fell into the general category (n=7,706), followed by the intermediary category (n=5,063). In instances where specific relationships were mentioned in search terms (either parental, spousal, or employee as specific classes of persons related to the surveillance), the data revealed that the most prevalent keyword search terms used to arrive at consumer spyware domains included parental (n=628), followed by spousal (n=128), and employee (n=5). Cross-coded categories include Parental/ Intermediary (n=332), Spousal/Intermediary (n=15), and Employee/Intermediary (n=1). Table 13 presents this data on a per company/application basis.

	Cerberus		FlexiSPY		Highster Mobile	
	Keywords	**Volume**	**Keywords**	**Volume**	**Keywords**	**Volume**
Parental	0	0	0	0	0	0
Intermediary	62	8090	1310	258210	190	16630
Parental / Intermediary	0	0	0	0	2	110
General	470	873810	672	282650	831	165840
Spousal	0	0	0	0	0	0
Intermediary / Employee	0	0	0	0	0	0
Intermediary / Spousal	0	0	0	0	0	0
Employee	0	0	0	0	0	0

Table 13a: Organic Keyword Searches by Company / Application

	Mobistealth		mSpy		Hoverwatch	
	Keywords	**Volume**	**Keywords**	**Volume**	**Keywords**	**Volume**
Parental	15	2440	20	2380	1	600
Intermediary	490	55230	612	135220	577	109740
Parental / Intermediary	0	0	56	4490	0	0
General	668	211100	1127	709370	1624	452920
Spousal	0	0	0	0	1	200
Intermediary / Employee	1	20	0	0	0	0
Intermediary / Spousal	0	0	0	0	0	0
Employee	3	460	2	150	0	0

Table 13b: Organic Keyword Searches by Company / Application

	TheTruthSpy		TrackView		TeenSafe	
	Keywords	**Volume**	**Keywords**	**Volume**	**Keywords**	**Volume**
Parental	7	1400	0	0	585	178240
Intermediary	1308	329640	54	2030	460	275780
Parental / Intermediary	0	0	0	0	274	64720
General	1531	459490	418	140060	365	231740
Spousal	127	23330	0	0	0	0
Intermediary / Employee	0	0	0	0	0	0
Intermediary / Spousal	15	336	0	0	0	0
Employee	0	0	0	0	0	0

Table 13c: Organic Keyword Searches by Company / Application

3.2.3 - Hidden HTML

We only found that one company, mSpy, used concealed text on their website. When we visited <https://www.mspy.com/sent-received-sms.html> and viewed the source code for the page, we found: “Have you ever considered using the SMS tracker to know who your spouse or children are texting with?” This text was preceded by an HTML tag, ; as a result, the content was not visible in a web browser unless switched to read the page’s source code. Similarly, when we visited <https://www.mspy.com/whatsapp.html> the user-visible page emphasizes child monitoring only: “View all WhatsApp sent and received texts with mSpy. Ensure that your kid is not talking to cyberbullies, online predators or any strangers online.” The word “spouse” did not appear. However, upon viewing the HTML source of the page, a div labeled “drop-seo-text” contained a very long block of hidden text, including the words:

> “Although this tracker was created for parents who want to control their rebel teenagers, it may also be used by spouses who want to spy on their significant others, or by companies who want to control their employees’ text messaging. The best advantage of this program is that it can spy on someone inconspicuously, and it does not need any special conditions to do it. It is not even necessary for you to learn the telephone number of a person to spy on him/her because the app installed on a cell phone will do everything for you.”

Similar concealed text was found on the page <https://www.mspy.com/mobile-phone-spy-software.html>. While the page described the company’s program features, it did not mention the word “spouse” in user-visible text. However, in the “drop-seo-text” div there was the following text:

> “Do you cherish a dream of secretly spying on your spouse’s mobile phone to know whether he/she is cheating? Are you worried about your children’s safety and contacts? Embarrassed to ask about their sexual activity or other risky behaviors? Now you can solve these delicate issues without mind-cracking and without discreditable interrogations! Look for the mSpy spy phone app – a perfect solution to spy to mobile phones of your family and keep track of safety and fidelity issues without sleepless nights and nervous breakdowns!”

3.2.4 - Visible HTML Text

In examining companies’ websites for content suggestive of spousal or partner surveillance, all companies but Cerberus and TeenSafe contained suggestive materials either on their companies’ websites, company blogs, or company social media accounts. In what follows we highlight examples with each of the companies.

FlexiSPY’s blog contained some content which promoted spying on one’s partner. One post included the text, “[w]e have reason to believe that Margaret (our target phone) has been hanging out with Bill again -with whom she supposedly broke off

an affair two months ago. We've been tracking call logs, text, and IM conversations, so we know they've been in contact again"[118] and "[a]s trends are showing, practically everyone will soon be using WeChat, or at least will have tried it. So, if it's not being monitored, whether for kids, teens, employees, your husband, or wife, then you're missing out."[119] Other pages described the company's product as being "[c]ompletely undetectable, it's targeted at catching cheating spouses, protecting children & enforcing corporate policies"[120] and as having been "used successfully worldwide to bring to light to extramarital affairs, disloyal employee activities, and to protect children from predators and SMS bullying, and the additional devices now bring these benefits to many more people."[121] The company had also posted social media posts on its Facebook profile that was focused on extramarital affairs, such as posting a link entitled "Cheating wives are on the rise,"[122] and "These are the telltale signs that show your partner is having a social media affair #FlexiSPY."[123]

In the case of Highster Mobile, the company outlined a series of applications that might be suspicious—in this case, to a female partner observing their male partner's behaviours on their phone—and suggested that:

> Since many of these cheating apps require passwords or pins to access them, or do not appear in the applications list, you will need a monitoring software to fully access the information you need. Monitor and track his device with cell phone spy software. Highster Mobile takes a few minutes to install and will give you access to his SMS text messages, iMessages, Facebook account, browser history, GPS location, photos, videos, social media accounts and more.
>
> You may never find some of these cheating apps if they're hidden properly. If you suspect he is cheating, trust your gut and get the evidence with cell phone spy software, so you can confront him on his infidelity. Once you know for sure he is cheating on you, you will be able to make a decision about how to move forward,

118 FlexiSPY (2013), "Spoof SMS – The Secret Weapon You Should Have Been Using," FlexiSPY (November 13, 2013) <https://blog.flexispy.com/spoof-sms-powerful-secret-weapon-shouldve-using/>.

119 FlexiSPY (2013), "How To Spy On Android WeChat Chats," *FlexiSPY* (November 27, 2013) <https://blog.flexispy.com/spy-wechat-flexispy-android/>.

120 FlexiSPY (2013), "Nokia's n900 Flagship & Maemo Platform Get First Spy Application," *FlexiSPY* (Accessed May 14, 2019) <https://www.flexispy.com/en/news/nokia-maemo-gets-first-spy-app.htm>.

121 FlexiSPY (2007), "FlexiSPY Spills Blackberry Secrets," *FlexiSPY* (Accessed May 14, 2019) <https://www.flexispy.com/en/news/news-flexispy-blackberry-windows-mobile.htm>.

122 FlexiSPY (2013), "Cheating wives are on the rise" *Facebook* (October 6, 2013) <https://www.facebook.com/flexispy/posts/1395908897308558>.

123 FlexiSPY (2013), "These are the telltale signs that show your partner is having a social media affair," *Facebook* (October 12, 2013) <https://www.facebook.com/flexispy/posts/1126186070751848>.

> with or without him. It will give you peace of mind to find out one way or the other instead of living in a world thinking you are crazy all the time.[124]

Furthermore, a series of websites that are styled similarly to Highster Mobile's main site—such as highstermobile.co—routinely indicated that spousal or partner surveillance was a legitimate use of the company's software and services. The company's stalkerware was described as, "[t]he perfect tool to catch a cheating spouse, Highster Mobile remains undetectable on the target phone. The user will never know the app is installed and collecting data"[125] and that "[p]eople spy on cell phone without accessing the phone for different reasons. Parents do it to monitor their children's cell phone activities, employers do it to ensure productivity in the workplace, and spouses do it to catch a cheating partner."[126] These are just two of over a dozen examples which praised the utility of the spyware for spying on a spouse or partner or girlfriend.

Hoverwatch was similarly explicit in the potential for its software and services to be used to monitor partners. The company has written, "[y]ou can monitor your employees, spouse, and other people as well. How to use the tool is up to you. Do not forget that it is a great way to learn more about the target person"[127] and, on other pages, clarified that "[j]ust imagine that you want to spy on your spouse, and your husband or wife has two SIM cards. Each time she or he replaces it, if you track just one phone number, you will never learn about the second."[128] The company was resoundingly clear in who it believed would benefit from installing and using the company's products, writing "[a] lot of people can benefit from using cell phone spy software. Whether you're a worried parent, a watchful employer, or even a spouse who thinks that they are being cheated on, you will greatly benefit from getting this app."[129]

---

124 Highster Mobile (2019), "Cheating Apps To Look For On His Phone," *Highster Mobile* (April 25, 2019) <https://highstermobile.com/blog/cheating-apps-to-look-for-on-his-phone/>.

125 Highster Mobile (2017), "Highster Mobile Review – Does it work?" *Highster Mobile* (December 13, 2017) <https://www.highstermobile.co/highster-mobile-review/>.

126 Highster Mobile (2016), "Tag Archives: spy on cell phone without accessing the phone" *Highster Mobile* (August 26, 2016) <http://highstermobile.co/blog/tag/spy-on-cell-phone-without-accessing-the-phone/>.

127 Hoverwatch (2018), "Why you should use cell phone spy software," *Hoverwatch* (October 29, 2018) <https://web.archive.org/web/20190131134854/https://www.hoverwatch.com/blog/why-you-should-use-cell-phone-spy-software>.

128 Hoverwatch (2019), "Whatsapp messages," *Hoverwatch* (Accessed April 30, 2019) <https://www.hoverwatch.com/blog/how-to-spy-on-whatsapp-messages-from-another-phone>.

129 Hoverwatch (2019), "Protect your kids and monitor your employees using cell phone spy software," *Hoverwatch* (Accessed April 30, 2019) <https://www.hoverwatch.com/cell-phone-spy-software>.

Mobistealth, in describing the benefits of using the company's software to monitor a targeted person's Snapchats, stated that "...a spouse would also want to keep tabs on their counterpart's Snapchat activity in order to find out if they are not being cheated. Therefore, Snapchat monitoring can really be helpful if used the right way and for the right purpose."[130] A posting on the company's Facebook account read "[s]nooping on your spouse through SMS tracking might not end well for 3 obvious reasons that no one wants to admit! #FF"[131] and included a bit.ly link that resolved to <https://web.archive.org/web/20160405203920/http://www.mobistealth.com/blog/sms-tracking-snooping-spouse/>. That URL returns a page not found at time of writing.

mSpy rationalized the purchase of their product, in past, to monitor social media accounts such as Kik. Specifically, the company wrote that, "...not only parents want to spy into kik accounts of their kids. Many people have their specific reasons to spy on their beloved ones. This can be a wife, who doubt her husband's loyalty." And the company marketed its own product as superior to free alternatives, but nonetheless described both as kinds of monitoring tools. Indeed, mSpy went so far as to say, "[i]f you use a monitoring tool for safety purposes and instead of finding all kinds of cunning ways on how to spy on text messages or how to spy on your girlfriend or boyfriend husband or wife, you will start reaping the many rewards the program can give you over the short and long term."[132]

TheTruthSpy explicitly, and across the main parts of its webpage, sold its product and services as useful for catching cheating spouses, writing that "[i]t's time to start spying...TheTruthSpy application is one of the best Catch Cheating Spouse App available today. It provides you lots of features which make your work easy."[133] The company had a section of its website which was dedicated to explicitly selling its products and services to catch cheating spouses, and asserted that "[t]aking the help of spy apps, you can collect evidence against your spouse. Although this seems a difficult task using spying application will make it easier than you could

130 Mobistealth (2019), "Hack Snapchat the Right Way Using This Monitoring Tool," *Mobistealth*, (Accessed April 30, 2019) <https://www.mobistealth.com/snapchat/hack-snapchat-right-way>.

131 Mobistealth. (2015). "Snooping on your spouse through SMS tracking might not end up well for 3 obvious reasons that no one wants to admit! #FF," *Facebook* (June 19, 2015) <https://www.facebook.com/themobistealth/posts/936194629781343>.

132 mSpy. (2018). "Is it enough to use a free revealer keylogger to know everything about kids' online life?" *mSpy* (February 19, 2018) <https://blog.mspy.com/enough-use-free-revealer-key-logger-know-everything-kids-online-life/>.

133 TheTruthSpy. (2019). "Homepage," *TheTruthSpy* (Accessed April 30, 2019) <http://thetruthspy.com>.

ever imagine. The best way to catch a cheating spouse is by spying on his/her smartphone."[134]

3.3 Discussion

Our examination of spyware companies' use of Google Ads revealed that only mSpy engaged in a concerted effort to promote its products through the use of adwords for generalised surveillance, including to promote their product explicitly for spousal monitoring. Similarly, when individuals searched for spyware products, they tended to favour search terms that referenced generalised ways of using stalkerware that would undermine the security of devices, social media platforms, and software such as messaging apps. And lastly, we found that companies deliberately marketed their products through advertising and blog content as stalkerware, and in one case concealed content referencing spousal tracking from visitors to their website while simultaneously ensuring that these terms could still influence search engine rankings.

3.3.1 Limited Adoption of Google Ads

mSpy was the only company that we found as having purchased Google Ads across all of the jurisdictions under study (i.e., Canada, Australia, and United States). As such, it seems that consumer spyware companies largely did not use Google Ads for advancing their SEO strategies.

mSpy's selection of adwords were as revealing for what they contained as for what they omitted. Specifically, the majority of the Google Ads that the company purchased to promote its products targeted consumer searches that included generic queries for how to "spy," "hack," or "track" devices. Such searches included: "cell phone spy without installing on target phone," "free cell phone hacking software," and "free hidden phone tracker."

A second order of Google Ads were targeted towards persons who ran search queries that pertained to generic hacking, spying, or tracking capabilities that were associated with specific products, apps, or service providers. For example, mSpy paid to attract search engine users who submitted queries such as: "secret spy apps for iphone," "text tracker android," and "facebook spy software."

134 TheTruthSpy. (2017). "All-in-One Catch Cheating Spouse by TheTruthSpy," *TheTruthSpy* (October 20, 2017) <http://thetruthspy.com/catch-cheating-spouses-with-thetruthspy/>.

Advertisements which presented mSpy's products as generic tools to conduct surveillance vastly outweighed any queries associated with specific use-cases, such as parental monitoring. Thus, it appears that mSpy invested more of their advertising budget in paying to attract customers who searched with terms such as "phone spy software" or "call and sms tracker," and less to attract customers looking for "parental monitoring app" or "how to monitor child's snapchat on iphone."

Perhaps most notable in the findings, mSpy had at least one paid adword that explicitly targeted search engine queries associated with spousal monitoring. That Adword was for the term "cheating spouse snapchat." Additionally, mSpy purchased keywords related to concealing the presence of the app (e.g., "undetectable cell phone tracker," "secret snapchat spy," "free hidden phone tracker"). The company's purchase of these keywords suggested to us that they believed that some prospective customers are seeking a surveillance application that can operate while remaining hidden, presumably rendering the surveillance undetectable to the persons targeted by the surveillance.

What was omitted from Google Ads was just as significant as what was included. No company purchased Google Ads to help attract website visitors to determine if they had been targeted by the companies' respective software or how to remove the applications. Similarly, no company purchased Google Ads to attract search users to information that might be used to mitigate harms associated with the given company's products. Such omissions affirm the findings of Harkin et al. (2019), who found that spyware companies' marketing materials were typically directed towards persons who are likely to use the applications as opposed to those who were the target of surveillance.[135] These omissions were particularly notable since our analysis of organic keywords in **Part 3.3.2** showcased instances of persons either trying to determine if spyware was on their device (e.g., "how to tell if highster is on your phone") as well as how to uninstall/remove the spyware (e.g., "how to remove highster mobile," "how to uninstall cerberus").

3.3.2 Organic Keywords Focused on Undermining Security

Our results show that a total of 92% of all organic keyword searches were related to the generic capabilities provided by the spyware tools (n=12,769). This included a combination of general and intermediary categories (e.g., Android, iPhone, or a social networking service such as "FB Messenger"). The remaining 8% included searches which were tied to specific use-case scenarios such as parenting, spousal,

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

or employee surveillance. Overwhelmingly, however, searches conducted to inquire about consumer spyware tools—and arrive at the domains of consumer spyware companies in our sample—were related to generic capacities to spy, hack, or track.

We recognize that understanding persons' organic queries demands accounting for how people generally use search engines. It is conceivable, perhaps even likely, that prospective spyware operators could have a specific use-case in mind prior to their search and, as such, were searching for a tool to help them achieve their aim of spying, hacking, or tracking a specific individual or group of individuals. Someone who intends to use a mobile app to covertly monitor an intimate partner may not necessarily specify this use case in their search query, perhaps because they believe that any generic surveillance app with the desired functionalities would suffice, or because they do not know that there are spyware companies that cater to specific use cases.

Regardless of the specific and individuated reasons behind each search, the data illustrated that a vast majority of traffic arriving at consumer spyware websites was related to interests in weakening or undermining of security provided by mobile devices or specific applications, engaging in surreptitious surveillance of a targeted person's communications or activities, or to obtain products designed to spy or engage in surveillance of other persons.

When we conducted a qualitative analysis of the keyword data, there were several trends which emerged in each category that broadly applied across stalkerware vendors:

- **General searches** were often associated with product services (e.g., "highster mobile customer service phone number"), product reviews (e.g., "best phone spy software"), and general spying tactics ("hacking into phones"). While many searches were ambiguous or lacked context, others provided insight into the type and manner of hacking that persons sought information about (e.g., "how to spy on someone through their phone camera").
- **Intermediary searches** were often associated with general spying practices for specific intermediaries (e.g., "how to spy on someone on facebook," "hidden spy apps for android"). In some cases, searches were directed towards learning about how to breach services that were specifically marketed as encrypted or secure (e.g., "hack whatsapp messages," "viber spying").
- **Parental searches** were often associated with general queries for parental monitoring products (e.g., "cell phone monitoring software for parents") and

some specified an intent to hide the products from being detected by persons being targeted by surveillance (e.g., "how to track my daughters phone without her knowing"). For TeenSafe, several searches were related to safety and guardianship issues (e.g., "cyber bullying statistics," "texting and driving facts"), indicating the extent to which powerful surveillance capabilities and social control can be connected to a moral duty of care.

- **Spousal searches** were often associated with an intent to monitor an intimate partner's actions (e.g., "how to spy on my wifes phone"). In some cases, tracking was directly tied to suspected adultery (e.g., "how to catch a cheating spouse using cell phone").
- **Employee searches** were the smallest sample represented in our data set but all related to queries regarding surveillance or control of employees in the workplace(e.g., "misuse of internet in the workplace").

Lastly, it became abundantly clear that persons used online search functions to seek information related to a belief that Highster, for example, may have been installed on their devices (e.g., "how to remove highster mobile," "how to tell if highster mobile is on your phone," "how to uninstall highster mobile"). We found similar examples with Cerberus, with individuals seeking answers on "how to uninstall cerberus," and TeenSafe, with individuals searching "how to block teensafe." In the event that the individuals conducting these searches reached the sites of consumer spyware companies, previous research has shown that companies tend not to provide information on how to detect, remove, or otherwise remediate the surveillance conducted by way of these companies' applications.[136]

3.3.3 Companies Deliberately Market Products as Stalkerware

We found that mSpy used hidden text on their website.[137] We conclude that this usage was a deliberate effort to improve the company's rank in search engines when individuals ran search queries associated with spousal surveillance, based on two observations. First, the hidden text itself references spousal surveillance:"Have you ever considered using the SMS tracker to know who your spouse or children are texting with?" Second, the HTML tag which preceded the text was " ". This tag, specifically, referenced search engine optimization as well

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

137 By "hidden text", we mean that text that is included in the backend coding of a website and visible to search engines and other forms of computer reading, but not visible to human users who would be reading the public-facing website.

as indicated that the text should not be presented as visible text when individuals browsed through to the spyware company's webpages.

We also examined the user-visible sections of companies' websites and social media accounts to understand how the companies, themselves, promote their software. While throughout this report we have been careful to recognize that there may be ostensibly legitimate uses of some spyware—such as in some instances of monitoring young children or employees who are alerted to the surveillance—our examination of how companies have marketed their products revealed that many are not selling applications that might abusively be repurposed for engaging in intimate partner surveillance and harassment. Instead, many of the companies presented such abusive purposes as legitimate insofar as the uses were amongst the marketed uses of the applications. That six of nine companies explicitly sold their applications for these purposes lays bare that companies are involved in the sale of stalkerware, which also has functionalities for other kinds of surveillance as well. In effect, the dual-use nature of many of these companies' products is that while they are designed for stalker they also have ancillary, ostensibly legitimate, uses for child and employee monitoring as well.

3.4 Conclusion

Marketing intelligence platforms can provide a productive source of data from which to draw insights about stalkerware and spyware vendors as well as general Internet users. In the case of vendors, marketing intelligence can shed light on how vendors selectively represent their products on search engine platforms. We found that adwords were relatively infrequently used as part of spyware companies' digital marketing strategies. Only mSpy had paid Google Ads in all jurisdictions included in our analysis. These adwords were overwhelmingly targeted towards queries that prospective customers might use to find products which could be used for spying, hacking, or tracking purposes. In many instances, mSpy explicitly purchased Google Ads that targeted major technology companies such as Facebook and Snapchat, and products such as Android and iPhone mobile phones. In at least one instance, mSpy purchased an adword that would reach individuals searching for how to "catch a cheating spouse."

The use of marketing intelligence platforms also provided insight into what individuals were searching for and which queries led them to the spyware companies' websites which we studied in this report. Overwhelmingly, these searches related to

general uses of consumer spyware as a tool to spy, hack, and engage in tracking. A number of the searches indicated interests in specific methods of spying (e.g., "how to spy on someone through their phone camera"), specific targets of spying (e.g., "how to catch a cheating spouse using cell phone"), and specific types of devices and third-party applications that prospective customers were looking to spy upon (e.g., "hack whatsapp messages").

Using marketing intelligence tools potentially has broader methodological implications in the critical social sciences. While the full value and limitations of the use of marketing intelligence platforms as a tool for critical inquiry is beyond the scope of this report, the repurposing of this tool can provide insight into the relative ranking of the prevalence (in terms of overall Internet traffic) of different kinds of consumer spyware, including stalkerware. It can also be used to collect information pertaining to private company practices, as well as how individuals and other public sector entities engage with companies. Together, these kinds of insights provide an important degree of clarity into the operations of private companies and especially of those which sell products designed to facilitate or enhance social or coercive control.

Finally, we found that the companies included in our study overwhelmingly and deliberately marketed their products, to at least some extent, for enabling or facilitating intimate partner surveillance. As such, the dual-use nature of many of these applications should be understood as enabling abusive surveillance, first, and being used for ostensibly legitimate child and employee surveillance, second.

Part 4: Company User-Facing Policy Assessments

Companies that produce spyware-based products often develop and publish privacy policies as well as terms of service agreements. These documents are ostensibly designed to inform consumers about their protections and rights pursuant to using the companies' products and services, as well as to disclaim liability on the part of the company. The policies often include critical information concerning what is, and is not, considered personal information by the company in question, how and the extent to which a person can request access to their personal data, outline the kinds of information that may be collected in the course of using the spyware and associated services, and the relative degrees of security used to protect collected information. Assessing companies' policies can provide insights into the stalkerware industry by clarifying what companies themselves hold out as their legal obligations. Such obligations may fail to account for broader obligations under Canadian law, as an example, or fail to adequately capture the range of actors who may be affected by the operations of stalkerware. However, such documents capture the public ways in which companies assert their operations and may be indications of the extents to which businesses comport with law; it is thus important to examine these policies for their omissions as well as their assertions.

In this section of the report, we analyse the relevant privacy policies and terms of service/use that are made publicly available by stalkerware companies. We ultimately conclude that companies:

- Failed to make it clear how the victims of stalkerware can have their data deleted when they have not meaningfully consented to the collection;
- Failed to fully account for the personally identifiable information that can be captured when operating the software, thus circumventing the purpose and rationale of privacy policies to educate those affected by software to understand how it operates and collects such information; and
- Failed to adopt policies to notify persons targeted by stalkerware in the case of data breaches, or even individuals contracting for the services.

In aggregate, we found that these policies focused almost exclusively on the rights and guarantees to the operators or purchasers of the stalkerware and, in the process, fundamentally failed to recognize how the software can be used for harmful or

deleterious purposes. This core finding underscores how policy assessments can be used to reveal—or confirm—companies' perceptions of who they are legally bound to protect or have duties towards, and those to whom they do not.

This section of the report begins by describing the methodology that we adopted to analyse company policies, followed by a presentation of the comparative data collected and the major findings that emerged in our analyses. Our conclusion highlights how the policies failed to adequately account for the rights of the targeted individuals of stalkerware-enabled surveillance, and the significance of this commonly held corporate position.

4.1 Methodology

To assess different companies' policies, we undertook three consecutive activities: downloading relevant policies, such as privacy policies, terms of service agreements, and End User Licence Agreements (EULAs); assessing the aforementioned policies using a pre-determined series of structured questions; and finally re-assessing the policies one year after the initial assessment to determine whether policies had been modified following the passage of the European Union's (EU) General Data Protection Regulation (GDPR).

4.1.1 Obtaining Relevant Policies

Relevant policies for the studied companies were downloaded from company websites. Further, where companies sold their products in application stores (e.g., Google Play Store or iOS App Store), the associated policies were downloaded for analysis. Initial policies were obtained in May 2018 and, approximately a year later, re-acquired for assessment in February 2019. We downloaded the policies for the following companies: Cerberus, FlexiSPY, Highster Mobile, Hoverwatch, Mobistealth, mSpy, TeenSafe, and TheTruthSpy.

4.1.2 Structured Question Set

In assessing privacy policies, terms of service, and End User License Agreements for the companies being studied, we downloaded the respective companies' documents and subsequently assessed them using a structured question set. This question set is based upon past policy assessments that the Citizen Lab has conducted of telecommunications companies, fitness tracker companies, and

online dating companies.[138] Assessment categories were divided into specific questions pertaining to:

- **How a company developed its privacy policy:** e.g., "Is there a link to a privacy policy on the company's homepage," "Is there a reference to compliance with: National privacy laws, international guidelines, self-regulatory instruments from associations?," or "Is there a statement concerning which nation/court proceedings must go through?"
- **How companies addressed questions from users of the software, or those who are targeted by the software:** e.g., "Is there a contact to a privacy officer listed?," "Is there a description/discussion of who you can complain to if you're unsatisfied with the information/processes given by the organization?," "Is there a procedure for deleting information; a "right to forget"?," or "Do you have to be an active user to make use of stated procedures?"
- **How a company captured personally identifiable information:** e.g., "Is there specification of the kinds of PII (i.e., information about the 'users') collected? If so, what types of categories are listed?," "Is any distinction made between sensitive and non-sensitive PII?," or "Is any distinction made between information on children/adults?"
- **How, or under what conditions, a company might disclose collected data:** e.g., "Is there a specification of the kinds of organizations that users' information may be disclosed to?" or "Does the organization make note that it may/may not share information with law enforcement and, if it does, under what conditions? Is there a link to more information about disclosure to law enforcement?"
- **How a company secured personally identifiable information:** e.g., "Are commitments made to security of PII?," "Are commitments made about encryption/de-identification of data?," or "Is there a note that users and/or government bodies will be alerted if a data breach occurs?"

138 Andrew Hilts, Christopher Parsons, and Jeffrey Knockel (2016), "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," *Open Effect* <https: //openeffect.ca/reports/Every_Step_You_Fake.pdf>; Christopher Parsons, Andrew Hilts, and Masashi Crete-Nishihata (2017), "Approaching Access: A comparative analysis of company responses to data access requests in Canada," *The Citizen Lab* <https://citizenlab.ca/wp-content/uploads/2018/ 02/approaching_access.pdf>; Christopher Parsons (2015), "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project* <http://www.telecomtransparency.org/release-the-governance-of-telecommunications-surveillance/>.

None of the companies enrolled in this study were approached to provide further clarity concerning their policies or terms of service. This methodology was adopted on the basis that we could not guarantee responses from all companies (thus potentially giving a more positive assessment of some policies over others, where only some companies were non-responsive to questions) and because we wanted to approach this as a semi-interested member of the public who would read the given policies, but might not raise questions about them to the relevant company. As such, our analyses are drawn from how we interpreted what we read: we did not seek additional corporate guidance nor did we consult with contract lawyers. The result is that our analyses are meant to provide insights of well-informed members of the public as opposed to constituting comprehensive legal analyses of each and every policy that we analyzed or assess the outer limits of what a text might possibly bear or withstand under litigation. In other words, these documents are ostensibly intended for any layperson member of the public as one of these company's potential customers, and our methodology thus takes them at face value as such.

4.1.3 Reassessment of Policies

In February 2019, all of the companies' policies were re-examined to determine if changes had been made. We suspected changes might occur because of the passage of the EU's GDPR, which imposed significant financial penalties on companies which were not GDPR-compliant. While our approach is to critically interrogate these companies' practices, many proactively assert that they provide entirely legitimate customer services and, as such, should be mindful of what is required for lawful compliance in the EU if they want to sell into that marketplace. To re-examine policies we, first, determined whether they had been updated since the earlier assessment and, second, noted where any updates had occurred and which impacted our assessment of the companies' respective policies.

4.2 Data

We assessed the privacy policies, terms of service, and End User License Agreements of the sample list of stalkerware companies selected for this study. This assessment entailed, first, detailed content-level analyses of the respective companies' policies and, second, comparisons of companies' policies against one another. The following sections present the most significant findings that emerged from these analyses.

4.2.1 General Policy Questions

We first investigated companies' websites to determine whether there were links to privacy policies or terms of service documents that pertained to the applications

that the companies sold to the public. All companies provided access to their privacy policies or terms of service on the homepage of their respective websites. FlexiSPY and Highster Mobile both indicated that their products were compliant with the Children's Online Privacy Protection Rule (COPPA).[139] Further, some of these policies underwent changes between our assessment periods, with FlexiSPY, Hoverwatch, and mSPY all having updated their documents to indicate they were GDPR-compliant.

Several companies specified which national or state laws pertained to contractual disputes which might arise between individuals and the respective company, with the majority referencing United States of America judicial systems. Highster Mobile indicated in 2018 that the laws of New York State govern any dispute "including those arising from ILFMobile Corp's use of personal information or otherwise relating to privacy," though, as of 2019, their policy more broadly referenced the United States courts.[140] Hoverwatch stated that the governing jurisdiction was the Commonwealth of Virginia,[141] TeenSafe asserted that disputes must be mediated in California,[142] and TheTruthSpy identified as a Texas-registered company that was subject to the laws of the United States of America.[143] Only mSpy referenced a European member state's legal system in their policy documents: that of the Czech Republic.[144]

While most of the companies' privacy policies referenced their terms of service, and vice versa, this wasn't the case for either Mobistealth or mSpy. When companies' policies do not reference one another, they establish a further challenge or hinderance to better understanding a company's practices, especially when readers are unfamiliar with the full range of public documents that tend to accompany any company's products and services. Moreover, while five companies—Cerberus, Hoverwatch, mSpy, TeenSafe, and TheTruthSpy—indicated when their privacy policies were last updated, they did not provide access to historical versions of the

139 COPPA is an American law which imposes requirements on operators of websites and services directed towards children under 13 years of age. The goal of the law is to ensure that parents can control what information is collected about children, and it has been significantly adopted by businesses offering service in the United States and internationally. Past research has showcased that businesses often adopt 'COPPA compliance' to generally suggest that their products are protective of children's privacy. See: Bennett, Colin; Parsons, Christopher; Molnar, Adam. (2014). "Forgetting and the right to be forgotten" in Serge Gutwirth et al. (Eds.), Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges (Springer).

140 Highster Mobile (2018), "Terms & Conditions," <https://www.highstermobile.co/terms/>.

141 Hoverwatch (2013), "Terms of Service," <https://www.hoverwatch.com/terms-of-service>.

142 KidBridge (formally TeenSafe) (2019), "Privacy Policy," <https://kidbridge.com/kidbridge-inc-privacy-policy/>.

143 TheTruthSpy (2019), "Privacy Policy," <http://thetruthspy.com/privacy-policy/>.

144 mSpy (2018), "Privacy Policy," <https://www.mspy.com/privacy-policy.html>.

policies to determine what had changed. It is worth noting that while TeenSafe did indicate when its terms of use policy last changed, as of April 2019 the company's last update occurred on February 4, 2015, or a full four years earlier.[145] Further, Hoverwatch's Terms of Use document was last updated in 2013.[146] FlexiSPY, Highster Mobile, and Mobistealth did not indicate when their policies were written or last updated, nor did they provide access to previous policies.

All companies reserved the right to change their privacy policies, with companies indicating varying update notification practices, including: recommending that visitors of the companies' websites or users of their products review privacy policies periodically to determine if changes had been made; stating website visitors or customers would receive an email indicating the update; or prompting users with the update information in the services homepages, dashboards, or portals which were provided as part of the companies' products. However, Highster Mobile did not indicate how it would notify customers of changes to the policy.[147] In the case of the services homepages that companies might use to notify customers of changes to privacy policies or terms of service, these homepages typically present information about the target of the stalkerware, such as collected text messages, phone calls, or other captured data. Persons targeted using stalkerware do not have access to such services pages nor are they likely to be emailed about changes.

Since historical privacy policies are unavailable, users of these companies' products must make copies of each version of the policies they are aware of and, subsequently, parse the new policy for any and all changes. Furthermore, persons targeted by stalkerware are highly unlikely to have known to collect different versions of policy documents to engage in such retroactive assessment, given the highly surreptitious nature of stalkerware.

4.2.2 Engaging with Company Through Questions or Complaints

After reading a company's policy documents, or if readers have questions about a given company's data handling or management practices, they need to have a method of contacting the appropriate company representatives. We examined whether companies provided specific contact information so that either the

145 KidBridge (formerly TeenSafe) (2015), "Terms of Use," <https://kidbridge.com/terms-of-use/>.

146 Hoverwatch (2013), "Terms of Service," < https://www.hoverwatch.com/terms-of-service>.

147 Highster Mobile (Undated), "Privacy Policy," <https://highstermobile.com/privacy/>.

purchasers of the stalkerware services or the persons who are targeted by them can communicate with the company. We found that only three companies—Cerberus, mSpy, and TeenSafe—had dedicated privacy or legal contact information, with four other companies only offering general support or contact information. Mobistealth was unique in not presenting any contact information.

Companies tended to only offer support to correct or delete information for the purchasers of the software. It may be the case that the targets of surveillance could contact the privacy officers or legal contacts, but this potentiality is cast into question given that companies which recognize data deletion or correction rights raise them in the context of the rights that a customer of the company can exercise. Companies such as Cerberus, FlexiSPY, Mobistealth, and TeenSafe all assert that the information being collected is done so with the consent of the operator of the stalkerware.[148] As such, these companies do not explicitly state how (or whether)

148 For specificity, TeenSafe wrote the following in its Privacy Policy: "Personal information means information that can be used to identify and contact an individual such as name, email address, screen name, mailing address and phone number (the "Personal Information"). We consider such Personal Information sensitive in nature. You, as a parent or legal guardian, need to submit Personal Information to access the Site and the KidBridge Service. By submitting information, you are consenting to our collection of such information...Additionally, though not necessarily Personal Information, the KidBridge Service collects and provides you access to certain cell phone and computer activities (including, but not limited to, email and text messages) of your children, including through the use of computers and/or other devices on which the KidBridge software is installed and/or the Service is used (the "Accessed Activities"). For clarity, we do not knowingly collect Personal Information from children or sell any products to children."

FlexiSPY asserted that the phone data collected belonged to the customer who purchased the FlexiSPY application. The company wrote: "FlexiSPY holds the following information about our customers...Email address that you registered at time of sale and the device data transmitted from the device you installed FlexiSPY on."

Mobistealth wrote: "In order to provide you with the ability to monitor and control your child's device (mobile phone & computer) usage MobiStealth Parental control application may read and transfer to our servers various information about the device or information stored on the device, including but not limited to: the phone number, the IMEI, the IMSI, the ICCID, the ESN and the model of the device. When registering MobiStealth Parental Control application on child's device we will collect and transfer to our servers using internet: the parent's email address & password, child's contacts, sms history, Gmail history, call history, web browsing history and applications that are installed on the child's device. When MobiStealth Parental Control application is in use/active on the device, we may read, collect and transfer to our servers using internet, the location of your child's device, child's contacts, text messages, Gmail history, Call details, web browsing details, installed applications and the usage of the applications on your child's device."

Cerberus wrote: "In order to subscribe to the LSDroid Services, you must consent to: (a) the use of your devices' location to provide the LSDroid Services to you, including the display and disclosure of your location information (b) receive SMS messages; and (c) pay operator data, messaging, and other fees resulting from LSDroid Services usage."

In all cases, companies indicate that the user who controls the data is the party whom purchased the surveillance software; in no case does it suggest that the collected information belongs to the individual targeted by the stalkerware operator.

the targets of surveillance can obtain access to, request deletion of, or otherwise learn about the collection of their personal data.

In contrast, terms associated with Hoverwatch's products—which included rights to fix data, erase personal data, restrict processing, have data portability, and complain to a supervisory authority—are seemingly meant to attach to both the purchaser of the service as well as the targets insofar as they are expected to have consented to the surveillance. The kinds of data collected on the targets of surveillance include:

> record calls; track calls and call history; track phone locations; track SMS and chats; track Facebook, WhatsApp, Viber, Snapchat and other messengers and social networks; take screenshots and photos; save all contacts, track the calendar and to-do list; and track the browser and Internet history[.][149]

It is left unstated how, exactly, an operator is expected to obtain the consent of all persons who are targeted by this product, but Hoverwatch (like many others in this field) attempted to impose liability on the acquirer of the software by asserting that "[b]y installing the software or using the service you certify that you act in accordance to the law and you take full responsibility for the use of the product."[150]

The nature of how rights are assigned by companies carry over to whether individuals targeted by abusers' surveillance can compel stalkerware companies to delete all data and records associated with the targeted person. While account holders often retain these rights—as is the case for Cerberus, FlexiSPY, and TeenSafe—it is also, sometimes, implicitly suggested that these rights are also held by the targets of surveillance in the case of companies which assert GDPR compliance. Companies asserting such compliance include FlexiSPY,[151] Hoverwatch,[152] and mSpy.[153] These implicit indications arise purely because, in asserting GDPR compliance, companies are expected to afford rights to all persons to whom they have collected data about; companies are not, however, explicit in stating that they will guarantee the rights of persons targeted by stalkerware as well as the explicit customers of the surveillance software. However, it remains uncertain from reading the policy documents how a non-customer would issue a specific complaint to have their personal information deleted, a process that would likely be regarded as legally complicated by the companies in question on the basis that the operator of the stalkerware was

149 Hoverwatch (2018), "Privacy Policy," <https://www.hoverwatch.com/privacy-policy>.

150 Hoverwatch (2019), "Homepage," <https://www.hoverwatch.com>.

151 FlexiSPY (Undated), "Privacy Policy," <https://www.flexispy.com/en/privacy-policy.htm>.

152 Hoverwatch (2018), "Privacy Policy," <https://www.hoverwatch.com/privacy-policy>.

153 mSpy (2018), "Privacy Policy," <https://www.mspy.com/privacy-policy.html>.

ostensibly required to obtain consent prior to installing it on the target's mobile device, and potentially technically out of reach where the operator has downloaded or made copies of the targeted individual's data and stored it elsewhere.

4.2.3 Capture of Personal Information

Companies which sell stalkerware are in the business of creating, and marketing, products which are designed to collect vast quantities of intimately personal information. Many of these companies distinguish between the information they collect about the customers of stalkerware products versus the targeted persons against whom the products are deployed. Specifically, while customers are informed about the billing and other personal information that is collected in the act of providing commercial services, the personal information pertaining to the targets of the surveillance are rarely identified as such; in any case, targeted persons' data is identified as belonging to the company's customer or as being the responsibility of the customer. Only a handful of companies' policies explained the kinds of information that were collected from target devices; these companies included Cerberus, Hoverwatch, Mobistealth, TeenSafe, and TheTruthSpy. For the remaining companies, the references to personally identifiable information all pertained exclusively to either a visitor to the respective company's website or the information a purchaser of the stalkerware must surrender to contract with the company (e.g., email address, credit card information, etc). Though TeenSafe recognizes some information associated with children as sensitive,[154] a number of companies assert that while children (i.e., under 13 or, in the case of Cerberus, 16-18, or Hoverwatch, 16) cannot install the applications, they can be targeted by the stalkerware provided that parental consent is first obtained.[155] Notably, companies such as Hoverwatch, mSpy, and TeenSafe state they do not knowingly collect data on children;[156] where the companies are not auditing data being collected by their

154 KidBridge (formally TeenSafe) (2019), "Privacy Policy," <https://kidbridge.com/kidbridge-inc-privacy-policy/>. "Personal information means information that can be used to identify and contact an individual such as name, email address, screen name, mailing address and phone number (the "Personal Information"). **We consider such Personal Information sensitive in nature.** You, as a parent or legal guardian, need to submit Personal Information to access the Site and the KidBridge Service. By submitting information, you are consenting to our collection of such information." (Bold not in original).

155 See as examples: KidBridge (formally TeenSafe) (2019), "Privacy Policy," <https://kidbridge.com/kidbridge-inc-privacy-policy/>; and mSpy. (2018). "Terms of Use," <https://www.mspy.com/terms-of-use.html>.

156 Hoverwatch (2018), "Privacy Policy," <https://www.hoverwatch.com/privacy-policy>. ("In some countries, age restrictions may be governed by the laws of a particular jurisdiction. In standard cases, the Hoverwatch Service is not directed towards children under the age of 16.") KidBridge (formally TeenSafe) (2019), "Privacy Policy," <https://kidbridge.com/kidbridge-inc-privacy-poli-

clients, this language is presumably intended to mitigate liability for when their products are used to collect data about children.

Beyond the data which is collected by the given companies' services, the studied companies typically denoted the kinds of personal information that procurers of the products must produce to contract with the company in question. In general, this amounted to billing information such as email addresses, usernames, and passwords for the service logins, credit card details, as well as IP addresses. In the case of TeenSafe, information extended to "information about your child(ren), such as the child(ren's) date of birth and state of residence."[157]

4.2.4 Disclosures of Information

Stalkerware products are obtained to monitor the activities of the given targets; this might be direct surveillance, where the software is installed on a current or former intimate partner's device, or indirectly, where the software is installed on the device of a child who is often in an intimate partner's presence. Given the breadth of the classes of information that these software products can obtain, there is the potential for the targeted individuals to be doubly victimized: first, by the party who procures and deploys the software on the victim and, second, by the firm which might subsequently sell, share, or lose control over the data which is collected about the targeted person. In light of these modes of victimization, we examined the companies' policies to determine the extents to which the companies asserted their right to disclose collected information to third-parties, the conditions under which such disclosures were authorized, and companies' notification practices to inform impacted individuals who may have had their data either deliberately disclosed, inadvertently leaked by the company, or breached by a third-party who was neither the stalkerware company nor the stalkerware operator.

Notably, seven of the eight companies examined in this study recognized that they may share information with law enforcement organizations under certain conditions; only TheTruthSpy's policy documents lacked a reference to law

cy/>. ("Additionally, though not necessarily Personal Information, the KidBridge Service collects and provides you access to certain cell phone and computer activities (including, but not limited to, email and text messages) of your children, including through the use of computers and/or other devices on which the KidBridge software is installed and/or the Service is used (the "Accessed Activities"). For clarity, we do not knowingly collect Personal Information from children or sell any products to children."). mSpy (2018), "Privacy Policy," <https://www.mspy.com/privacy-policy.html>. ("We do not collect information you have gathered from the child's target device. All this information is encrypted.")

157 KidBridge (formally TeenSafe) (2019), "Privacy Policy," <https://kidbridge.com/kidbridge-inc-privacy-policy/>.

enforcement. Companies would disclose information where they received a court order or, alternately, if they believed in good faith that it was "necessary" to share such data; as one example, TeenSafe defined necessity as situations where:

> (i) access, use, preservation or disclosure of such information is reasonably necessary to satisfy any applicable law, regulation, legal process, such as a court order or subpoena, or a request by law enforcement or governmental authorities, (ii) such action is appropriate to enforce the Terms of Use for the KidBridge Service, including any investigation of potential violations thereof, (iii) such action is necessary to detect, prevent, or otherwise address fraud, security or technical issues associated with the KidBridge Service, or (iv) such action is appropriate to protect the rights, property or safety of KidBridge, its employees, users of the KidBridge Service or others.[158]

In all cases the policy documents strongly implied that the disclosed information would relate to the purchaser of the software, as opposed to the target of surveillance. However, the way these policies were phrased would not necessarily preclude applying them to the target of surveillance as well, insofar as all of the information that was collected tended to be associated with the purchaser of the surveillance software itself. Thus, the disclosed information might include the customer's billing information *as well as* all of the information that they collected about "their" device that they were targeting with the stalkerware.[159]

4.2.5 Security of Personal Information

The companies which provided stalkerware often gave commitments to keeping data secure, though with a range of caveats and limitations. Mobistealth, TeenSafe, and theTruthSpy all failed to provide meaningful commitments. Mobistealth's EULA stated that it did "not manage the data, nor control distribution of data, nor access personal data captured or stored on servers and databases" that the company provided.[160] TeenSafe merely discussed certain information as sensitive in nature.[161] TheTruthSpy asserted that "[t]he Publisher shall ensure that the User's personal data is kept suitably secure and shall take all useful precautions to preserve and ensure that its hosting subcontractors preserve the security and the confidentiality

158 KidBridge (formally TeenSafe) (2019), "Privacy Policy," <https://kidbridge.com/kidbridge-inc-privacy-policy/>.

159 Targeted devices likely belong to persons other than the stalkerware operator, at least in terms of who uses the device if not outright owns it. Companies asserted that their customers needed to obtain consent prior to installing the stalkerware or, alternately, only install it on their own devices (wherein they could automatically be assumed to consent to the installation of the software on their own property).

160 Mobistealth (Undated), "End User License Agreement," <https://www.mobistealth.com/eula.php>.

161 KidBridge (formally TeenSafe) (2019), "Privacy Policy," <https://kidbridge.com/kidbridge-inc-privacy-policy/>.

of this data, and in particular prevent it from being distorted, corrupted or disclosed to unauthorised persons."[162] Cerberus noted that it uses "commercially reasonable physical, managerial, and technical safeguards" but, nevertheless, cannot :

> ensure or warrant the security of any information that LSDroid receives on your behalf to operate the LSDroid Services or that you transmit to LSDroid and you do so at your own risk. We also cannot guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, ethical, or managerial safeguards.[163]

Hoverwatch provided comparable assurances in May 2018 as Cerberus, insofar as the company recognized that despite its efforts to keep data secure: "[n]o data transmission over the Internet can be guaranteed secure. As a result, while we strive to protect your personal information, we cannot guarantee the security if any information you transmit to us or from our online products or services, and you use these services at your own risk."[164] Since then, the company shortened its explanation and simply stated that it "always do[es] our best to protect data; however, no system can be absolutely safe."[165]

FlexiSPY, a company which has suffered several catastrophic security breaches and data exfiltrations,[166] asserted in its policies that the company took "great pride in the trust that you have placed with our company to keep this data secure. Our company has taken painstaking efforts to ensure that this data will be secure."[167] For Highster Mobile, we found that the company principally focused on the security of its website, and noted that the website was "scanned on a regular basis for security holes and known vulnerabilities".[168]

mSpy stood out as a unique case amongst the studied companies insofar as it provided a significant number of details about how the company works with third-parties, the kinds of encryption used, the manner in which users' credentials are

162 TheTruthSpy (2019), "Privacy Policy," <http://thetruthspy.com/privacy-policy/>.

163 Cerberus (2018), "Privacy Policy," <https://www.cerberusapp.com/privacy>.

164 Hoverwatch (Undated), "Privacy Policy," <https://www.hoverwatch.com/privacy-policy>.

165 Hoverwatch (Undated), "Privacy Policy," <https://www.hoverwatch.com/privacy-policy>.

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

167 FlexiSPY (Undated), "Privacy Policy," <https://www.flexispy.com/en/privacy-policy.htm>.

168 Highster Mobile (Undated), "Privacy Policy," <https://highstermobile.com/privacy/>.

secured, as well as how data was stored in servers' RAM and decrypted using private keys. mSpy, like FlexiSPY, suffered a pair of serious data breaches since 2015.[169]

In case of a data breach, Cerberus and Highster Mobile asserted they would notify individuals whereas mSpy would notify both individuals affected and relevant competent supervisory data protection authorities. Of note, the individuals contacted were always those who had contracted services with the company; the companies do not seek out, or alert, persons who had been targeted by their software. As a result, those who may be worst affected by a massive data breach are those who may never learn that their communications, intimate photographs or videos, geolocation data, or web browsing history had become publicly available.

4.3 Discussion

In assessing companies' policies, we considered what companies would need to do to ensure that the targets of surveillance knew that they were being monitored so as to ensure that those affected by the surveillance could be regarded as more likely to have meaningfully consented to the surveillance. We propose this not so that the targets of intimate partner violence, abuse, or harassment can be considered to have 'consented to' the monitoring and tracking but, instead, to emphasize that the secretive nature of the surveillance ought to be highly visible so that those targeted by an intimate partner are better aware of the digital surveillance they are being subjected to when using a stalkerware-infected device. Furthermore, we argue that such visibility of surveillance is important in employment situations—where companies sometimes state that their products are designed for—so that employees remain aware of the surveillance they are being placed under during the course of their employment.[170] Finally, we broadly discuss the need for companies to recognize the rights of not just the parties contracting the companies' services and software but, also, those who are targeted by the surveillance: these persons must have their basic data control and privacy rights recognized in any privacy policy or terms of service document associated with stalkerware.

This discussion should not be interpreted as asserting that fixing policies will

169 Brian Krebs (2018), "For 2nd Time in 3 Years, Mobile Spyware Maker mSpy Leaks Millions of Sensitive Records," *Krebs on Security* (September 4, 2018) <https://krebsonsecurity.com/2018/09/for-2nd-time-in-3-years-mobile-spyware-maker-mspy-leaks-millions-of-sensitive-records/>.

170 See: Cynthia Khoo, Kate Roberson, and Ronald Deibert (2019), "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications, Citizen Lab Research Report https://citizenlab.ca/docs/stalkerware-legal.pdf at Part 5Aii.

remediate harms experienced by persons targeted by stalkerware operators. For persons targeted by stalkerware to know they need to investigate company policies presumes that they are aware of the surveillance, and responsible company, in the first place: given the surreptitious nature of the surveillance, this cannot be expected to be a normal situation with this class of software. As such, the critiques of companies' policies should be understood as not asserting what targeted persons ought to do—such as read random companies' policies—but, instead, represent the outcome of third-party academic research into the nature of these policies, their contents, and their striking deficiencies.

4.3.1 Deploying Stalkerware on Children

Stalkerware can be installed directly on a target's device or, alternately, on the devices of persons who are routinely around the targeted person. As such, current or former intimate partners might install stalkerware on a child's device or repurpose dual-use technologies as a means of tracking their former partner; this is a tactic that is sometimes used where former partners have a shared child custody arrangement.[171] While two of eight companies that we studied asserted that they complied with the United States' Children's Online Privacy Protection Act (COPPA), this is an insufficient accreditation given the dual-use nature and clear harms associated with stalkerware, even if all spyware applications adhered to COPPA. Per this legislation, websites are required to post a complete privacy policy, notify parents directly about company's information collection practices, and get verifiable parental consent before collecting personal information from their children – or sharing it with others. In joint parenting situations, it is arguably insufficient to obtain consent from just one parent: all parents in the shared custody situation should be appraised of, and consent to, the surveillance of the child in question. The need for such mutual consent is heightened in situations of intimate partner violence, abuse, and stalking, insofar as single-parent consent may lead to significant harms to the partner who is fearful of violence linked with stalking behaviours.

171 See: Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell (2017), "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders," *Proceedings of the ACM on Human-Computer Interaction* 1 (CSCW, 46). "[I]t is very easy for the child and their device to become tools that are used by the abuser to continue to harass, stalk, and control the client." at 46:9. See also: Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell (2018). ""A Stalkers Paradise": How Intimate Partner Abusers Exploit Technology," *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. "We also heard of at least ten cases where abusers gave devices to *children* that they shared with the survivor, which provides additional control and access to the survivor even after they have managed to leave the relationship … in such situations, since the abuser is legally entitled to contact the child, the victim may not be allowed to remove the device."

Information Box 4: Children's Privacy Rights in the Context of Stalkerware

This discussion concerning stalkerware operators installing stalkerware on a child's phone is just one class of issues associated with using parental monitoring software to facilitate intimate partner violence, abuse, and harassment for the purpose of monitoring a former intimate partner who is the child's (co-)parent. However, surveilling children using spyware out of parental concern may also warrant scrutiny. While beyond the scope of this report, the Citizen Lab's report, "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," provides further analysis of the relevant legal issues with respect to children's privacy rights in the context of stalkerware.[172]

4.3.2 Verifying Meaningful and Informed Consent

Stalkerware companies must ensure that they obtain verifiable meaningful and informed consent from those individuals who operators use the companies' software to target for surveillance. The studied companies tended to assert that the installers of the stalkerware are responsible for obtaining appropriate consent and, moreover, that liability rested with the individuals acquiring and using the software as opposed to the companies developing and selling it. Should companies' professed intention to operate legitimately and legally be taken at their word, then they must implement a slate of changes in their existing policy regimes to remove the effectiveness of their applications as surreptitious surveillance software.

In our assessment of companies' policies there were five companies—FlexiSPY, Highster Mobile, Hoverwatch, Mobistealth, and TheTruthSpy—that lacked specific privacy-related contact information that targets of inappropriate or illegal surveillance could utilize to determine whether they had been targeted and, if so, obtain redress such as deletion of the collected materials from the company's and operator's possession, blocking the operator's access to the collected data, and assisting the targeted individual in removing the application from their phone where the individual requests it. Instead, companies focused principally on assisting the installer of software and made few or no mentions of the victims of stalkerware.

4.3.3 Technical Measures to Prevent Covert Surveillance

Stalkerware companies must implement technical measures in addition to policy changes in order to prevent their applications from being used abusively. For

172 See: Cynthia Khoo, Kate Roberson, and Ronald Deibert (2019), "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications, Citizen Lab Research Report https://citizenlab.ca/docs/stalkerware-legal.pdf at Part 5Ai.

instance, they should modify their software to present a clear dialogue message to users whenever the surveillance features of the application are triggered, and prevent those messages from being permanently dismissed or hidden. In the case of workplace surveillance, as an example, employees in Canada do not abandon all of their privacy interests to their employers; some degrees of private activity are permitted, even when using corporate devices during employment hours.[173] As such, employees should be notified by way of a prompt on the devices with this software installed with some regularity—as, at a minimum, a best practice—to inform them that their devices are being monitored by software such as those produced by the companies studied in this report. It follows that conforming with best practice around employee surveillance in Canada would also mitigate the ability of stalkerware operators to surreptitiously conduct surveillance of their current and former intimate partners.

Furthermore, while marketing documents routinely discussed the range of data which are, or can be, collected by operators using stalkerware software, there was rarely an equivalent listing of the types and range of data that stalkerware can collect in company policy documents. Save for Mobistealth, data collection is under-specified in user-facing corporate policy documents, which means that an individual who is fearful that they might have been targeted by stalkerware may be left unaware as to what the software can *actually* do, as opposed to what it is marketed as being able to do: without coherence between marketing language and policy language, a targeted person may be left uncertain as to what their abuser can, or has, actually been able to collect from the affected mobile device. Stalkerware companies broadly failed to recognize that individuals possess a quasi-constitutional right to privacy, such as in their personal information, to the extent that they should not be made targets of surveillance for other private individuals' personal purposes. Insofar as individuals think they may have been targeted by operators using stalkerware, they should be able to contact privacy staff at the companies selling and maintaining the stalkerware to request the detection of their personal information in the company's system and databases, and have the data deleted upon request.

4.3.4 Data Breach Notification

Stalkerware victimizes the targets at least once, when the data is simply collected—whether without consent, under false pretenses, or coercively—and then potentially

173 Office of the Privacy Commissioner of Canada (2004), "Privacy in the Workplace," Privacy Commissioner of Canada <https://www.priv.gc.ca/en/privacy-topics/privacy-at-work/02_05_d_17/>.

multiple additional times should the operator of the surveillance take actions against the target. Additional victimization may follow from the developers of stalkerware applications and whoever else stores the exfiltrated information suffering major data breaches. Depending on the breach, personal communications, Internet activity, photos, videos, audio recordings, travel history and locations, and more may be made publicly available. As of the time of writing, should a breach occur, only three companies asserted that they would disclose the security incident: Cerberus, Highster Mobile, and mSpy would notify the persons who had contracted with the affected company, and mSpy would also notify the relevant data protection authority. Notably, none explicitly state that they would notify individuals targeted by their software, whose personal information would in all likelihood constitute the greatest proportion of leaked data. Beyond it being critical that all companies notify individuals and data protection authorities as a matter of course, in the case of stalkerware companies they should be obligated to provide notice to those persons who are likely to be worst affected by any data breach: the actual targets of the surveillance. The need to include robust data notification is essential for companies selling or licencing child monitoring and employee surveillance applications and whose applications are being abused as stalkerware given that a vast number of these companies' databases and corporate systems have been hacked and data subsequently publicized.[174]

Even in cases where the applications are not being used to facilitate intimate partner violence or harassment, application developers should proactively ensure that they can inform employees or any other persons whose communications and activities have been monitored, on the basis that some (if not much) of their private activities will have been swept up in the monitoring. Furthermore, in Canada, employees retain privacy rights regardless of whether the device(s) happen to be provided or owned by their employer.

Finally, companies in this study are largely domiciled in the United States, with a smaller subset operating out of the European Union. This means that they might be liable under American law for unlawfully selling products and services for the purposes of intruding into the private life of individuals, and in violation of the EU's GDPR along with other European legislation should the targets of surveillance be unable to exercise their data privacy rights over collected information, including preventing any such collection in the first place. None of the companies included in

174 Since 2016, the following stalkerware companies have suffered catastrophic data breaches: Retina-X (twice), FlexiSPY, Spy Master Pro, SpyHuman, Spyfone, TheTruthSpy, Family Orbit, mSpy, Copy9, and Xnore.

this study noted having specific obligations associated with any facet of Canadian law.

4.4 Conclusion

Having assessed the publicly presented policy documents of the eight spyware companies included in our study, we found that few of them prioritized or recognized the rights of the parties subjected to surveillance. Instead, most companies focused on recognizing rights associated with the operator or purchaser of the stalkerware itself. These policy deficiencies were particularly troubling given the potential for stalkerware applications to collect large volumes of intensely intimate personal information—as designed and advertised—without the consent of the targeted person, and for the purposes of meting out either violence, abuse, or harassment towards that individual.

One area for potential future work with respect to investigating and assessing data protection practices would be to file data access requests upon a range of companies in the stalkerware industry, as both a purchaser of a given companies' products and services as well as a target of the surveillance software. The goal would be to determine how responsive the companies are in practice when responding to persons who have deployed versus who have been exploited by the stalkeware. Moreover, this process might be used to ascertain the extent to which companies meaningfully address abusive uses of their software, if at all. Previous research studies undertaken by the Citizen Lab which have used this methodology of issuing data access requests have found that companies often decline to provide substantial information to even the legitimate purchasers of software, services, and products; extending this method to the stalkerware industry would seek confirmation that data access requests are often disregarded and, as such, limited in their abilities to actually understand the classes of information collected by private companies about private individuals.

Part 5 - PIPEDA-Based Assessment

Individuals in Canada have a quasi-constitutional right to privacy.[175] These privacy rights persist to varying context-dependent extents across all manner of situations, including those associated with mobile devices, the personal data they contain, and the software which is installed on them. The data privacy implications associated with mobile applications where individuals have knowingly or willingly installed them on mobile devices "are heightened beyond traditional data collection means because of apps' ability to collect data instantaneously, continuously, and often without knowledge of the user … [and] micro-level collection of data by sensors creates more pressing data privacy implications for individuals."[176] Privacy concerns are further amplified in cases of stalkerware installations, where targeted persons may either be unaware of it having been installed on their device or have been pressured by an abusive operator into installing the tracking software. In either of these cases, the targeted person might not be regarded as having meaningfully consented to the installation or subsequent surveillance. Moreover, many spyware applications are marketed as being undetectable once installed on a targeted person'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 as compared to the already heightened concerns that mobile applications implicate more generally.

Consumer privacy rights and data protection in the context of private companies fall under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA)[177] or, alternately, under "substantially similar" provincial legislation.[178] PIPEDA applies to private sector use and management of individuals' personal information. The Office of the Privacy Commissioner of Canada is responsible for upholding and enforcing PIPEDA.

---

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

176 Adrian Fong (2017), "The role of app intermediaries in protecting data privacy" *Int'l JL & Info Tech* 25:2 at 90 (footnotes omitted).

177 Personal Information Protection and Electronic Documents Act *(PIPEDA)*, SC 2000, c 5.

178 Office of the Privacy Commissioner of Canada (2017), "Provincial legislation deemed substantially similar to PIPEDA" *Office of the Privacy Commissioner of Canada* (29 May 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. Constitutional Act, 1982,* Part 1, "*Canadian Charter of Rights and Freedoms*," s 8.

Information Box 5: A Fuller Legal Assessment of Stalkerware Under Canadian Law

The PIPEDA analysis of stalkerware in this report is excerpted and adapted from the broader legal research concerning stalkerware that was conducted by the Citizen Lab. Our full legal analysis of this class of software is found in a companion report, "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," which provides a comprehensive review of how stalkerware implicates a wide range of legal and policy issues across multiple areas of law. We assess the legality of using, creating and developing, selling, or facilitating the distribution of stalkerware applications, applying Canadian criminal law, tort law, privacy law, product liability, consumer protection, intellectual property, and intermediary liability law, as well as make recommendations for legal and policy reform to address the harms that stalkerware engenders. "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications" can be found at: https://citizenlab.ca/docs/stalkerware-legal.pdf

In this part of the report, we conducted a PIPEDA-based law analysis of stalkerware vendors, including stalkerware developers who sell their products or services.[179] We ultimately conclude that:

- Stalkerware companies should be found accountable for the collection and processing of targeted persons' personal data on the basis that the companies collect personal information, engage in relevant commercial activities, and collect, use, or disclose targeted persons' data;
- Given the potential for stalkerware companies to argue that they are exempt from PIPEDA's obligations, the OPC should issue an interpretation bulletin or additional accompanying statement to the *Guidelines for obtaining meaningful consent* or *Guidance on inappropriate data practices* that specifically address stalkerware, or the use of spyware in abusive contexts. Additionally, Parliament should consider reforming commercial sector data protection legislation to close loopholes that we have identified;
- Stalkerware companies ought to be obligated under PIPEDA to have extremely stringent data security practices based on the sensitivity of the data that they collect, process, disclose, and store; this pertains when these applications are used for ostensibly legitimate purposes and, as such, should apply to the collection of intimate data in the course of products being (re)purposed for stalkerware; and

179 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. See e.g., Personal Information Protection Act, SBC 2003, c 63 (British Columbia); and Personal Information Protection Act, SA 2003, c P-6.5 (Alberta).

- PIPEDA and the European Union's General Data Protection Regulation (GDPR) identify significant obligations that are imposed upon companies which sell products that have features enabling them to be used as stalkerware. The strength of the GDPR is ultimately found in the significant financial penalties which can be assigned to companies that fail to comply with the law. This is a strength that Parliament should add to PIPEDA by way of enabling the Privacy Commissioner of Canada to impose Administrative Monetary Penalties (AMPs) and directly enforce its recommendations on companies.

This section of the report begins by briefly noting the methodology adopted for this line of research. It then proceeds to discuss why stalkerware vendors and developers who sell their software, but not the users of the stalkerware applications, are accountable under PIPEDA for their activities. We also analyze potential exceptions that may raise challenges to holding stalkerware companies accountable under PIPEDA. Next, we identify a number of data protection rights that PIPEDA guarantees to individuals and which stalkerware companies likely violate. We then provide a brief parallel analysis of stalkerware companies under the European Union's *General Data Protection Regulation* (GDPR) to highlight ways in which Canadian legislation could better protect targets' privacy rights in the context of stalkerware-facilitated abuse. We conclude by summarizing our key findings and asserting the overall importance of looking at stalkware through the lens of PIPEDA as well as through criminal and civil law.

5.1 Methodology

We used a typical methodological approach for legal scholarship in drafting this section of the broader report. First, we conducted an review of literature associated with stalkerware. This literature review included journalistic, technical, and academic sources. Second, since stalkerware had not been closely considered in the Canadian legal system at the time of writing, our analysis drew on analogous contexts involving the legal treatment of other forms of intimate partner harassment and abuse, alternative forms of malware, or the approach that privacy law has taken in adjacent contexts. Such analysis drew on what we considered to be pertinent legal cases and judicial rulings. Finally, our legal analysis drew on pre-existing literature and research about stalkerware, particularly in the context of intimate partner abuse and gender-based violence. In aggregate, this desk research let us frame a series of legal theories concerning the extent to which stalkerware is (non) compliant with PIPEDA.

5.2 PIPEDA Assessment of Stalkerware

5.2.1 Stalkerware Vendor and Developer Accountability under PIPEDA

PIPEDA applies to every organization that collects, uses, or discloses personal information in the course of commercial activities.[180] In the stalkerware context, PIPEDA would apply to a vendor or developer if the targeted person's data was considered "personal information" and if the data collection, use, or disclosure was considered to occur as part of "commercial activities." Canadian law and jurisprudence has defined both of these terms; the subsections below 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.[181] This connection is likely established where the following conditions are met: companies are selling to, and supporting their applications' use by, operators in Canada; companies are collecting, using, and disclosing the personal information of targeted individuals in Canada; and/or companies are operating and doing business in Canada.[182]

5.2.1.1 Do Stalkerware Companies Collect "Personal Information"?

PIPEDA defines personal information as "information about an identifiable individual."[183] Both the OPC and the courts have applied this definition broadly and found that various types of data constitute personal information where such data is linkable to an identifiable individual.[184] Personal information has been found to include biometric information, photographs, videos, Global Positioning System

180 *PIPEDA*,s 4(1)(a).

181 *Lawson v Accusearch*, 2007 FC 125; Office of the Privacy Commissioner of Canada (2017), "Canadian adware developer Wajam Internet Technologies Inc. breaches multiple provisions of PIPEDA," (17 August 2017) PIPEDA Report of Findings #2017-002 <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2017/pipeda-2017-002/> at para 200; Privacy Commissioner of Canada v. SWIFT (2 April 2007), Report of Findings, Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2007/swift_rep_070402/> at para 54.

182 *Lawson v Accusearch*, 2007 FC 125; Office of the Privacy Commissioner of Canada (2017), "Canadian adware developer Wajam Internet Technologies Inc. breaches multiple provisions of PIPEDA," (17 August 2017) PIPEDA Report of Findings #2017-002 <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2017/pipeda-2017-002/> at para 200; Privacy Commissioner of Canada v. SWIFT (2 April 2007), Report of Findings, Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2007/swift_rep_070402/> at para 54.

183 *PIPEDA*, s 2(1).

184 Office of the Privacy Commissioner of Canada (2013), "Personal Information" (11 October 2013) <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/>.

Information Box 6: Privacy and Consent in the Digital Economy

When it comes to discussing privacy and data protection in the context of spyware applications, 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 an application collects from the targeted person's device and makes available to a stalkerware operator. The second sphere of concern considers how spyware applications may simultaneously collect, use, or disclose data in the way that many mobile applications 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 software in question. The result is that stalkerware may violate a targeted individual's consent on multiple levels: first, with respect to being monitored and tracked by the stalkerware operator, and second, with respect to having the application itself collecting data from the their device, regardless of whether that data is passed on to the operator.

Indeed, the Office of the Privacy Commissioner of Canada has issued a guidance specifically setting out best practices for mobile application 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.[185] The guidance emphasizes that the timing of consent is critical: applications should notify and obtain consent from individuals in real time, such as by activating a notification or symbol at the moment the software activates collection of data such as the user's location, or records a video or accesses photos.[186] This would mean that a stalkerware application should notify the targeted individual, through their device, each time it actively accesses that individual's personal information. If the software 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 it is collecting the user's personal data.

(GPS) data, and Internet Protocol (IP) addresses.[187] Data may also become personal information if there is a "serious possibility" that someone could combine it with

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

186 Office of the Information and Privacy Commissioner of Alberta and Office of the Information & Privacy Commissioner for British Columbia (2012), "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps" (24 October 2012) <https://www.priv.gc.ca/media/1979/gd_app_201210_e.pdf> at 8.

187 Office of the Privacy Commissioner of Canada (2013), "Personal Information" (11 October 2013) <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/>.

other data to identify an individual, even if the initial piece of data itself would not lead to an identifiable individual.[188]

Stalkerware applications generally collect and disclose any to all of the following information to the operator: 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 targeted person makes while using the device, and photos and videos stored on the device.[189] Much of this information would reveal or be easily linked to an identifiable individual (i.e., the targeted person) and thus be considered personal information under PIPEDA.

Information Box 7: 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, the collection or disclosure of certain kinds of information also involves data that may constitute personal information (as defined by PIPEDA) of third-party individuals with whom the targeted person communicates, such as their friends, family, colleagues, or support workers. Such data includes, for instance, SMS text conversations, call logs, or private chat or messaging histories. The privacy rights of those in contact with the targeted person are also engaged, and their consent and data protection rights may also be violated by a stalkerware application on the targeted person's device.[190] See Part 5.2.2.2 for discussion on how the OPC may consider third parties' consent to be implied in this context.

5.2.1.2 Do Stalkerware Businesses Engage in "Commercial Activity"?

PIPEDA defines commercial activity as "any particular transaction, act or conduct or

188 Office of the Privacy Commissioner of Canada (2013), "Personal Information" (11 October 2013) <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/>.

189 See Part 1.3 ("Stalkerware Capabilities") for a detailed assessment of different stalkerware applications' capabilities.

190 See, for instance, Office of the Privacy Commissioner of Canada (2009),"Mother and daughter were videotaped during covert surveillance of another individual," *PIPEDA Case Summary #2009-007*(Accessed May 14, 2019) <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.

any regular course of conduct that is of a commercial character[.]"[191] The definition of commercial activities excludes private individuals' actions from the scope of PIPEDA. The Act thus would not apply to the individual operators buying and using stalkerware (i.e., the customers of stalkerware companies) but would apply to the companies themselves. Stalkerware developers and vendors derive revenue from trafficking in the personal information of targeted persons, monitoring and tracking them through their personal devices, collecting identifying data, and disclosing such data to another party who has paid for these services. Payment for digital surveillance and stalking is core to these organizations' business model. The centrality of such actions for how businesses derive their revenue clearly brings the sale of stalkerware goods and services within the scope of commercial activity under PIPEDA.

5.2.1.3 Do Stalkerware Companies Collect, Use, or Disclose Targets' Data?

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

Primary findings from Citizen Lab researchers indicated 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 Table 1 in Part 1.3), each company routed data from targeted devices through its own servers before making the data available to the operator. For clarity, the companies collected targeted persons' data on a technological level; they did 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 disclosed the collected data to an operator through purpose-built dashboards or portals, which were maintained and provided as a way through which their customers could 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.[192] Stalkerware is functionally a service that the company

191 *PIPEDA*, s 2(1).

192 See for example: TheTruthSpy (2019), "Packages & Prices," *Thetruthspy.com* (Accessed 10 April 2019) <thetruthspy.com/the-best-free-spyware/>; Hoverwatch (2019), "Choose your plan," *Hoverwatch.com* (Accessed 10 April 2019) <https://www.hoverwatch.com/pricing>; Mobistealth (2019), "Products," *mobistealth.com* (Accessed 10 April 2019) <https://www.mobistealth.com/

provides so long as the operator continues to pay the monthly fee. A company's direct and ongoing involvement in collecting targeted persons' personal information and disclosing that data to operators through platforms that they control or develop constitute an integral aspect of the stalkerware service and business model.

5.2.1.4 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 technical summation of stalkerware applications' functionalities, as described in Part 1.3 and legally assessed in Part 5.2.1.3, suggests that targeted persons' personal information comes into, and remains, in the "possession or custody" of these application companies. As such, these businesses are responsible for the data which are exfiltrated from targeted individuals' devices, in addition to being responsible for their own customers' (i.e., the stalkerware operators') personal information.

Suppose that a stalkerware developer designed their application such that the operator could use it to monitor and exfiltrate data from the device of the targeted individual but where the developer could not access any of the targeted person'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 application company's servers or other infrastructure, or, alternatively, the data might be routed through the developer's servers without the developer(s) themselves having access it. Under the latter scenario, the developer might still be considered accountable because the data remains in their "possession and custody" by virtue of it being routed through the developer's servers.

Establishing liability may depend on the type of stalkerware involved. For example, spyware designed and expressly advertised for activities associated with intimate partner abuse, such as covert surveillance, would have a high likelihood of violating PIPEDA as a matter of course, by virtue of lacking an "appropriate purpose" under section 5(3). Ostensibly legitimate child and employee monitoring spyware is designed and used for the purpose of either covert or coerced surveillance of other individuals by the operator. The degree of sensitive information collected in tandem with its surreptitious nature is likely to give rise to harms associated with data protection law and, thus, vendors and developers of such products merit higher degrees of scrutiny than those producing software which is less involved with the collection of intimate personal information. Given that these kinds of spyware can

products.php>; and FlexiSPY (2019), "Select Your Platform to Get Started," *Flexispy.com* (Accessed 10 April 2019) <https://www.flexispy.com/en/buy-flexispy.htm>.

also be repurposed to constitute stalkerware, we argue that these kinds of dual-use applications are particularly deserving of heightened scrutiny. The third category of stalkerware includes other, narrower technologies such as "Find my phone" apps which 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 to the same degree as spyware and stalkerware, more may be required to establish a nexus between the app developer or vendor and an operator's abusive practices, such as demonstrating specific knowledge in a specific case.

Much of the analysis in this part of the report contemplates stalkerware as a kind of spyware that is designed and deployed to covertly or non-consensually monitor current or former intimate partners, or to surveil children or employees. The analysis is thus less focused on repurposed phone features (e.g., GPS) or "find my phone"-type applications.

5.2.2 Exceptions that May Remove Stalkerware Companies from PIPEDA's Ambit

There are at least three possible reasons for which PIPEDA might not apply to stalkerware companies should a private individual be responsible for deploying the software against another individual's device. This subsection reviews each argument and discusses the challenges each may pose for holding stalkerware companies accountable under PIPEDA.

5.2.2.1 "Personal or Domestic Purpose"

Section 4(2)(b) of PIPEDA excludes "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" from the Act's scope of application.[193] This provision prevents PIPEDA from being applied to individual persons.[194] Thus, pursuing legal action against a stalkerware operator who is acting in the capacity of a private individual would likely require turning to civil litigation or the criminal law.[195]

193 *PIPEDA*, s 4(2)(b); equivalent provisions appear in the *Personal Information Protection Act*, SBC 2003, c 63, s 3(2)(a) [BC PIPA] and *Personal Information Protection Act,* SA, 2003, cP-6.5, s 4(3)(a) [AB PIPA].

194 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.

195 For a legal analysis applying Canadian criminal and civil laws to the operation of stalkerware in Canada, see "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications" at https://citizenlab.ca/docs/stalkerware-legal.pdf.

Some case law around the scope of PIPEDA's application, however, suggests that stalkerware companies also may not fall under 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.[196] Under this line of reasoning, the stalkerware company acts as the agent of the stalkerware operator when collecting and disclosing the targeted person's data. In this line of legal theorization, it is the stalkerware operator that is engaging in monitoring and tracking for a personal or domestic purpose—i.e., the operator is using the technology to intimidate, harass, or abuse an individual for non-commercial purposes.

Several factors suggest that it may be inappropriate to apply the agency argument in the stalkerware context. First, all of the cases that have relied on this principle have 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 a private individual pursuing legal action or defending against a legal action to be a "personal" purpose, and this purpose 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 investigation companies' activities with respect to the person whose personal information was collected, used, or disclosed without consent, by force of section 4(2)(b) in PIPEDA. However, PIPEDA already accounts for these kinds of legal dispute-related investigations under section 7(1)(b),[197] which suggests allowing section 4(2)(b) to cover organizations would be redundant and, thus, not capture 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 investigations contexts, and based this reasoning on equivalent provisions in the Alberta *Personal Information Protection*

196 *Ferenczy v MCI Medical Clinics*, [2004] OJ No 1775, [2004] OTC 362, at para 30 [Ferenczy]; *State Farm Mutual Automobile Insurance Co v Canada* (Privacy Commissioner), 2010 FC 736, at para 106 [State Farm]; *Borowski v Aviva Canada Inc,* FSCO A07-002593, Financial Services Commission of Ontario, at paras 38-41 [Borowski]. See also Office of the Privacy Commissioner of Canada (2009), "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," *Office of the Privacy Commissioner of Canada* (Accessed May 14, 2019) <http://publications.gc.ca/collections/collection_2010/privcom/IP54-31-2009-eng.pdf, at paras 310-11>.

197 "For the 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[.]" PIPEDA, s 7(1)(b).

Act (AB PIPA).[198] 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 arguably specifically includes, in section 7, all of the exemptions where an organization's activities are of a commercial nature and collect or disclose personal information, and yet does not require knowledge or consent. The implication is that organizations that commercially collect, use, or disclose personal information without consent and under circumstances not specifically exempted are not exempt from PIPEDA, even if done "on behalf of" an individual for their own personal purpose. For clarity: there are no exclusions in PIPEDA that would explicitly exclude stalkerware vendors from being obligated to comply with PIPEDA.

Public policy considerations and the overarching objective of PIPEDA militate towards interpreting section 4(2)(b) of PIPEDA to apply only to individuals who are acting 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 personal or domestic purpose. The Alberta Information and Privacy Commissioner noted in Re Engel Brubaker, while applying the substantially similar legislation in Alberta and its equivalent to PIPEDA's section 4(2)(b):

> [R]eading section 4(3)(a) [of AB PIPA] 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).[199]

Moreover, interpreting section 4(2)(b) to exempt the commercial activities of organizations retained by private individuals for their own personal purposes

198 "While it is true that in Alberta, a similar conclusion can be achieved if section 4(3)(a) [AB PIPA's equivalent of PIPEDA's section 4(2)(b)] is read as though it embraced 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." *Re Engel Brubaker* (30 September 2010), Order P2008-010, Alberta Office of the Information and Privacy Commissioner <https://www.oipc.ab.ca/media/125275/P2008-010Order.pdf> at para 104.

199 *Re Engel Brubaker* (30 September 2010), Order P2008-010, Alberta Office of the Information and Privacy Commissioner <https://www.oipc.ab.ca/media/125275/P2008-010Order.pdf>, at para 105.

from PIPEDA would exculpate entire businesses and sectors that set themselves up specifically, or ostensibly, to only serve private individuals for a variety of personal purposes. For example, 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 are seeking DNA tests only for the personal or domestic purposes of discovering more about their own biology, and paying the company to help them further that personal purpose.

Applying section 4(2)(b) of PIPEDA to exempt stalkerware companies from accountability would have especially troubling implications where an individual uses stalkerware services in the context of intimate partner abuse or gender-based violence, due to the specific wording of "personal or domestic purposes." In the context of Canadian family law and gender equality more broadly, 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 serious and important public policy issues. 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.[200]

Should section 4(2)(b) be read to shield the commercial activities of stalkerware companies because such activities are harnessed in pursuit of a personal or domestic purpose by an abusive operator, the law would be returning intimate partner violence and gender-based abuse to the personal or domestic sphere. Such a return would be contrary to decades of legal and societal progress in pulling intimate partner violence into the open and collectively addressing it as a systemic sociopolitical problem.

5.2.2.2 Implied Consent of Third Parties

An operator's use of stalkerware implicates both third-parties' privacy rights and personal information as well as to those of the targeted person. The targeted 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

200 Beverly Balos (2004), "A Man's Home Is His Castle: How the Law Shelters Domestic Violence and Sexual Harassment," *St Louis U Pub L Rev* 77, at 87.

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 how a private individual used the company's services.

For example, 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 company's website. Specifically, the OPC wrote:

> 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.[201]

However, this application of PIPEDA would be unworkable in the stalkerware context if the "second party" (the targeted person) cannot obtain consent from their contacts to share their personal information with the operator and the stalkerware company. The targeted person may be unaware that the surveillance is occurring or, if they are, they may be prevented from revealing the operator's activities to their friends and family out of a sense of shame or fear of harm or retribution. Even if the targeted person did attempt to obtain consent, the consent or refusal to give consent 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 and thus lead 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. Thus, the onus would be upon the operator to obtain consent from the targeted individual and their contacts.

201 Office of the Privacy Commissioner of Canada (2009), "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," *Office of the Privacy Commissioner of Canada* (Accessed May 14, 2019) <http://publications.gc.ca/collections/collection_2010/privcom/IP54-31-2009-eng.pdf> at para 312.

However, the stalkerware company must in all cases "nevertheless take reasonable measures to ensure that consent is obtained by the second party"[202]—in this case, the operator.[203]

5.2.2.3 Delegating PIPEDA Compliance through Terms of Use and License Agreements

Businesses can meet their PIPEDA obligations associated with transferring data to other parties by including compliance and safeguard provisions in contract agreements.[204] As such, a stalkerware company might assert that they have complied with PIPEDA by including clauses regarding legal use and demanding that operators obtain targeted persons' consent in their privacy policy, terms of service (ToS), end user license agreements (EULAs), or other public-facing policy documents with their customers.[205]

To explore this legal theory as pertains to stalkerware vendors, we can turn to an OPC investigation into a daycare centre that had set up a live webcam feed that let parents watch their children at the daycare. Parents had to input unique passwords that were assigned to them to access the feed. One parent launched a

202 Office of the Privacy Commissioner of Canada (2009), "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," *Office of the Privacy Commissioner of Canada* (Accessed May 14, 2019) <http://publications.gc.ca/collections/collection_2010/privcom/IP54-31-2009-eng.pdf> at para 312.

203 An April 2019 joint investigation into Facebook which was led by the OPC and Information and Privacy Commissioner for British Columbia determined that "it is unreasonable for Facebook to rely on consent from the Installing User" in the context of an application collecting the personal information of the installing user's Facebook "friends" without the friends' knowledge or consent. 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/>.

204 See, e.g., in the context of using cloud providers, "In 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 (2012), "Cloud Computing for Small and Medium-sized Enterprises" *www.priv.gc.ca* (Accessed May 14, 2019) <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 (2012), "PIPEDA Interpretation Bulletin: Accountability," *www.priv.gc.ca* (Accessed May 14, 2019) <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/>.

205 See for example, FlexiSPY (2015), "Legal Disclaimer," *Flexispy.com* (Accessed 1 March 2019) <https://www.flexispy.com/en/legal-disclaimer.htm>; TheTruthSpy (2019), "Terms of Use / Legal," *TheTruthSpy.com* <thetruthspy.com/terms-of-use/>; mSpy (2018), "MSPY END USER LICENSE AGREEMENT," *mSpy.com* <https://www.mspy.com/legal-info.html>; Hoverwatch (2013), "Terms of Service," Hoverwatch <https://www.hoverwatch.com/terms-of-service>; and Highster Mobile (2018), "Terms & Conditions," Highster Mobile <https://highstermobile.com/terms/>.

complaint upon learning that the daycare was recording and storing the webcam feed. 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." This was held 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."[206] 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 for illegal activities—suffices to fulfil the developer's or vendor's obligations under PIPEDA.

Several factors distinguish the situation where an operator uses spyware abusively from that of the daycare webcam feed. In the case of the daycare webcam feed, the OPC required the daycare to implement several recommendations to bring it into compliance with its PIPEDA obligations.[207] At the least, it would seem that stalkerware developers and vendors would also have to implement measures to ensure that they are compliant with PIPEDA:

- 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 technology;
- ensuring that all monitored individuals are fully informed of the monitoring activity and associated risks; and

206 Office of the Privacy Commissioner of Canada (2012), "Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection," *PIPEDA Report of Findings #2011-008* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-008/> at paras 15-16 "Daycare Centre Modified Webcam Monitoring".

207 The additional measures included: continually updating and reviewing a list of authorized users and passwords; deactivating passwords of former clients; enabling HTTPS encryption of the video feed; regularly reviewing system logs for unusual activity or unauthorized access; clearly setting out consequences of breaching the parental contract (including removing the parent's access to the webcam feed, up to terminating their child's enrollment in the daycare); and clearly stating in a Webcam Viewing Policy that "the integrity of the webcam viewing policy is ultimately dependent upon parental compliance with the terms of agreement because there is no technology that can be employed to enforce its terms" in order to ensure all parents, particularly those not using the webcam service, are meaningfully informed of the risks. Office of the Privacy Commissioner of Canada (2012), "Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection," *PIPEDA Report of Findings #2011-008* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-008/> at paras 34 and 50-51.

- terminating the accounts of operators who are found to be using the companies' applications illegally or 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 childcare options available that do not utilize live video streaming, there is no evidence that parental consent is not freely and voluntarily provided."[208] 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[209] insofar as without that 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 or harassment.

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 the 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

208 Office of the Privacy Commissioner of Canada (2012), "Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection," *PIPEDA Report of Findings #2011-008* (Accessed May 14, 2019) <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.

209 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 for example "Child care crisis in Ontario: How to fix it?" (April 13, 2017), *Global News* (Accessed May 14, 2019) <https://globalnews.ca/video/3377473/chid-care-crisis-in-ontario-how-to-fix-it>; "Short notice of daycare closure leaves parents in limbo, highlights childcare crisis in Toronto" (June 26, 2018) *CBC* (Accessed May 14, 2019) <https://www.cbc.ca/news/canada/toronto/humberside-daycare-closing-childcare-crisis-1.4723855>; Joshua Ostroff (2017), "It's Time To Rip The Band-Aid Off Canada's Daycare Crisis," *Huffington Post* (April 27, 2017) (Accessed May 14, 2019) <https://www.huffingtonpost.ca/joshua-ostroff/justin-trudeau-parental-leave_b_9778552.html>; David MacDonald and Thea Klinger (2015), "They Go Up So Fast: 2015 Child Care Fees in Canadian Cities," *Canadian Centre for Policy Alternatives* (December 2015) (Accessed May 14, 2019) <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 (2015), "Solving BC's Affordability Crisis in Child Care," *Canadian Centre for Policy Alternatives* (July 2015) (Accessed May 14, 2019) <https://www.policyalternatives.ca/sites/default/files/uploads/publications/BC%20Office/2015/07/ccpa-bc-solving-childcare-summary_0.pdf>.

to the individual on social media."[210] 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.[211]

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 given that 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.[212] This finding suggests that stalkerware companies may be unable to escape liability by pointing to clauses, statements, or terms in clickwrap, browsewrap, or "installwrap" agreements that merely inform users that their software should only be used legally and with the knowledge and consent of those tracked.[213] 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 their disclaimers admonish against illegal or abusive uses, the same companies' marketing language sometimes encourages or appeals to such uses to drive sales.[214]

210 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.

211 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).

212 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 paras 8, 145, and 147.

213 This conclusion is further bolstered by an April 2019 joint investigation into Facebook, by the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of British Columbia, which considered Facebook's reliance on contractual agreements with application developers and reactive monitoring and enforcement measures as constituting inadequate safeguards to protect users' personal information. 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/>.

214 We identify instances where companies explicitly market their products to facilitate intimate partner violence, abuse, and harassment in Part 3.2.3 and 3.2.4 of this report. See also: Diarmid 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.

5.2.3 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. Stalkerware implicates three major principles in particular. First, a business must obtain meaningful and valid consent from the individual whose personal data is being collected, used, or disclosed. 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 unintentional exposure or unauthorized access. The following subsections discuss each of these rights—and the corresponding obligations for businesses—in turn and apply them to the stalkerware context.

5.2.3.1 Meaningful Consent

The ability to give, refuse, and withdraw consent is one of the most core rights that PIPEDA protects with respect to individuals' personal information.[215] The PIPEDA guidance page on consent establishes that organizations must obtain informed consent from "*the individual whose personal information is collected, used or disclosed*".[216] This wording ensures that consent and knowledge are tied to the individual whose personal information is implicated and, as a result, does not allow for confusion or loopholes dependent on who is considered the "user" of an application. 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 a relationship with the stalkerware application company. Explicitly requiring consent from the person who is being tracked avoids the danger that consent is tied to financial control, for instance, where the targeted individual may not be legally or contractually linked to

215 See generally *PIPEDA Schedule 1, section 4.3* ("Principle 3 - Consent"); "PIPEDA Interpretation Bulletin: Form of Consent" (11 December 2015), *Office of the Privacy Commissioner of Canada,* (Accessed May 14, 2019) <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 "Guidelines for obtaining meaningful consent" (24 May 2018), *Office of the Privacy Commissioner of Canada,* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

216 "PIPEDA Fair Information Principle 3 – Consent" (8 January 2018), *Office of the Privacy Commissioner of Canada*, (May 14, 2019) <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_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 in section 6.1, 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." *PIPEDA*, s 6.1.

their own device (e.g., if the targeted person is in a relationship where the operator legally owns the targeted person's device or is paying for the targeted person's phone plan).

Organizations must fulfill a set of obligations 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) or the targeted persons are coerced into having the stalkerware installed, or the operator repurposes an otherwise innocuous application on the targeted person'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 companies' marketing often emphasizes that operators can use the respective companies' products and services without the targeted individuals ever knowing about the applications' presence on the infected devices, let alone such applications' uses or implications for the targeted person's personal data.[217]

Stalkerware applications regularly collect sensitive or highly sensitive information without seeking consent (4.3.4), such as personal conversations and web browsing history. An individual would not reasonably expect that using their phone would result in extensive logging, tracking, and monitoring of all of their digital activity across several different applications and platforms, as well as their location, for the systematic compilation and delivery to another private individual who has specifically targeted them for ongoing tracking and surveillance in a personal context.[218] Consent is either not obtained, or may otherwise involve deception or

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

218 This is to differentiate the activity of stalkerware applications from such tracking and monitoring that online businesses and websites engage in for the purposes of user data analytics and tar-

coercion; thus consent cannot be considered obtained (4.3.5).[219] Further, stalkerware businesses often do not seek or obtain express or otherwise valid consent from targeted individuals and, instead, 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), and stalkerware businesses' lack of regard for obtaining consent persists irrespective 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 actually 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.[220] Stalkerware companies thus cannot rely on this step of obtaining the target's consent—that is, the acceptance of the capacity to access personal information—as a basis to in fact collect their data without further consent.[221]

PIPEDA contains exceptions which 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.[222] 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 disclose it to another private individual without the former's knowledge or consent, in the course of the business's commercial activities.[223]

geted or third-party advertising. Information Box 6: Privacy and Consent in the Digital Economy.

219 Danielle Keats Citron, "Spying Inc.", (2015) 72:3 *Washington and Lee L Rev* 1243 (1 June 2015) at 1250-51.

220 OPC Decision: *PIPEDA Report of Findings #2014-008* (14 May 2014): 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.

221 This line of argumentation may be 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"-type application that was already installed on the targeted person's mobile device.

222 PIPEDA, ss 7(1) (collection), 7(2) (use), and 7(3) (disclosure).

223 To the extent that stalkerware apps 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

Information Box 8: 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.[224] The consultation resulted in a report to Parliament as well as two guidance documents: "Guidelines for obtaining meaningful consent" ("Meaningful Consent Guidelines," or "Guidelines") that are effective as of January 1, 2019 and "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)" ("Inappropriate Data Practices Guidance") that are effective as of July 1, 2018.

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 the key aspects of the data collection, use, or disclosure, such as risk of harm and other consequences; stalkerware applications in typical cases do not inform the targeted persons of the applications' existence at all, let alone their 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).[225] Stalkerware applications do not 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 as well as 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."[226] An organization must implement practices based on risk of harm to the impacted individual. By their nature, stalkerware applications operate in a way that necessarily deprioritizes respecting the sensitivity of the target's information and their risk of harm; these

5.2.2, "Exceptions that May Remove Stalkerware Companies from PIPEDA's Ambit".

224 Office of the Privacy Commissioner of Canada (2018), "Consultation on consent under the Personal Information Protection and Electronic Documents Act,"*Priv.gc.ca* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/>.

225 Office of the Privacy Commissioner of Canada (2018), "Consultation on consent under the Personal Information Protection and Electronic Documents Act,"*Priv.gc.ca* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/>, see "Meaningful Consent Guidelines."

226 "Guidelines for obtaining meaningful consent" (24 May 2018), *Office of the Privacy Commissioner of Canada*, (Accessed May 14, 2019) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

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 itself as well as rendering it vulnerable to security risks such as data breaches.

The Guidelines also emphasize that individuals have the right to withdraw consent and that "[c]onsent is not a silver bullet."[227] 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."[228] This position reinforces the importance of business activities having to comport with meaningful consent for such activities to be compliant under PIPEDA. The position also speaks to broader considerations that prompt questions concerning the validity of consent in the context of an operator using stalkerware to target an individual in violent or abusive situations. The inability of some targeted individuals to unilaterally uninstall a stalkerware app from their device, let alone avoid or be protected from surreptitious surveillance in the first place, hollows out any sense of ongoing consent regardless of whether they may have initially consented to having the stalkerware application installed on their device.

5.2.3.2 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."[229] 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."[230] If an organization fails to pass muster under section 5(3) and collects or processes information for an inappropriate purpose, then it does not matter if the organization meets any other obligations under PIPEDA, such as obtaining consent, limiting collection, implementing safeguards, or ensuring data accuracy.[231]

227 "Guidelines for obtaining meaningful consent" (24 May 2018), *Office of the Privacy Commissioner of Canada*, (Accessed May 14, 2019) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

228 "Guidelines for obtaining meaningful consent" (24 May 2018), *Office of the Privacy Commissioner of Canada*, (Accessed May 14, 2019) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

229 *PIPEDA*, section 5(3).

230 See "Inappropriate Data Practices Guidance" in "Guidance on inappropriate data practices: Interpretation and application of subjection 5(3)" (Office of the Privacy Commissioner of Canada (2018), "Consultation on consent under the Personal Information Protection and Electronic Documents Act,"*Priv.gc.ca* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/.>)

231 See "Inappropriate Data Practices Guidance" in "Guidance on inappropriate data practices:

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.[232] This test assesses:

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

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

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

d) whether the privacy loss is proportional to the benefit gained.[233]

Where a stalkerware application is purpose-built to enable paying customers to covertly and non-consensually monitor and track the digital activities of those with whom they are in current or former personal relationships—possibly as part of a broader situation of intimate partner abuse or gender-based violence or harassment—that almost certainly violates section 5(3) of PIPEDA. The analysis becomes more complicated where an application does not explicitly market itself for such purposes and, instead, brands itself 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 and without meaningful 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 takes, if any, to ensure that its software is not used for harmful or illegal purposes.[234]

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 are generally "considered 'inappropriate' by a reasonable

Interpretation and application of subjection 5(3)" (Office of the Privacy Commissioner of Canada (2018), "Consultation on consent under the Personal Information Protection and Electronic Documents Act,"*Priv.gc.ca* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/.>)

232 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.

233 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.

234 For further discussion on this point, see Part 5.2.2.3 (Delegating PIPEDA Compliance through Terms of Use and License Agreements).

person" based on "more than fifteen years of applying PIPEDA, and comments received during [the] consultation on consent."[235]

Stalkerware companies' collection and disclosure of targeted individuals' personal information likely unlawfully ventures into at least three of the six (at time of writing) No-Go Zones 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 done for purposes that contravene the laws of Canada or its provinces."[236] 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.[237]
- **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'."[238] Stalkerware applications are often closely tied to intimate partner abuse and violence against women and have been used to stalk, harass,

235 See "Inappropriate Data Practices Guidance" in "Guidance on inappropriate data practices: Interpretation and application of subjection 5(3)" (Office of the Privacy Commissioner of Canada (2018), "Consultation on consent under the Personal Information Protection and Electronic Documents Act,"*Priv.gc.ca* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/>.)

236 See "Inappropriate Data Practices Guidance" in "Guidance on inappropriate data practices: Interpretation and application of subjection 5(3)" (Office of the Privacy Commissioner of Canada (2018), "Consultation on consent under the Personal Information Protection and Electronic Documents Act,"*Priv.gc.ca* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/>.)

237 For a comprehensive accounting of how stalkerware applications also likely constitute or enable criminal offences such as criminal harassment and intimidation, tortious acts such as intrusion upon seclusion and intentional infliction of mental suffering; see https://citizenlab.ca/docs/stalkerware-legal.pdf.

238 For a comprehensive accounting of how stalkerware applications also likely constitute or enable criminal offences such as criminal harassment and intimidation, tortious acts such as intrusion upon seclusion and intentional infliction of mental suffering; see https://citizenlab.ca/docs/stalkerware-legal.pdf.

intimidate, and further abuse women who have left situations of intimate partner violence.[239] The only reason that 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. Simultaneously, the company 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 likely and 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."[240] Some of the features included in stalkerware applications 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., due to having been pressured or coerced by their partner), there are several reasons for which the individual likely could not be said to have control over such recording. 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

239 Rachel Williams (2015), "Spyware and smartphones: how abusive men track their partners", *The Guardian* (January 252015) <https://www.theguardian.com/lifeandstyle/2015/jan/25/spyware-smartphone-abusive-men-track-partners-domestic-violence>.

240 "Inappropriate Data Practices Guidance" (emphasis in original) in "Guidance on inappropriate data practices: Interpretation and application of subjection 5(3)" (Office of the Privacy Commissioner of Canada (2018), "Consultation on consent under the Personal Information Protection and Electronic Documents Act,"*Priv.gc.ca* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/>.). See also, "Guidelines for Overt Video Surveillance in the Private Sector" (March 2008), *Priv.gc.ca* (Accessed May 14, 2019) <https://www.priv.gc.ca/en/privacy-topics/surveillance-and-monitoring/gl_vs_080306/>.

> 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 disclosures if they occur in the context of an abusive relationship, which may include dynamics of being controlled and manipulated by the abuser in addition to experiencing 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.[241] Stalkerware applications run afoul of this requirement by design when 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.[242]

5.2.3.3 Safeguards

PIPEDA requires organizations to safeguard the personal information in their custody and to safeguard information in ways that are proportionate with the data's degree of sensitivity.[243] Given the type and volume of personal information that are potentially collected and stored about the stalking victims whose devices are infected with stalkerware—and setting aside other legal issues around these companies'

241 *PIPEDA* Schedule 1, section 4.2.3.

242 For more, see the discussion in Part 5.2.2.2.

243 *PIPEDA* Schedule 1, section 4.7, "Principle 7 – Safeguards"; and "PIPEDA Interpretation Bulletin: Safeguards" (10 June 2015), *Office of the Privacy Commissioner of Canada* (May 14, 2019) <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/>.

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 that 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.[244] 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."[245] 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.[246]

In interviews with journalists, hackers have indicated that breaching stalkerware companies' systems was "[n]ot particularly difficult … I didn't need any 0days," in FlexiSPY's case,[247] 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."[248] 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 was comprised of photos and other data that was taken from the devices of persons targeted by stalkerware operators.[249]

244 For example, Joseph Cox and Lorenzo Franceschi-Bicchierai (2018), "'Stalkerware' Website Let Anyone Intercept Texts of Tens of Thousands of People," *Motherboard* (Accessed May 14, 2019) <https://motherboard.vice.com/en_us/article/pa97g7/xnore-copy9-stalkerware-data-breach-thousands-victims>; and Lorenzo Franceschi-Bicchierai (2018), "Spyware Company That Marketed to Domestic Abusers Gets Hacked," *Motherboard* (Accessed May 14, 2019) <https://motherboard.vice.com/en_us/article/mb4y5x/thetruthspy-spyware-domestic-abusers-hacked-data-breach>.

245 Joseph Cox and Lorenzo Franceschi-Bicchierai (2017), "'I'm Going to Burn Them to the Ground': Hackers Explain Why They Hit the Stalkerware Market," *Motherboard* (Accessed May 14, 2019) <|https://motherboard.vice.com/en_us/article/vvabv3/hackers-why-they-hit-stalkerware-flexispy-retina-x>.

246 Joseph Cox and Lorenzo Franceschi-Bicchierai (2017), "'I'm Going to Burn Them to the Ground': Hackers Explain Why They Hit the Stalkerware Market," *Motherboard* (Accessed May 14, 2019) <|https://motherboard.vice.com/en_us/article/vvabv3/hackers-why-they-hit-stalkerware-flexispy-retina-x> and Lorenzo Franceschi-Bicchierai (2018), "A Hacker Has Wiped a Spyware Company's Servers—Again," *Motherboard* (Accessed May 14, 2019) <https://motherboard.vice.com/en_us/article/3k7a5k/hacker-wipes-spyware-retina-x-flexispy>.

247 Joseph Cox and Lorenzo Franceschi-Bicchierai (2017), "'I'm Going to Burn Them to the Ground': Hackers Explain Why They Hit the Stalkerware Market," *Motherboard* (Accessed May 14, 2019) <https://www.vice.com/en_us/article/vvabv3/hackers-why-they-hit-stalkerware-flexispy-retina-x>.

248 Joseph Cox and Lorenzo Franceschi-Bicchierai (2017), "'I'm Going to Burn Them to the Ground': Hackers Explain Why They Hit the Stalkerware Market," *Motherboard* (Accessed May 14, 2019) <https://www.vice.com/en_us/article/vvabv3/hackers-why-they-hit-stalkerware-flexispy-retina-x>.

249 Lorenzo Franceschi-Bicchierai (2018), "A Hacker Has Wiped a Spyware Company's Servers—

PIPEDA requires organizations to implement "appropriate security safeguards to provide necessary protection," including physical, organizational, and technological measures, such as encryption.[250] In the case of Retina-X, the hacker found a critical key and credentials which were required to access a server that held the private data taken from persons targeted; this information was stored in plaintext.[251] 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"[252] after previously being hacked in 2015.[253]

The Office of the Privacy Commissioner of Canada does not consider the inadvertent disclosure of personal information alone, in and of itself, to automatically mean that there were inadequate safeguards in place.[254] However, the track record of data breaches 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."[255]

Again," *Motherboard* (Accessed May 14, 2019) <https://motherboard.vice.com/en_us/article/3k7a5k/hacker-wipes-spyware-retina-x-flexispy>.

250 "PIPEDA Fair Information Principle 7 – Safeguards" (2018), *Priv.gc.ca* (May 14, 2019) <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/>.

251 Lorenzo Franceschi-Bicchierai (2018), "A Hacker Has Wiped a Spyware Company's Servers—Again," *Motherboard* (Accessed May 14, 2019) <https://motherboard.vice.com/en_us/article/3k7a5k/hacker-wipes-spyware-retina-x-flexispy>.

252 "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." ("For 2nd Time in 3 Years, Mobile Spyware Maker mSpy Leaks Millions of Sensitive Records" (2018), *Krebsonsecurity.com*(May 16, 2019) <https://krebsonsecurity.com/2018/09/for-2nd-time-in-3-years-mobile-spyware-maker-mspy-leaks-millions-of-sensitive-records/>.

253 "Mobile Spyware Maker mSpy Hacked, Customer Data Leaked" (2015), *Krebsonsecurity.com* (May 16, 2019) <https://krebsonsecurity.com/2015/05/mobile-spy-software-maker-mspy-hacked-customer-data-leaked/>.

254 Office of the Privacy Commissioner of Canada (2018), "PIPEDA Interpretation Bulletin, 'Safeguards,'"*Priv.gc.ca* (May 16, 2019) <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/>.

255 Office of the Privacy Commissioner of Canada (22 August 2016), "Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Act-

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.

5.3 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 its privacy and data protection provisions. While the GDPR is not Canadian legislation, it does pertain to stalkerware operated and sold in Canada in two ways, 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."[256] This means that European stalkerware companies whose software is sold to customers in Canada or 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—then 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 else outside the EU.[257]

Many technology companies have taken their obligations under the GDPR seriously. Their recognition of these obligations and the corresponding changes to their

ing Australian Information Commissioner" *PIPEDA Report of Findings #2016-005* (May 16, 2019) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/>, at para 44.

256 GDPR, Art. 3

257 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.

business practices likely follows from 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. Both Google and Apple appeared to revitalize their data protection enforcement efforts in ensuring developer compliance with each company's respective app stores policies and developer agreements, with these moves taking place ahead of the GDPR's imminent enforcement date. Two weeks before the GDPR compliance deadline, Apple contacted all the 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.[258]

Apple also began requiring all applications to include privacy policies as of June 2018. Such policies had to "detail any third parties that [user] data is shared with—such as analytics tools, advertising networks, and third-party [software developer's kits]—and must ensure these parties are also compliant with the new policy."[259] Notably, developers of new applications submitted for review could not edit their privacy policies after obtaining approval for distribution on Apple's App Store. Instead, they could only change their policy alongside subsequent versions of the application which were also 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.[260]

5.3.1 Privacy Obligations under GDPR

Many of the GDPR's key provisions and principles align with those of Canadian commercial privacy law under PIPEDA and substantially similar provincial

258 Christian Zibreg (2018), "GDPR is coming soon so Apple starts clamping down on apps that sell your location data," *iDB* (Accessed May 16, 2019) <https://www.idownloadblog.com/2018/05/09/apple-removing-apps-location-data>; and William Judd (2018), "Apple removes location leaking apps ahead of GDPR deadline,"*Developer-tech.com* (May 16, 2019) <https://www.developer-tech.com/news/2018/may/11/apple-removes-leaky-apps-ahead-gdpr-deadline/>.

259 Danny Palmer (2018), "Apple looks to plug App Store privacy hole with new personal data policy," *Zdnet.com* (May 16, 2019) <https://www.zdnet.com/article/apple-looks-to-plug-app-store-privacy-hole-with-new-personal-data-policy>.

260 See Part 4 of "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications" for a discussion of PIPEDA's application to online intermediaries that facilitate distribution of stalkerware apps, such as mobile app stores (e.g., Google, Apple), payment processors (e.g., Paypal), and hosting providers (e.g., Codero), in the context of intermediary liability. https://citizenlab.ca/docs/stalkerware-legal.pdf

legislation, with unfavourable implications for the legality of at least certain kinds of stalkerware. The GDPR defines personal data as "any information relating to an identified or identifiable natural person," including online identifiers, and 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.[261] Stalkerware routinely captures personal data as well as 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 (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 the above obligations, such as requiring explicit consent from the data subject or notifying a data protection authority of a data breach.[262]

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."[263]

261 GDPR, Art 9.

262 "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/>.

263 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.[264]

In addition to meeting one of the above conditions for lawful collecting or processing of data, organizations and businesses subject to 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 (e.g., collecting only what is adequate, relevant, and necessary);

d) Accuracy and currency of personal data;

e) Storage limitation (e.g., 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.[265]

264 GDPR, Art. 9.

265 GDPR, Art. 5.

The GDPR mandates that companies integrate privacy by design[266] 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 of 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 of whether to share their data, the default option should be 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 designed specifically 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.

5.3.2 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"[267] 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.[268] 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 presumably applies to the broader context of intimate partner abuse and gender-based violence surrounding the stalkerware industry.

In addition, 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 forms of obtaining consent that would be considered more legitimate or less legitimate for the purpose of GDPR compliance. For example, "[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent."[269]

266 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>.

267 GDPR, Art. 4(11).

268 GDPR, Recital 43.

269 GDPR, Recital 32.

The GDPR's emphasis on valid consent, the particular form of consent, what constitutes meaningful consent (freely given, specific, informed, and unambiguous), as well as 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. 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."[270]

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 is often to strip 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 that would generally not be considered abusive on the level of stalkerware, such as applying data analytics for the purpose of targeted advertising. 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 violence, abuse, and harassment. 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).

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 their 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

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

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. Some experts have noted that this provision raises troubling implications for freedom of expression and access to information.[271] However, confined to the context of stalkerware, Article 17 provides users with an effective tool to exercise core data protection rights against entities in the context of pure collection and processing of their personal data (i.e., as opposed to user-generated content or information in the public interest, as experts concerned with the right to be forgotten most often focus upon). In the stalkerware context, for example, a targeted individual could request that the company erase their personal data "without undue delay" on grounds that the data was unlawfully processed.[272]

Article 18 lets data subjects restrict processing of their personal data under any of four circumstances: contested accuracy of data, unlawful processing (i.e., where the data subject does not desire the data to be erased), lack of further need for the data by the controller or processor, and 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 either the stalkerware vendor or developer, or against the operator who installed the stalkerware on the targeted person's device.

5.4 Discussion

In our discussion of the application of PIPEDA to companies producing stalkerware, as well as comparisons between PIPEDA and GDPR legislation, we reached

271 See for example, Daphne Keller (2017), "The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation" 33 *Berkeley Tech LJ* 297; and Michael Geist (26 January 2018), "Why a Canadian right to be forgotten creates more problems than it solves," *Globe and Mail*(May 16, 2019) <https://www.theglobeandmail.com/report-on-business/rob-commentary/why-a-canadian-right-to-be-forgotten-creates-more-problems-than-it-solves/article37757704/>.

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

the following issues of note. First, loopholes in PIPEDA may render stalkerware companies unaccountable for the collection of targeted persons' personal information. Second, an interpretation bulletin should be issued to make clear how stalkerware runs afoul of the OPC's *Guidelines for obtaining meaningful consent* and *Guidance on inappropriate data practices*. Third, companies selling this form of software are obligated to adopt the highest and most stringent standard of data protection practices. Fourth, the OPC needs the power to levy Administrative Monetary Penalties (AMPs) and independently enforce its own recommendations so as to encourage companies to bring themselves into compliance with PIPEDA where they are able to, or otherwise discontinue their operations where they are not able to. We address each of these points of discussion in turn.

5.4.1 PIPEDA Accountability: Technical Mechanism-Based Loopholes

In Part 5.2.1 we outlined why companies which produce stalkerware ought to be found accountable under PIPEDA. Part of that analysis is predicated on the position that companies cannot and ought not be permitted to exclude themselves from the PIPEDA regime even in the case that a stalkerware application extracts information from a target's device and either never routes the information through the companies' own infrastructure, or in the case that the company cannot access the exfiltrated information even if it is stored on infrastructure controlled by the company.

If a privacy commissioner or a court finds that more is required to make developers who sell and vendors accountable for their commercial activities in enabling stalkerware abuse, then the "app servers [are] not involved" situation as well as the "direct to operator" situation may constitute loopholes in PIPEDA. Should such a loophole exist, then a stalkerware company would not be responsible for complying with the *Act*, at least as far as the personal information of targeted individuals is concerned.

We argue that the developer still controls the design of the application and its functionalities, and thus bears responsibility for those who use it the way it is designed to be used—particularly as the developer may alter the functionalities and features of the application at any time by issuing updates to devices which are infected by their software. However, it is unclear whether this form of ongoing control necessarily meets the criteria for accountability under PIPEDA. Thus, further guidance concerning spyware application companies' accountability for facilitating the surreptitious collection and processing of personal information may be required.

5.4.2 Need for Legislative Reform

Our analysis in Part 5.2.2 demonstrated that there were at least three possible routes that stalkerware companies might take to assert that their activities were either exempt or beyond the scope of the legislation, or that they were compliant with PIPEDA given the companies' respective existing business practices. However, in light of the distinguishing factors from prior cases under those existing provisions, and the public policy considerations that were discussed, these companies may in fact be found to be violating PIPEDA in the event that a complaint is launched against one of these companies or in a case where they are brought before the courts.

For absolute clarity, the Office of the Privacy Commissioner of Canada, as well as its provincial counterparts, should issue an interpretation bulletin or additional accompanying statement to the *Guidelines for obtaining meaningful consent* or *Guidance on inappropriate data practices* that specifically address the use of stalkerware or use of spyware in abusive contexts, such as intimate partner violence or gender-based harassment. In the alternative or in addition, Parliament may consider reforming commercial sector data protection legislation to close these loopholes. Specifically, legislators could draft new provisions to address stalkerware-facilitated abuse.

Without this additional clarity, PIPEDA may be of limited use in providing remedy to targeted individuals or others seeking to prevent stalkerware-facilitated violence, abuse, and harassment as a privacy and data protection matter, despite such harms being systematically made possible through the commercial activities of stalkerware developers and vendors.

5.4.3 Stringent Data Security Obligations

Many of the applications which are abused to facilitate intimate partner violence, abuse, and harassment possess ostensibly legitimate purposes, such as employee or child monitoring. In the course of such business operations, the companies selling such software are responsible for collecting, storing, and transmitting incredibly intimate information, such as from all major messaging and social media applications, location information, browsing history and call logs, and more. Furthermore, many companies providing these applications have suffered catastrophic data breaches, to the effects of making monitored persons' personal and intimate information publicly available.

The classes of data which are collected for the aforementioned ostensibly legitimate purposes already require companies to adopt stringent data security protocols

based on the intimacy of the data. Such obligations are further heightened given that these applications can be repurposed or abused to facilitate intimate partner violence, abuse, and harassment; it is imperative that companies not be in situations where targets of such aggression and coercive control are doubly harmed by the act of the nonconsensual collection of their personal information *as well as* the disclosure or publication of it as a result of a major data breach. As such, companies, per PIPEDA, should enhance existing security provisions, and the OPC should open investigations into stalkerware companies to evaluate the efficacy of existing data safeguarding practices.

Information Box 9: Data Security Obligations of Stalkerware Companies

It may be the case that the very functionality of stalkerware, which is designed to grant a private individual unauthorized access to a target's personal information, inherently constitutes a fundamental breach of the obligation to implement technical safeguards.[273] On a certain level, it is challenging to meaningfully speak of stalkerware applications' safeguard obligations when, arguably, stalkerware itself is a form of malware which such safeguards are typically intended to protect against. Speaking of safeguards with regard to stalkerware also involves a certain suspension of the finding that such software should not be in operation to begin with, due to likely violating section 5(3) of PIPEDA (use, collection, or disclosure of data for an "appropriate purpose").

5.4.4 Comparing Enforcement Powers under GDPR and PIPEDA

The GDPR provides robust protection for individuals whose data is collected and processed, in addition to providing for meaningful enforcement. Such enforcement capabilities have implications for the sustainability 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, such as:

- ordering compliance with GDPR provisions;
- ordering compliance with an individual's data protection request that the GDPR has provided for;

273 "The *security safeguards shall protect personal information against loss or theft*, as well as *unauthorized access*, disclosure, copying, use, or modification." PIPEDA Schedule 1, section 4.7.1 (emphasis added).

- imposing a ban on processing data; and
- 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 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 (i.e., "name and shame") or on regulated entities' cooperation in the form of voluntarily implementing recommendations after a complaint investigation, or on compliance agreements negotiated with the non-compliant entity itself. The OPC 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.[274] There is thus comparatively little meaningful recourse in the way of either preemptive deterrence or ex post remedy and enforcement; this is particularly the case with stalkerware businesses, which are no stranger to (and demonstrably inured to) public shaming.[275] As such, legislative reforms which confer on the OPC powers similar in nature to those assigned to European data protection authorities under the GDPR would likely be helpful in regulating or disciplining companies whose products are used to, in part, facilitate stalking and intimate partner abuse and harassment.

5.5 Conclusion

Having assessed the data protection obligations of companies that sell software which can be abusively used as stalkerware, we found that such companies have extensive obligations under PIPEDA. It is worth reiterating that PIPEDA does not attach obligations to the operators of the stalkerware itself and, instead, only attaches to the companies responsible for selling the spyware apps themselves. PIPEDA is thus inherently limited in the extent to which it can be used to address stalkerware and the range of harms to which it facilitates. These limits make it important for the OPC and legislators to make clear the extent to which stalkerware companies may be held accountable under PIPEDA, and to close potential loopholes

274 "Enforcement of PIPEDA" (2019), *Priv.gc.ca* (Accessed May 16, 2019) <https://www.priv.gc.ca/biens-assets/compliance-framework/en/index#>.

275 Joseph Cox (2017), "Meet FlexiSpy, The Company Getting Rich Selling 'Stalkerware' to Jealous Lovers" *Motherboard* (Accessed May 16, 2019) <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" (2015), *Krebsonsecurity.com* (Accessed May 16, 2019) <https://krebsonsecurity.com/2015/05/more-evidence-of-mspy-apathy-over-breach/>;Lorenzo Franceschi-Bicchierai (2018), "'Stalkerware' Seller Shuts Down Apps 'Indefinitely' After Getting Hacked Again" *Motherboard* (Accessed May 16, 2019) <https://motherboard.vice.com/en_us/article/neqgn8/retina-x-spyware-shuts-down-apps>.

that would exclude such companies from responsibility for the data their software collects, uses, or discloses.

Despite the data protection obligations attaching to stalkerware companies, these same companies have sought to delimit those obligations through public policy documents, such as terms of service, privacy policies, and EULAs. Furthermore, the ambit of the OPC's capabilities to act are restricted as compared to their European data protection authority colleagues.

The legal analysis in this report is strictly confined to PIPEDA-based assessments of stalkeware companies' obligations. However, stalkerware clearly engages in classes of activities which may give rise to criminal offences on the part of operators as well as developers and vendors, or civil remedies to individuals detrimentally affected by the software. Moreover, the very development, sale, or operation of the software for the purposes of facilitating intimate partner violence, abuse, or harassment may give rise to action that the Canadian government can take, even absent a complaint from a targeted person. The Citizen Lab's report which accompanies this one, "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," provides a comprehensive legal analysis of a wide range of legal issues that may apply to the use, creation, development, sale, and third-party distribution of stalkerware in Canadian law—including criminal law, tort law, privacy law, product liability, consumer protection, and intermediary liability law.[276]

276 Cynthia Khoo, Kate Robertson, and Ronald Deibert (2019), "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," Citizen Lab, University of Toronto https://citizenlab.ca/docs/stalkerware-legal.pdf.

Part 6 - Major Findings, Recommendations, and Conclusion

Stalkerware poses serious risks to those targeted by it. Risks relate to how the stalkerware acts as a tool to facilitate controlling behaviours that inflict serious psychological, emotional, social, and financial harms associated with living under the shadow of such persistent surveillance. Stalkerware is also a tool that can accompany forms of direct abuse and violence, and which can also undermine survivor-victims' attempts to mitigate or remove themselves from such harms. In addition to the ways that stalkerware is implicated in practices of technology-facilitated violence, abuse, and harassment, the spyware also broadens the risk of impacted persons by capturing information of persons affiliated with the primary target as well as when the illicitly collected information becomes publicly available following a data breach. These risks are further accentuated in Canada due to the limits of consumer privacy law, which is federally governed by the *Personal Information Protection and Electronic Documents Act* (PIPEDA), insofar as PIPEDA only applies to the developers or businesses selling stalkerware applications and not to the actual operators of stalkerware.

Each section of this report contains discrete findings that pertain to the broader challenges that stalkerware poses for security and privacy, particularly for women and girls. In this section we present the findings that emerge as a result of layering the different methodologies that were used throughout this report to interrogate stalkerware companies' technologies, marketing, public policies, and obligations under Canadian federal consumer privacy legislation. We also present recommendations that we believe would alleviate some of the most serious harms that are raised by operators' use of these applications. Our major findings include:

- There were significant and disturbing failures by the companies in this study to obtain meaningful and ongoing consent, which seriously increased the risks and threats faced by those who operators target with stalkerware. This omission was further marked by failures to ensure that targeted persons could exercise their data access and deletion rights under Canadian privacy law;
- While these companies were accountable under Canadian consumer privacy law, the limited 'bite' of that law may impede its ability—and, by extension, that of the Office of the Privacy Commissioner of Canada (OPC)—to establish preemptive deterrence or ex post remedy and enforcement;

- Not all of the companies in this study indicated that data security was a meaningful element in their privacy policies, despite Canadian law imposing data security obligations; and
- Google's Play Protect service in tandem with antivirus applications appeared, in initial testing, to relatively reliably identify stalkerware. However, more long-term testing is required to further confirm these results.

In aggregate, we found that these companies have not developed business practices that are clearly and meaningfully designed to protect persons from inappropriate or unlawful surveillance, nor have they actively sought to assist persons targeted by stalkerware from the deleterious effects of such surveillance. Moreover, they have not clearly established business practices that would enable targeted persons to delete data collected about them by stalkerware operators and, in fact, the majority of companies in our sample promoted the use of their software for malicious purposes. Given our findings, we find it deeply concerning that these companies operate in Canada in their present capacity, and we argue that their present operations would likely require significant modification for the businesses to operate lawfully in Canada. The following sections summarize the key concerns identified in our research and highlight a number of recommendations pursuant to these concerns.

6.1 Issues Associated with Stalkerware and Consent

Organizations are required to provide individuals with the ability to give, refuse, and withdraw consent under PIPEDA. The importance of obtaining consent increases with the sensitivity of the information which is being collected. Many of the monitoring applications studied in this report have dual uses that are, on the one hand, ostensibly legitimate, and on the other, clearly deeply inappropriate. Meaningful consent is required under PIPEDA for legitimate uses. As such, companies' implementation of meaningful consent that pertains to the targets of the ostensibly legitimate uses of surveillance ought to extend to those who are inapporpriately targeted by the applications. However, and as discussed in this report, in no case did we find that the ostensibly legitimate uses conformed with meaningful consent requirements.

Recommendation 1: Prominent, Ongoing, and Meaningful Consent Dialogues

Stalkerware is often surreptitiously installed on targeted persons' devices, or devices which are operated by their children. The stealthy nature of such surveillance is by design, with some companies advising customers on how to install the software without the targeted person being aware of the surveillance. Such installation advice on the stealthy operation of the software runs counter to PIPEDA's meaningful consent provisions.

As such, we recommend that these companies implement prominent, ongoing, and meaningful consent messages so that persons affected by the ostensibly legitimate modes of surveillance associated with such software, as well as those inappropriately targeted, are kept aware of the surveillance and given opportunities to consent or, alternately, to remove consent to having their personal and intimate information collected. We would note that, given the coercive control which individuals who are subject to intimate partner violence, abuse, and harassment experience, meaningful consent may in fact be impossible to secure from the directly targeted person, to say nothing of the other persons who have their data captured by stalkerware-enabled surveillance practices.

While companies asserted in their public policy documents that the operators were obligated to obtain the consent of those targeted by the software, at no point did companies require positive and affirmative consent—on an ongoing basis—of the actual persons targeted by the surveillance. Furthermore, in the case of children being monitored, the companies presumed that only a single parent was required to consent to the monitoring. This presumption, however, belies the fact that child monitoring applications are sometimes used as a surreptitious way of spying on current or former partners by-way-of a child's mobile device. For the negatively affected partner to become aware of the surveillance, ongoing and prominent consent and surveillance notification messages must be implemented into product design.

Issues of ongoing consent are accentuated by the fact that companies did not make explicitly clear how, and under what conditions, and to what effect, the persons targeted by stalkerware could compel a company to disclose or delete the information collected by them. In short, while a range of contractual rights are assigned to the purchasers and operators of stalkerware, no equivalent agreements are reached with the actual targets of surveillance. Given that much of this surveillance takes place outside of employment situations where an employer might be subject to such disclosure requirements, it is imperative that the stalkerware companies themselves clearly explain to individuals who are inappropriately targeted by

such software that they can either withdraw their consent when it was improperly compelled (i.e., in cases where a partner applied coercion to get the targeted person to 'consent' in a non-meaningful way) or remove their data when their consent was never obtained in the first place (i.e., in cases where the operator secretly installed the stalkerware on their device, or the device of their child). Rights of access and deletion pertain to all companies which operate in Canada, and clear processes of access and deletion are needed so that those who are detrimentally affected by stalkerware understand the specific processes that companies have put in place to mitigate the harms associated with their products.

Recommendation 2: Data Access and Deletion Rights for Targets

Organizations operating in Canada and Europe have obligations to develop business practices so that persons can request access to the personal information which an organization has collected about the given persons, or have that data deleted. Such obligations are especially important to codify into discrete organizational practices where there is a potential for an organization's products to be used to significantly harm an individual's life chances and opportunities: this is the case with stalkerware.

As such, we recommend that the organizations studied in this report meaningfully implement data access and deletion policies for those detrimentally affected by their products and, in addition, that government organizations in Canada and Europe launch investigations designed to ensure these companies substantively implement practices that give meaningful effect to targeted persons' data protection rights.

Finally, we addressed how the companies which sold the dual-use products studied in this report invested in marketing their products. This report specifically investigated how companies purchased search keywords; we found that no company had invested in keywords designed to assist persons who were inappropriately targeted by the respective companies' software to remove the software from affected devices. This finding coheres with what we found when studying companies' public-facing corporate policies: in no case did those policies clearly and explicitly explain how persons targeted by stalkerware could mitigate or remediate the surveillance. Given that companies are presumably aware of how their products are perceived by members of the public, by way of popular media accounts as well as the organic search queries which drive people to their respective websites, companies should adopt practices meant to assist persons targeted by stalkerware if they are to continue selling their products and services to the prospective operators.

Recommendation 3: Stalkerware Remediation Guidance

Companies examined in their report sold dual-use products, for which one use involves the facilitation of intimate partner violence, abuse, and harassment. Most if not all companies are aware of the dual-use nature of their products.

As such, we recommend that to the extent a company is genuinely in the business of selling surveillance software that exclusively facilitates legal and ethical monitoring purposes, and to the extent these companies are allowed to continue operating, these companies implement meaningful programs and processes to assist victims of stalkerware surveillance in mitigating and remediating the surveillance and its impacts, to the extent it compromises the targeted individual's device. These companies must also make information easily accessible and actively promote it on their webpages. This information should clearly explain how stalkerware victims may seek and obtain help from the respective company. Companies should also purchase search queries to help persons targeted by such surveillance more readily find this information through general online searches. Finally, companies should educate customer service relations staff to help individuals targeted by stalkerware regain control over their data and, also, train representatives to not assist prospective stalkerware operators in acquiring the company's services. Moreover, relevant government agencies should conduct ongoing investigations into such companies in order to ensure they are in fact engaging in good-faith and responsible business practices with respect to their products and services, and providing appropriate responses to potential or impacted individuals targeted by abusive uses of their software.

Indeed, companies are already arguably compelled to adopt many of these practices by Canadian or European regulators. For example, data protection obligations under PIPEDA and the GDPR require companies to respect data subjects' right to delete their personal information in the companies' possession as well as to withdraw consent from any further use, collection, or disclosure of data. The ability to exercise such rights, of course, assumes that the targeted person had even provided any such consent initially. In fact, companies should not be enabling any type of monitoring without first obtaining explicit, informed, and ongoing consent from the intended targeted individual.

6.2 Issues with Accountability and Redress by Jurisdiction

Stalkerware developers are legally obligated to meet requirements set out in PIPEDA when operating in Canada. Given that the companies which were studied in the course of this report are involved in commercial activities and the collection of personal information of Canadians, they must comply with obligations set out in PIPEDA that pertain to consent, control of data, and the maintenance of appropriate safeguards.

However, despite these obligations, we did not find that that companies clearly recognized, or abided by, their requirements to be accountable under Canadian consumer privacy law. Furthermore, and as discussed in Section 6.1, companies routinely failed to meet their obligations concerning consent, as well as around data access and deletion rights. Obtaining redress from these violations, however, is challenged by the Office of the Privacy Commissioner of Canada's existing enforcement regime which undermines its inability to meaningfully compel changes in organizational practices that violate PIPEDA. We further found that many stalkerware companies at least modified their public facing policies to profess compliance with the General Data Protection Regulation. This step, however superficial, suggests that enabling data protection agencies to issue substantial monetary penalties in tandem with closing off potential loopholes in PIPEDA concerning stalkerware companies' practices could lead to similar changes to companies' privacy policies to recognize accountability under PIPEDA. Such changes may at the least serve to put potential operators on notice regarding the legality of stalkerware and spyware in certain contexts, while the monetary penalties themselves, combined with granting enforcement orders to the OPC, would serve as more substantive checks on abusive practices by stalkerware companies.

Recommendation 4: Update the Office of the Privacy Commissioner of Canada's Enforcement Powers

The Office of the Privacy Commissioner of Canada principally operates in an ombudsperson role. While the OPC may engage in investigations of organizations' practices and issue recommendations, binding enforcement of those recommendations requires a federal court order. This enforcement structure is significantly less robust than the powers possessed by European data protection agencies, as well as by some Canadian provincial privacy commissioners.

As such, we recommend that the Government of Canada update the federal Privacy Commissioner's enforcement toolkit to include the ability to compel companies to modify their practices instead of being able to only recommend changes. We also recommend that the OPC's toolkit be updated to empower the Commissioner to issue Administrative Monetary Penalties (AMPs) to better compel companies to modify their business practices when those practices fall short of the requirements under PIPEDA and companies refuse to modify them following a decision from the Office of the Privacy Commissioner of Canada.

Recommendation 5: Close PIPEDA-Related Loopholes Associated with Stalkerware

While we argued that stalkerware companies are, or ought to be, accountable under PIPEDA's regime, we have identified three potential legal arguments that companies might advance to try and evade accountability. Furthermore, with technical modifications to how such companies facilitate the surveillance of targeted persons, the companies might also be able to advance a technical mechanism-based argument to evade accountability. Either of these legal or technical evasions risks significantly undermining the scope and purpose of PIPEDA.

As such, we recommend that the Office of the Privacy Commissioner of Canada release information bulletins to clarify that stalkerware companies operating in Canada, when they are involved in the collection, use, or disclosure of personal information, are unambiguously accountable under PIPEDA, and that this accountability persists regardless of evasive technical mechanisms and attempted delegation of accountability to operators. Should the OPC decline to develop or release such information bulletins then federal legislators should amend PIPEDA to this end. Alternatively, provincial regulators with substantially similar legislation as PIPEDA might issue their own information bulletins, while provincial governments in those same jurisdictions might amend their own legislation

6.3 Issues with Data Security and Data Protection

Persons who acquire the surveillance software studied in this report can readily use it to facilitate intimate partner violence, abuse, and harassment. These corrosive behaviours are facilitated due to the extent of the sensitive and detailed information which is collected by the respective companies' stalkerware, typically without any notice given or meaningful consent having first been secured from the person targeted by the stalkerware operator. Both the volume and intimate nature of this data means that companies responsible for collecting or processing the data should adopt stringent security practices. This obligation is made especially clear under PIPEDA and was discussed in Section 5.2.3.3.

Companies that collect or process data in the course of providing stalkerware services have routinely suffered catastrophic security breaches. In the best case of these events, breaches have resulted in hackers deleting collected data in an effort to erase data which may have been illicitly or inappropriately collected about targeted persons. In the worst cases, organizational security failures have resulted in huge volumes of sensitive data being accessible on the public Internet. Further compounding the fact that many of the organizations which sell stalkerware services are deficient in meeting their PIPEDA requirements to safeguard data, these

deficiencies are problematically amplified by companies' malfeasance surrounding security and data breaches. Specifically, companies do not commit to informing affected persons when such breaches take place. While this moral or legal duty to notify may appear somewhat absurd in the context of a business model that is premised on deliberately engaging in deception and obfuscation, these companies sometimes advertise their core, or primary, services as child or employee monitoring. Consequently, given the intimacy of the information collected, and the primary use-case scenario that is sometimes advertised by companies, these companies should have statutorily-required notification processes in place should a breach occur which affects the persons who are targeted in the course of ostensibly legitimate surveillance activities. Ensuring that all customers and users of affected devices are notified—including those who are illicitly and inappropriately monitored using a private company's stalkerware—constitutes rudimentary social responsibility and is an increasingly common and legally required business practice.

Recommendation 6: Breach Notification Should be Adopted

Organizations must conduct data breach notifications in cases where the lost information raises significant threats or risks to individuals or groups. These obligations exist under PIPEDA as well as under the European Union's GDPR. However, most companies selling stalkerware products do not explicitly communicate that they will notify persons targeted by stalkerware and, instead, typically only focus on notifying the purchaser or operator of the stalkerware in the event that a breach should occur.

As such, we recommend that companies selling software which might have dual-uses as stalkerware explicitly assert that they will notify persons who have been targeted by stalkerware, as well as operators of the software, in the case of a data breach. Notifications should, at a minimum, be sent to the device which is being targeted by the surveillance software. We further recommend that mandatory data breach notification be statutorily required in jurisdictions where it does not already exist as a way to encourage ongoing compliance.

Academic literature and publications from non-profit organizations have often asserted that antivirus protection programs regularly fail to identify stalkerware as malware and, as such, are of limited use for protecting the targets of such surveillance. In our assessment of the capabilities of antivirus engines to detect the malicious software we found that, in many cases, the engines successfully identified three or four applications being assessed. Specifically, while a significant number of the engines identified FlexiSpy, Hoverwatch, and mSpy as malicious or suspicious, a smaller number of engines detected Cerberus as malicious or suspicious. The

only stalkerware application not identified by any of the antivirus engines was TheTruthSpy. The variation in detection rates may be associated with Cerberus having a non-obfuscated version available for sale in the Google Play Store, whereas the other stalkerware is exclusively available for sideloading onto Android devices. It remains unclear why TheTruthSpy was not detected: it may have been due to some of its development characteristics or lack of popularity. However, even though many antivirus engines detect the malware we presented to it, the mere fact that many engines are successful does not assist targeted persons that may not be aware which antivirus product(s) provide the best potential to detect and remediate the specific stalkerware on their devices.

Recommendation 7: Assessment of Antivirus Engines

Individuals who are targeted by stalkerware, and those who provide support services to them, often struggle to determine which services or products are best able to mitigate digitally-facilitated violence, abuse, and harassment. It is neither common, nor expected, that impacted persons and front-line service support workers be able to meaningfully ascertain what antivirus engines are more- or less-likely to detect stalkerware. Similarly, academic literature (including this report) tends to periodically present information about the efficacy of antivirus engines rather than producing regular reporting on how effectively antivirus engines will detect stalkerware over time.

As such, we recommend that a government body—such as the Office of Consumer Affairs—or an academic institution conduct ongoing tracking of antivirus engines and their capabilities to detect stalkerware apps on mobile devices, and make their results publicly available online. Alternatively, organizations such as Google or Samsung should present a series of antivirus programs that have a high probability of detecting stalkerware should their users search their respective application stores for ways of removing or detecting keyloggers, spyware, stalkerware, or similar kinds of illicit and surreptitious software. A non-profit organization might also periodically evaluate either government or private companies' assessment of the efficacy of the highlighted services or might, alternately, develop its own ranking of antivirus engines on an ongoing basis.

For this research study, we focused exclusively on Android-based stalkerware. We evaluated the efficacy of Google's Play Protect system and found that it was generally successful in detecting stalkerware with the exception of Cerberus, which we hypothesize may be due to a non-obfuscated version of the application which was sold as legitimate software on the Google Play Store at the time of writing. Emergent from these tentative findings, we argue that dual-purpose stalkerware may be an even more serious problem than what is initially apparent: should an

application's ostensibly legitimate uses be approved for official sale by Google, then Google's own protective systems may fail to detect ways in which the application is being used to facilitate intimate partner violence, abuse, and harassment. It is possible that there may be common practices associated with such inappropriate uses of these applications, to the effect that additional heuristics might determine when an ostensibly legitimate application is being used to facilitate harms towards the targeted device and their owner.

Recommendation 8: Updating Platform Heuristics

Stalkerware applications are often dual-use. While there are sometimes ostensibly legitimate uses of the software, such software can also be repurposed to facilitate intimate partner and familial violence, abuse, and harassment. While the Google Play Protect system appeared to be relatively effective in detecting side-loaded Android stalkerware, it is less effective in mitigating the potential for abusive social uses of dual-use software which is sold in the Google Play Store.

As such, we recommend that Google and other platform maintainers evaluate whether there are heuristics associated with abusive operations of ostensibly legitimate software, and integrate such heuristics into on-device protection services. When a potentially inappropriate use of dual-use software is detected the platform developer might re-present an application permissions screen or other user interface dialogue to mitigate the likelihood of falsely detecting—and automatically disabling—applications that are, in fact, being used for legitimate purposes.

Furthermore, we found that some of the stalkerware applications include deleterious software update mechanisms. These mechanisms might expose targets to additional threats should the update channels be abused to install software in excess of the stalkerware on targeted devices. The owners of mobile devices are unlikely to detect well-hidden stalkerware, nor are they likely to identify surreptitious software updates. As a result, operating system developers should integrate protections to prevent applications from silently running updates when doing so is not done over an encrypted or otherwise secured channel.

Recommendation 9: Protecting Against Insecure Application Updates

Operating system developers are well positioned to ascertain whether application calls are of a secure or insecure class. At the time of writing, web browsers routinely warn users when they visit insecure websites. It is not a stretch to expect that sideloaded applications' software update systems similarly be required to use encrypted channels to mitigate prospective man-in-the-middle attacks linked with unencrypted software updates. This change in behaviour could apply to insecure stalkerware programs' update channels as well as to entirely legitimate software updates for games or other applications.

As such, we recommend that operating system developers integrate protections to prevent, or at least warn, users from inadvertently trusting insecure channels to update their applications. Integrating these protections would limit the likelihood that insecure update channels for stalkerware applications could be exploited, and could more broadly enhance the security of update channels for other legitimate software applications (e.g., games, business apps, etc) that could currently be compromised by a man-in-the-middle attack.

6.4 Conclusion

Ultimately, we have found a number issues associated with the development, marketing, public policy, and legal compliance of organizations involved with the production and sale of stalkerware applications. Our recommendations in this section would, if followed, mitigate some of the worst harms associated with stalkerware. They would restrict the extent to which the software could be surreptitiously deployed, would empower targeted persons to access and delete their information, and would potentially impede the ability for stalkerware to operate on devices without their owners' awareness. To be abundantly clear however, these solutions would not address the reason for which stalkerware is a problem in the first place: the broader context of patriarchal gender inequalities, misogyny, and corrosive societal norms around controlling, abusive, and violent behaviour directed at women, girls, non-binary persons, and children. It is essential to remember that the pernicious social problem of gendered violence cannot be addressed solely by defensive technical and policy modifications. Furthermore, it is critical that any of the proposed changes in this report do not make targeted persons, who are predominantly women, responsible for their own digital safety. While modifications that principally serve to rebalance information asymmetries between the operator and target(s) of stalkerware are important, they must also be considered part of a shared responsibility that seeks to transcend systemic gender-related inequalities.

The recommendations we have listed are, on the whole, confined to the analysis conducted on stalkerware companies as part of this report. They underscore the need for a fulsome rearticulation in how all digital products and services are developed so that gender is taken into account when they are being envisioned or developed. To provide a concrete example, where a normally legitimate application is being repurposed as stalkerware, such as a 'Find My Friends' geolocation application, then antivirus engines and automated heuristics alike are unlikely to detect the software stalkerware. This deficiency speaks to the inherent challenges in developing technical solutions to prevent bad actors from abusing what might otherwise be regarded as ostensibly legitimate kinds of software. But this deficiency also reaffirms much more than the challenges of mitigating harmful uses of software: it vividly illustrates how gendering processes are inescapably embedded in software development. Determinations about what features are regarded as 'good,' and which are therefore broadly integrated into operating systems or made available on application stores, still carries risks that these features might be repurposed as stalkerware. In effect, we believe that application developers need to conduct gender-specific analyses of products prior to launching them to ensure that they do not inadvertently (or, in some cases, advertently) create dangers for women, non-binary persons, girls, and children.

Software development companies routinely release products without considering or realizing the broader social consequences or implications of their products. While developers might imagine a particular series of use-cases, customers of the products might repurpose product features for malignant purposes. In the case of surveillance software that has dual-uses, the goal of social control—of knowing where friends are, where lost phones are, where children are and what they are doing on their mobile devices—can be exploited to facilitate coercive control over current and former partners and children.

In conclusion, we believe that developers must consider potential gender-related impacts of their products prior to their release or, alternately, commit to engaging in product and service changes after learning about how their products are being used to facilitate abusive relations. Educators in computer science and engineering programs can assist in this process by including materials in curricula for students that address the importance of gender-related dimensions of software design and application. Engaging in gender-related analyses may clarify what kinds of user interface changes are required to mitigate harmful uses of companies' products and, at the same time, enhance the likelihood that companies are better able to produce products that cohere with the (presumably) positive social intervention that they

so readily insist are an important part of their products. Today, contemporary computer technology products are typically driven by masculine or patriarchal values in either explicit or implicit structural ways. It is well past time that these uneven and corrosive elements of society be directly challenged. Doing so must include confronting the implicit values, reasonings, and structures which are inherent to technologies of social control, and which are themselves far too often made available and legitimized by the largest technology companies in the world.

Appendix A - Stalkerware Policy Assessment Questions

1. Questions Concerning Company Privacy Policies/Terms of Service/ End User Licence Agreements

a) Is there a link to a privacy policy on the homepage?

b) Is there a reference to compliance with: national privacy laws, international guidelines, or self-regulatory instruments from associations?

c) Is there a "good housekeeping" seal of approval of some sort (e.g., TRUSTe)?

d) Is there a statement concerning which nation/court proceedings must go through?

e) Is there a reference in the privacy policy to the Terms of Service or End User License Agreement, and vice versa? Are there any notable contradictions between them?

f) Is there information about when the privacy policy was last updated? Is it dated? Can one access previous versions?

g) Does the company reserve the right to change the privacy policy or other public policy documents that might establish terms around the collection, use, or processing of personal information without notification? If notification is promised, under what conditions are users notified? Is notification promised to all persons whose personal information has been collected (e.g., persons targeted by stalkerware as well as operators of stalkerware)? What are the terms of accepting the new policy?

h) Is there mention of compliance with the European Union's General Data Protection Regulation?

i) Is there an arbitration clause?

2. Accessing Information About a Company's Policies

a) Is there a contact to a privacy officer listed?

b) Is there a description/discussion of who a person can complain to if they're unsatisfied with the information/processes laid out in an organization's public facing documents?

c) Is there a process for deleting one's information (i.e., a "Right to forget)?

d) Do you have to be a customer or active user of a company's products to make use of any stated procedures (e.g., right to access or delete information)?

3. Questions About a Company's Collection of Personal (or Personally Identifying) Information

a) Are there details of the specific kinds of Personally Identifiable Information (PII) which are collected? If so, what types of categories are listed?

b) Is there any distinction made between sensitive and non-sensitive PII?

c) Is any distinction made between information pertaining to children or adults?

d) Does the company require that certain information is provided, as a precursor to signing up for the service or acquiring products from the company? If so, what is asked for or collected?

4. Questions Concerning the Disclosure of Information

a) Does the company note whether it may share information with law enforcement? If so, under what conditions may information be shared? Is there a link to granular information pertaining to disclosing information with law enforcement or state agencies (e.g., a transparency report or law enforcement disclosure guidelines manual)?

5. Questions Concerning Data Security

a) Are commitments made to the security of PII?

b) Are commitments made to the encryption or deidentification of data?

c) Is there a note that users or government bodies are alerted if a data breach occurs? Are all persons who have their information disclosed notified, or only those contracting with the company?

6. Questions Concerning Access and Correction Rights

a) Is there a distinction between “users” and “targeted persons” when it comes to access and correction rights?

b) Are commitments made to allow the access of either PII or non-PII?

c) Are commitments made to all correction of either PII or non-PII?

d) Are procedures for access and correction specified? For persons contracting with the company? For persons targeted by the company’s products or services?

Appendix B: Digital Security Guides and Resources

Various non-governmental agencies or research institutions have created publicly available resources to help individuals take steps to protect their cybersecurity. Over time, these resources might become outdated; therefore, 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 intermediaries. The onus must not be on victims to avoid this harm or secure themselves.

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/resources
  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