UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

Submission of the Citizen Lab to the Ministry of Government and Consumer Services (MGCS) Consultation: Strengthening Privacy Protections in Ontario

The Honourable Lisa Thompson
Minister of Government and Consumer Services
5th Floor — 777 Bay Street
Toronto, ON M7A 2J3

[*delivered electronically*]

1 October 2020

Dear Minister Thompson:

1. The Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto ("Citizen Lab"), is an interdisciplinary laboratory which focuses on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. Our work relies on a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Citizen Lab research has included, among other work: 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 related to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

2. Our members who have prepared this submission are specialized in the privacy impacts and related human rights implications of emerging technologies, including consumer spyware apps, social media apps and platforms; predictive policing and algorithmic surveillance; corporate data collection, management, and disclosure; and the relevant law and policy issues which are engaged by such issues. Each of us have conducted in-depth legal, policy, academic, or technical research on a variety of contemporary technologies and technological systems, as well as domestic and international laws, policies, or legal processes, and have routinely provided recommendations for technology, policy, and legal reform in our respective findings. This submission was prepared under the supervision of the Director of the Citizen Lab, Professor Ronald Deibert.

3. The Citizen Lab was pleased to see that the Ontario government is committed to seeking comments on ways of improving the state and quality of privacy protections which are afforded to residents of Ontario. We are heartened to see that the government is focused on improving consent requirements, as well as enhancing the transparency of data collection, processing, and disclosure activities that are linked with personal information. We are also encouraged that the government is placing emphasis on the ability of individuals to manage their personal data through potentially enhancing data access rights and data portability, establishing enforcement powers, and prospectively including nonprofits and political parties under any reformed privacy legislation. Individuals today require more robust privacy protections than ever, given the increasingly ubiquitous 'datafication' of our behaviours, bodies, online and offline activities, and lives, for both commercial and non-commercial purposes. Further, the failure of the federal government to modernize the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") has left the province to fill in the gap. Moreover, without legislative reform, Ontario-based organizations will not be equipped to legally process European Union citizens' data or meet the high standards of the General Data Protection Regulation ("GDPR") and forthcoming assessments of Canadian privacy law's adequacy status under the EU privacy regime.

4. In this submission, the Citizen Lab makes 21 recommendations for legal and policy reform in Ontario, with a view to strengthening the privacy and data protection rights of individuals in the province. Our recommendations also provide guidance for establishing clear practices that private organizations should adhere to when interacting with collected personal information. In addition to indicating and enumerating specific recommendations throughout this submission, we have provided a consolidated list of all recommendations in **Appendix I**, which is attached to this submission.

5. The remainder of this submission is organized as follows. Part 1 provides comments and recommendations on overarching concepts and principles that we believe should guide the government in its privacy reform endeavours across the board. Parts 2 through 4 provide recommendations for focused privacy reform aimed at specific technological issues that engage privacy and data protection rights in unique ways. These recommendations emerged from Citizen Lab research investigations and legal and policy analysis of these technologies. The specific contents of each part include the following:

    - **Part 1** provides an overview of key principles, which include: a) principle-based rulemaking; b) consistency between private and public privacy governance; c) corporate transparency and accountability; d) a statutory scheme that includes all types of non-governmental organizations; e) a rights-protective approach to deletion and de-indexing as privacy remedies; f) compliance with the EU GDPR; and g) an effective remedial framework tied to statutory purpose.
    - **Part 2** presents privacy reforms to address harms arising from consumer spyware apps, or "stalkerware", in the context of intimate partner violence and gender-based abuse.
    - **Part 3** discusses the limitations of PIPEDA with respect to effectively regulating foreign companies and their exploitation of data from users in Canada in order to train censorship algorithms in China, such as the China-based Tencent, which owns and operates the popular social media and multipurpose platform, WeChat.

- **Part 4** provides recommendations for privacy reform relating to companies that sell algorithmic policing technologies to law enforcement authorities in Canada, an issue which raises complex questions where consumer privacy law intersects with constitutional privacy law and related protections in criminal justice.

1. Overarching Principles to Guide Privacy Reform in Ontario

A. Principle-Based Rulemaking

6. Reforms to Ontario privacy legislation should adopt high-level, principle-based prescriptions that avoid unduly focusing on any particular technology. Modernized legislation should, in effect, focus on achieving specific objectives rather than be overly prescriptive as to how those objectives are achieved. This approach will ensure that legislation is able to keep pace with technology and business practices as they continue to develop.

7. Principles-based rule-making is one of three types of rulemaking that new legislation often models. Below, we explain why a principles-based approach is preferred to the other two types of rule-making (known as bright-line rules, and complex or detailed rules).

8. Bright lines are designed to be simple and easily understood, such as "organizations must not collect email addresses unless they have previously obtained an individual's meaningful consent." The disadvantage of such rules is that, first, they may read narrowly and technically by actors who seek to avoid liability (e.g., under the rule, other kinds of personal information could be collected without a person's consent) and, second, that they may not capture the entirety of the conduct that the spirit of each rule is intended to address.[1]

9. Complex or detailed rules provide more granular information about what an organization would need to do in order to comply with a rule. Their very complexity can leave them susceptible to gaming. A complex rule such as, "A private organization [defined] must not collect [defined] personal information [defined] unless the following conditions are met: [defined]."[2] This language can give organizations latitude to adopt self-serving interpretations, or to assert that novel kinds of information collection, processing, or disclosure are not technically included within the scope of the rule(s) in question.[3] Ironically, increased specificity does not always increase the predictability of the rule or its application in practice.

---

1 J Black, "Principle Based Regulations: Risks, Challenges and Opportunities", London School of Economics and Political Science (2007) <http://eprints.lse.ac.uk/62814/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Black,%20J_Principles%20based%20regulation_Black_Principles%20based%20regulation_2015.pdf>.

2 JJ Siganto, "Transparent, Balanced, and Vigorous: The Exercise of the Australian Privacy Commissioner's Powers in Relation to National Privacy Principle 4" (2015) (PhD Dissertation) <https://eprints.qut.edu.au/83792/>.

3 For a discussion of why top-down bright line or complex rulemaking can inhibit robust cybersecurity and, thus, safeguards policies consider: Scott J Schakelford, Scott Russell, and Jeffrey Haut, "Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks" (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2702039>.

10. Principle-based rule frameworks are, in contrast, less susceptible to gaming or check-box compliance because the ultimate objective does not change, but rather provides a persistent normative purpose. Organizations must develop processes to achieve that purpose, but have the ability to do so in a way that is sensitive to their own business contexts. Since principles remain flexible over time due to the lack of over-prescriptiveness, as new technologies, business practices, or technical capabilities become commercially or more widely available, they are more adaptable than either bright line or complex rules.[4]

11. The increased flexibility of the principles-based approach can raise concerns regarding uncertainty or inconsistent decision-making on the part of governing bodies. However, such concerns can be mitigated through clear and careful drafting of laws and their legislative purposes, and transparency and accountability on the part of the regulator. The advantages of a built-in focus on the ultimate purpose of such rules and whether or not their objectives have been achieved through organizational practices outweighs such concerns, particularly once mitigated. Additional measures to help ensure that private organizations comply with principle-based rules include the following:

    - Close engagements between the regulator and the regulated classes of organizations based on mutual trust;
    - Clear communications by the regulator of the intended outcomes and goals of the principles; and
    - A predictable enforcement regime.[5]

12. To help organizations comply with principles-based privacy law, the Information and Privacy Commissioner of Ontario (IPC) should publish guidelines or interpretive bulletins to explain the intended outcomes and objectives of applicable laws, and explain how an organization is expected to achieve them. Educational outreach, similar to activities which the Office of the Privacy Commissioner of Canada (OPC) currently undertakes, to inform private organizations about PIPEDA, could be emulated by the IPC to assist private organizations' compliance with new legislative requirements. A robust enforcement regime, which includes the ability to assign Administrative Monetary Penalties (AMPs) that are consistently applied, would additionally incentivize organizations to comply with their lawful obligations.[6]

13. In summary, we **recommend** that the government adopt a principles-based approach to privacy legislation, in order to ensure that the law may more easily adapt to future technological advances while providing equivalent levels of privacy protection in Ontario regardless of the specific technical nature of such future technologies. This framework should be supplemented by charging the IPC with an educational mandate to help organizations to comply with their privacy law obligations, which may evolve alongside the world's evolving technological context. Any such framework should be backstopped by a strong enforcement regime to ensure effectiveness, such as providing the IPC with the ability to issue significant AMPs. (**Recommendation 1**)

---

[4] JJ Siganto, "Transparent, Balanced, and Vigorous: The Exercise of the Australian Privacy Commissioner's Powers in Relation to National Privacy Principle 4" (2015) (PhD Dissertation) <https://eprints.qut.edu.au/83792/>.

[5] Julia Black, "Forms and paradoxes of principles-based regulation" (2008) Capital Markets Law Journal 3(4) 425.

[6] For more on the need for robust enforcement, see Section G ("An Effective Remedial Framework") below.

B. Consistent High Standards Between Private and Public Privacy Governance

14. Differences between privacy laws that pertain to private organizations and government agencies can lead to irregular privacy protections and controls, to the detriment of the privacy rights of individual residents of Canada or Ontario, by way of subjecting private sector entities to a multitude of overlapping privacy regimes depending on the source of the personal data they collect, use, process, or disclose. While there can be good reasons for differentiating between personal information in custody of a public body versus in custody of a private business, such differences can sometimes weaken the privacy protections that might be applied to personal information. Where there is one set of privacy protective safeguards that apply to data obtained from private organizations and another to data obtained from the government, it can be challenging for private businesses and the government alike to assess which standards of privacy protections must be applied. More importantly, such inconsistencies can lead to personal information being less protected than it ought to be, while simultaneously increasing the costs of complying with government regulation.

15. The United States Federal Trade Commission (FTC) has found that consistency between public sector and private sector privacy regimes—where there are not compelling and contextual reasons for them to differ—both reduces the costs imposed on private organizations while also increasing compliance with privacy standards.[7] Ensuring that there is consistency in rules that apply to private sector treatment of data from government and from private organizations can specifically reduce costs on the basis that when companies contract with one another, with residents of Ontario, or with the government of Ontario, they must abide by the same rules.To have rules that apply differently to data from the government versus from private organizations may increase the numbers of staff and professionals that organizations need to ensure they are meeting either governmental or private sector privacy standards, and also is more likely to lead to errors in how personal information is protected.

16. We hasten to emphasize that any standardized rules should provide the *higher standard* of privacy protection, whether it originated in private or public sector regulation. Without this objective, there is danger that reforms will lower privacy protections for Ontarians' personal information and, as such, run exactly counter to the aims of this consultation and of any new legislation. Standardization is only a worthwhile objective if it supports strong privacy protections for personal information overall, and does not come at the expense of such protections.

17. Having a similar principle-based set of rules that apply robust privacy standards to the private sector as well as public sector will also improve the efficiency of the IPC insofar as training, research, education, legal expenses, governance, and administrative costs are likely to be reduced. Moreover, under such a set of rules, guidance promulgated by the IPC to educate on how principles are to be applied, and goals to be met, would have better applicability to the public and private sectors alike. Finally, ensuring that there are common and strong privacy regimes that rise to at least the levels

[7] United States Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," (2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

promulgated through the GDPR as applied to public and private data will increase the likelihood of Ontario privacy legislation being considered adequate under EU law.

18. In summary, we **recommend** that the government ensure that there is consistency in how private organizations are expected to protect personal information in their care and that, to accomplish this, organizations be compelled to apply either the public or private sector regulations that would maximally protect the class(es) of personal information in question. Ensuring consistency may, in addition to reforming private sector privacy legislation, also entail updating or supplanting public sector legislation where private sector regulations are found to be more protective. Such reforms will ensure that the privacy protections that apply to private sector treatment of both private sector and public sector data both are more easily complied with and will provide Ontarians with the highest standard available of privacy protection. (**Recommendation 2**)

C. Corporate Transparency

19. Private companies regularly collect and disclose personal information in the course of their legitimate organizational practices. However, research undertaken by the Citizen Lab[8] as well as other academic researchers[9] has demonstrated that the ways in which companies represent to their customers or users whom they share information with, and the purposes for such sharing, are routinely opaque to the individuals whose information has been collected. Today, commercial data sharing agreements are routinely disclosed in privacy policies or terms of service documents without making clear which specific third-party organizations receive the shared personal data, which specific purposes particular data is collected or disclosed to satisfy, or whether information has or has not been disclosed to government agents or law enforcement agencies.[10]

20. The Ontario government should implement annual transparency reporting obligations concerning disclosures without consent to law enforcement. In a 2014 report to Parliament, “Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance", the OPC recommended requiring “organizations to publicly report on the number of disclosures they make to law enforcement under paragraph 7(3)(c.1), without knowledge or consent, and without judicial warrant, in order to shed light on the frequency and use of this

---

[8] Jeffrey Knockel, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert “We Chat, They Watch: How International Users Unwittingly Build up WeChat’s Chinese Censorship Apparatus,” Citizen Lab Research Report No. 127, University of Toronto, May 2020; Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security. Open Effect Report (2016) <https://openeffect.ca/reports/Every_Step_You_Fake.pdf>.

[9] Office of the Privacy Commissioner of Canada. (2013). “Backgrounder: Results of the 2013 Global Privacy Enforcement Network Internet Privacy Sweep,” Office of the Privacy Commissioner of Canada, August 13, 2013, retrieved September 23, 2014, <https://www.priv.gc.ca/media/nr-c/2013/bg_130813_e.asp>; AM McDonald & LF Cranor, “The cost of reading privacy policies” (2008) I/S: A Journal of Law and Policy for the Information Society 4; AM McDonald, RW Reeder, PG Kelley, LF Cranor “A Comparative Study of Online Privacy Policies and Formats,” in I Goldberg, MJ Atallah, eds, Privacy Enhancing Technologies. PETS 2009, Lecture Notes in Computer Science, vol 5672 (2009: Springer Berlin Heidelberg); Jonathan A Obar & Anne Oeldorf-Hirsch, “The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services,” (2016) TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016.

[10] Colin Bennett, Christopher Parsons & Adam Molnar, “Forgetting and the right to be forgotten” (2014) in Serge Gutwirth et al, eds, Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges (Springer).

extraordinary exception."[11] While Industry Canada (now Innovation, Science and Economic Development Canada) published voluntary transparency reporting guidelines for private telecommunications service providers in 2015,[12] the Government of Canada has not fully implemented the OPC's recommendation by obligating private organizations to issue such 'transparency reports'.

21. Where the private sector is involved in the disclosure of collected or acquired information to law enforcement agencies (or any other government agency), and especially where such data is used to fuel algorithmic policing practices, such companies ought to be required to issue annual transparency reports which clarify the extent(s) to which they are sharing information with government agencies, the rationales for such disclosures, and the quantities of data which are being disclosed. Such annual reports could be filed with the IPC on an annual basis, and adhere to a template that was created by the Government of Ontario in collaboration with external stakeholders drawn from industry, civil society, and academia. We thus **recommend** that transparency reporting templates are generated in consultation between government, industry, civil society, and academia. (**Recommendation 3**)

22. In view of the above, we also **recommend** that where information has been disclosed to government agencies, organizations should be required to notify individuals of such disclosures unless pressing public interest reasons militate against such notification. Organizations should additionally be compelled to publish annual reports that disclose the frequency of, and rationales for, any disclosures to government agencies, including law enforcement authorities. (**Recommendation 4**)

23. Further, for individuals to be able to exercise their privacy and data rights, such as in the form of launching a complaint about a given business's privacy practices, they must first know that what the business is doing, or has done, with their information. As such, we **recommend** that in reforming its privacy laws, the province require private organizations to specifically disclose the information that is being collected (i.e., stating precisely what particular information is in fact collected, as opposed to stating that particular information "may" be collected) and for what specific purpose, and with whom that information has been specifically disclosed to and under what terms. (**Recommendation 5**)

D. A Statutory Scheme that Includes All Forms of Non-Government Organizations

24. Private commercial organizations, such as businesses, must already comply with federal privacy law where there is no equivalent or superceding provincial legislation. While there are routine failures to meet their requirements under the law, there is no doubt that businesses are at least expected to comply with their legal obligations under PIPEDA.

25. Businesses, of course, are not the only groups that collect personal information. Charities, non-profit organizations, and political parties all collect such information for legitimate organizational purposes. Many of these types of organizations are involved in significant data collection, processing, retention, or disclosure in order to fulfil their mandates to their members, their communities, or the electorate.

---

11 "Special Report to Parliament: Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance," Office of the Privacy Commissioner of Canada (18 July 2014) <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201314/sr_cic/>.

12 See: Industry Canada, "Transparency Reporting Guidelines," Government of Canada (2015) <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html>.

All of these groups should bear privacy and data protection obligations as private businesses are expected to, in a way that is similarly protective of personal information but contextually appropriate to the different types of non-commercial organizations.

26. Members of Parliament have been challenged to pass legislation that would place their political parties under the same rules as exist under PIPEDA but, to date, have refused to do so. They have proffered various reasons: such obligations would impose undue burden on parties; they would inhibit parties' abilities to interact with the electorate; and they would disrupt campaign offices with an influx of data access requests during the course of election campaigning.

27. However, during the last federal election, candidates who sought to represent residents of British Columbia were subject to that province's privacy laws. There is no evidence that the laws inhibited the abilities of parties to engage in their lawful and legitimate activities during the course of the election, or in the preceding or following periods of time. In addition, a civil society organization—Open Media—deployed an online system to enable individuals Canadians to ask parties to share what information they had collected about said individuals, to the individuals themselves. These requests were made to take effect the day *after* the election, to ensure that there was no undue or detrimental impact on the abilities of political parties to legitimately collect information about Canadians or use that information in the course of the election.[13]

28. That said, we acknowledge that certain kinds of organizations and activities may require special treatment under new legislation. Complex regulatory schemes can have a chilling effect on technical and artistic innovation, freedom of expression, political organization, journalistic activities, and public interest research if the legislation fails to account for the particular realities of those activities or if penalties for breach are disproportionate. As an organization that is first and foremost a research laboratory, we are particularly concerned that proposed legislation could have a chilling effect on legitimate—and vitally important—forms of security research, particularly where they involve inadvertent or technical forms of breach.

29. It may be that the most appropriate legislative framework is one which establishes exceptions or particular regimes that shield certain kinds of public interest activities from liability or applicability of certain aspects of the law. We note that in our view, it is the particular *activity* and public interest *purpose* of that activity that may deserve special legal protection, rather than the particular corporate or statutory form the organization engaged in that activity happens to take. Indeed, it is essential that any such exception be narrowly tailored in relation to the constitutional or public interest purpose it seeks to advance. Careful drafting in this regard will both mitigate concerns of overbroad enforcement, as well as discourage powerful actors from adopting specious legal arguments to evade liability.

30. In light of the above, we **recommend** that the government of Ontario include all private organizations—including businesses, charities, non-profit organizations, and political parties—in any new privacy or data protection legislation that emerges from its consultations. However, the law must

[13] While an organization could, in theory, use such a process at inopportune times such as during an election, the government could establish regulations that prevent any abuse of process while simultaneously advancing privacy rights for constituents overall.

exercise the utmost care to ensure any such regime applied to non-governmental or non-commercial organizations is contextually appropriate and proportionate to the particular purpose and activity of the regulated organization, especially where public interest activities and purposes are concerned. (**Recommendation 6**)

E. A Rights-Protective Approach to Deletion and De-Indexing as Privacy Remedies

31. The Discussion Paper's section on "data erasure" encompasses a wide range of potential activities and remedies, not all of which raise the same legal or constitutional issues. For example, the ability to request that one's personal information be deleted once it is no longer required to provide a service is a relatively straightforward principle that flows naturally from the right to withdraw consent to the use of one's personal information. On the other hand, the right to request that personal information be removed from a public website or de-indexed from search engine results necessarily implicates freedom of expression and freedom of the press, both of which are entitled to strong constitutional protection in Canada.

32. While there will doubtlessly be circumstances in which individuals' privacy rights outweigh countervailing freedom of expression concerns as a matter of constitutional law, any proposed legislation must strike a very careful balance in this regard. The ability to seek the removal or obfuscation of information online is an attractive remedy not only for those with a legitimate claim, but also for those seeking an opportunistic vehicle to silence criticism, chill dissent, and conceal valuable information of public interest.

33. We therefore **recommend** that the creation of any statutory remedy in Ontario in the nature of a "right to be forgotten" ensure that all requests for removal or de-indexing be subject to rigorous constitutional scrutiny—including the principles of minimal impairment and proportionality—by an independent and impartial court or tribunal. (**Recommendation 7**)

F. Ensuring GDPR Compliance

34. Ontario businesses which collect, process, disclose, or retain personal information pertaining to European citizens or residents are presently required to comply with the EU General Data Protection Regulation (GDPR). The GDPR is, on the whole, designed to provide European citizens and residents of Europe with a consistent and high degree of data protection, and requires that all companies which do business with Europe, or with European citizens and residents, comply with the Regulation. While some Ontario companies may be aware of their obligations and have actively modified their business practices to be in compliance, many certainly have not. In the absence of legislation mandating equivalent—or adequate—protections for Ontario businesses, there is a risk that Ontario-based businesses could be cut off from the European market on the basis of inadequately respecting Europeans' data protection rights.

35. We encourage the government of Ontario to carefully consider all elements of the GDPR and, in particular, direct its attention to specific articles that especially pertain to this consultation and which would substantially improve on the privacy and data protection rights that are currently afforded to

Ontarians. Ontario businesses should be required to provide all consumers of their products and services with heightened privacy protections, not just European customers.

36. Articles 12-23 all establish a range of rights for data subjects, from placing an onus on private organizations to explain how they interact with individuals' personal information (Art. 12), to communicating when information is being collected while also guaranteeing a right of access to personal information (Art. 13-15), to guaranteeing the ability to remove consent and restrict processing of personal data, up to and including asserting a 'right to be forgotten' or obtaining a copy of one's personal data to migrate it to another private organization (Art. 16-20), to being able to object to, know about, and place limits upon automated decision-making processes that impact individuals' legal or similarly significant interests (Arts. 21-22).[14]

37. While outside the scope of our submission, we encourage the government of Ontario to closely study these articles of the GDPR and how they have been implemented by European jurisdictions, as well as jurisdictions which have seen their privacy regimes deemed 'adequate' by the European Union. Ensuring adequacy status, which confirms that European residents'—as well as Ontarians'—data protection and privacy rights are safeguarded is critical if Ontario organizations are to be able to lawfully collect, process, retain, or disclose European residents' personal information in the course of their business operations.

38. In summary, we **recommend** that the government carefully review the GDPR and ensure that any legislation that is passed to protect Ontario residents' personal information and privacy rights are compliant with the GDPR. Compliance with the GDPR will ensure that the legislation will be deemed adequate by the European Union, so as to provide both Ontarians and Europeans with a commensurate high level of data protection. (**Recommendation 8**)

G. An Effective Remedial Framework

39. Weak or nonexistent investigative and enforcement powers are one of the greatest shortcomings of Canada's current approach to private sector privacy legislation. This is as true for Ontario and the limited powers of the IPC as it is for the OPC's ability to enforce PIPEDA. It is essential that any new legislative scheme entail powers to proactively investigate and sanction illegal conduct. Such measures, when properly calibrated, incentivize compliance with the law and the adoption of best practices.

40. In the absence of effective statutory and administrative remedies for privacy violations, private litigation (including in the form of class actions) is one of the only meaningful avenues available to deter and sanction illegal use, collection, and disclosure of personal information. While class litigation is an important tool for access to justice, it is not always adequate to deal with the full spectrum of privacy breaches and privacy harms. Private law damages arising from privacy breaches can also be difficult to articulate and quantify, creating an additional hurdle for litigants seeking a fair remedy. A

[14] See Section 4.C ("Provide GDPR-Level Due Process Rights in Automated Decision-Making") below for our recommendations on implementing the relevant GDPR articles in Canadian law, in the context of algorithmic policing technologies.

statutory presumption of prejudice and/or provisions that facilitate the award of punitive damages may help to address this concern.

41. In light of the above, we **recommend** that the government of Ontario ensure that any proposed legislation facilitates a range of remedial avenues for complainants and litigants to seek recourse for breach of their privacy rights. Recourse should be available both on an individual basis and to those seeking systemic redress for unlawful practices that violate the collective privacy rights of a particular defined group or community. This should include robust investigation and enforcement powers provided to the Ontario IPC, sufficient to deter illegal conduct and to encourage the proactive adoption of best practices. (**Recommendation 9**)

2. Focused Privacy Reform: Consumer Spyware and Stalkerware Apps

42. Mobile applications ("apps") that are deliberately designed to facilitate surreptitious real-time and remote access to digital devices, and which can be and often are used to enable intimate partner violence, harassment, or abuse, are colloquially known as stalkerware. These are mobile apps that an individual may easily and affordably purchase online and install on an unsuspecting target's phone. Stalkerware apps can enable ongoing monitoring of and access to text messages, call and messaging histories, emails, photos, videos, incoming and outgoing phone calls, GPS location, banking or other account passwords, social media accounts, and more. This technology is closely associated with technology-facilitated gender-based violence, abuse, and harassment.

43. In addition to stalkerware apps created and sold for the purposes of intimate partner violence and related gender-based abuse, there are a range of spyware apps with similar intrusive capabilities, but whose companies claim are intended for a legitimate or lawful purpose, such as child monitoring or legal employee monitoring. (It bears mentioning, however, that children and employees also possess privacy rights and thus the legitimacy of such surveillance may also be questionable.) These purported 'dual-use' vendors should be compelled to develop their apps to make it impossible—on a technical and practical basis—to use them surreptitiously on an unsuspecting individual.

44. Spyware apps designed as stalkerware, however, or which share identical features as stalkerware even if they are not marketed as such, should not be permitted to operate at all, and may in fact be subjected to criminal prosecution by way of enabling interception of private communications. The discussion and recommendations in this section of the submission which pertain to consumer spyware and stalkerware apps are mostly concerned with ostensibly legitimate spyware apps. We focus on the so-called 'legitimate' apps on the basis that intentionally designed and marketed stalkerware apps, by definition, cannot and ought not be 'rehabilitated' by bringing them superficially into compliance with commercial privacy law, given their inherently malicious nature and the ways in which they cause harms and rights violations that go far beyond the purview of data protection law, with respect to gender-based violence.

45. The Citizen Lab report, "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," contains a full analysis of stalkerware

apps under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), and briefly analyzes such apps under the European Union's General Data Protection Regulation (GDPR).[15] Its partner report, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry", which contains a holistic assessment of stalkerware apps—including technical analysis of such apps' security vulnerabilities and examining specific companies' privacy policies and search engine optimization (SEO) marketing practices—further illuminates our recommendations for privacy reform to address this class of harmful technology.[16]

46. Stalkerware apps violate several fundamental aspects of privacy and data protection laws, such as PIPEDA, on their face, due to how they operate and the purpose they serve, either by explicit advertisement or implicit design. While the problems of stalkerware and technology-facilitated gender-based violence cannot be solved through the regulation of privacy or technology alone, and reflect a much broader sociopolitical issue, a number of steps can still be taken that may mitigate or prevent harm in some cases.

47. Broadly, the Ontario government must implement laws and policies to ensure that users of stalkerware apps are not able to continue violating the consent of those targeted by this form of technology, whether through mandating built-in prominent consent mechanisms or enacting legislation to fill in interpretative or other gaps in PIPEDA. Specifically, there are potential loopholes in PIPEDA that private developers or sellers of stalkerware might exploit to argue for exemption from privacy obligations, in contravention of the spirit and objectives of privacy legislation. Ontario legislation must be developed to address this deficiency. Below we provide specific recommendations for privacy law and policy reform to address harms associated with stalkerware.

A. Protection Must Follow the Individual Whose Data Is Collected, Used or Disclosed

48. Companies that deliberately or knowingly produce software which is designed to enable digital stalking, or which they are aware is used for this purpose, violate the consent provisions in Schedule 1, section 4.3 ("Principle 3 - Consent") and section 6.1 of PIPEDA, by foreclosing on the targeted individual's ability to give, refuse to give, or withdraw consent to being monitored, tracked and surveilled through a stalkerware app on their phone. Stalkerware is not designed to seek—and often is intentionally designed to bypass—consent from the targeted individual. In addition, the full implications of such applications is often not made clear to the targeted individual whose personal information is collected and disclosed. Many stalkerware apps are designed to explicitly conceal their presence on the targeted person's smartphone. At the same time, these apps regularly collect

[15] See Cynthia Khoo, Kate Robertson, and Ronald Deibert. "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," Citizen Lab Research Report No. 120, University of Toronto (June 2019) <https://citizenlab.ca/docs/stalkerware-legal.pdf>

[16] See 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) <https://citizenlab.ca/docs/stalkerware-holistic.pdf>

sensitive or highly sensitive information and disclose the collected data to a third party, the perpetrator of the abusive surveillance.[17]

49. In research undertaken by the Citizen Lab, we found that many stalkerware companies claim to adhere to privacy laws and have privacy policies which make reference to respecting their users' privacy and data protection rights.[18] Similarly, major app stores such as Google Play and the Apple App Store, through which some stalkerware apps are distributed (despite repeated efforts to ban the most egregious forms of such apps), have explicit policies against apps collecting or disclosing personal data without clear and informed consent from users, including collection via malicious or deceptive behaviour and through other means that match how stalkerware apps operate.

50. The problem in both cases—stalkerware apps and app stores—is that one could interpret "user" to refer to the person who bought and is using the stalkerware app, that is to say, the stalkerware *operator*, or the individual perpetrating the abusive monitoring. The policies do not make clear that they are meant to apply to the *targeted individuals whose data is being wrongfully exfiltrated* by the app's user, because the targeted individuals are not themselves, technically, the "user" of the app. This gap leaves vulnerable and unprotected the individuals who are most in need of protective measures regarding consent, privacy, and malicious behaviour.

51. Under PIPEDA, privacy protective obligations are, in all cases, meant to apply to any individual whose personal information is being collected, used, or disclosed by a company's activities. Guidance from the Office of the Privacy Commissioner of Canada (OPC) clearly establishes that organizations must obtain informed consent from "the individual whose personal information is collected, used or disclosed."[19] As such, consent and knowledge requirements must be tied to the individual whose personal information is implicated and, as a result, does not allow for confusion or loopholes dependent on who is formally or technically considered the "user" of an app. Specifying the individual whose consent is required also prevents the obfuscation of obligations that may turn on the specific nature of the relationship with the stalkerware company or mobile device, and thus avoids the danger that consent is tied to financial control, for instance. App stores, online platforms, and third-party download sites should be required to specify that their data protection, privacy, consent, malicious behaviour, and related policies and terms of developers' agreements meant to protect users apply to any individual whose data, device, or activity is being tracked, monitored, collected, or disclosed by the app, even if they are not the app purchaser, the primary app "user," or the owner of the device where the app is installed.

52. In light of the above, and in view of increasing and clarifying consent requirements as set out in the Discussion Paper, we **recommend** that in enacting new privacy legislation the Ontario government make clear that the individual from whom consent is required, in all cases, is the individual whose

---

17 For a full accounting of the intrusive capabilities of a sample selection of stalkerware applications, see Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo & Ronald Deibert, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry" (June 2019), The Citizen Lab, at 20-21 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>.

18 *Ibid*, at 77-94 ("Part 4: Company User-Facing Policy Assessments").

19 Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principle 3 – Consent," (8 January 2018) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/>.

personal information is being collected, used, or disclosed, whether or not they are termed the "user" or "customer" of a particular app. To comply with this requirement, companies' privacy policies must explicitly protect and apply to individuals whose data is being collected, used, or disclosed by their product or service—whether or not that individual is considered the official "user" or "customer"—regardless of app purchase, device ownership, or whether or not the individual is the one who paid for or is controlling the surveillance software in question. (**Recommendation 10**)

B. "Personal or Domestic Purpose" Should Not Apply to Commercial Entities

53. Child and employee monitoring software, which is routinely repurposed as stalkerware, and apps designed to facilitate intimate partner surveillance, typically include features to hide their presence on someone's phone. Such features result in these app vendors inherently violating section 5(3) of PIPEDA, which requires that any collection, use or disclosure of personal information is done only "for purposes that a reasonable person would consider are appropriate in the circumstances".[20] Where a stalkerware application is purpose-built to enable paying customers to covertly, or without consent, monitor and track the digital activities of those they are in personal relationships with—possibly as part of a broader situation of intimate partner abuse or gender-based violence or harassment—this cannot by any measure be considered a reasonably appropriate purpose.

54. When apps are designed or repurposed for intimate partner surveillance, harassment, violence, or abuse they, on their face, violate at least three of the "No-Go Zones" designated by the Office of the Privacy Commissioner of Canada: collection, use, or disclosure that is otherwise unlawful (such as collection that amounts to interception of private communications, a criminal offence); collection, use, or disclosure for purposes known or likely to cause significant harm (such as where software is used to intimidate or control a person in situations of intimate partner abuse); and surveillance through audio or video functionality of the individual's own device (some child monitoring and employee apps, as well as intentionally designed stalkerware apps, allow covert remote access to, and the activation of, the targeted person's phone microphone or camera).[21]

55. While section 5(3) of PIPEDA seemingly prohibits stalkerware vendor activities (in addition to other provisions concerning consent and safeguards), section 4(2)(b) opens a potential loophole that may undermine this prohibition. Section 4(2)(b) states that the Act does not apply where an individual collects, uses, or discloses personal information for their own "personal or domestic purposes". This provision has been used to exempt commercial services that collect and disclose personal information without consent, where such services are hired by a private individual for a "personal or domestic purpose", based on the agency principle.[22] An example is hiring a private investigator to surveil and

---

20 PIPEDA, s 5(3).

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

22 *Ferenczy v MCI Medical Clinics*, [2004] OJ No 1775 at para 30 (SCJ); *State Farm Mutual Automobile Insurance Co v Canada (Privacy Commissioner)*, 2010 FC 736 at para 106; Financial Services Commission of Ontario (Arbitration Decision), *Borowski v Aviva Canada Inc*, FSCO A07-002593 at paras 38-41. See also Office of the Privacy Commissioner of Canada, "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic

surreptitiously gather personal information about an individual for the purpose of a legal proceeding, which courts have deemed a "personal" purpose.[23]

56. Following the "agency" line of reasoning, one interpretation of section 4(2)(b) is that *only* the stalkerware operator (i.e., the perpetrator) is engaged in monitoring and tracking the targeted person, and they are doing so for a "personal or domestic" purpose—i.e., using the technology to intimidate, harass, or abuse an individual for non-commercial purposes and outside the course of commercial activities. To the extent the app vendor is involved, they are only collecting and disclosing data on the operator's behalf. As a result, a spyware app vendor may argue that they do not fall under PIPEDA and are not subject to its requirements. This is despite the fact that collecting and disclosing personal data occurs in the course of their commercial activities—indeed, such illicit collection and disclosure is what the surveillance technology is designed to do and the central service for which the company is paid to provide, often on a monthly subscription fee basis.

57. As the Alberta Information and Privacy Commissioner has pointed out, however, regarding the equivalent provision of PIPEDA section 4(2)(b) in AB PIPA, section 4(3)(a),

> [R]eading section 4(3)(a) in this way [to exempt commercial activity conducted "on behalf of" paying individuals pursuing a "personal or domestic" purpose] would result in the position that not only organizations that act for the purpose of legal proceedings and related investigations would have no responsibilities under the legislation; the same would be true of any organizations that act on behalf of an individual for a personal or domestic purpose, This would be a significant result and one which, had the legislature intended it, might have been expressed specifically, rather than by way of the somewhat ambiguously-worded section 4(3)(a).[24]

58. Interpreting the "personal or domestic purpose" provision to exempt the commercial activities of organizations retained by private individuals for their own personal purposes would exculpate entire businesses and sectors that set themselves up specifically, or ostensibly, to serve private individuals for a variety of personal purposes (e.g., retail DNA analysis services, which collect sensitive personal data as part of their business model, yet whose services are used for the personal purpose of discovering one's own genetic information). Moreover, such an exemption would be particularly troubling in the case of apps that are designed or repurposed to facilitate intimate partner surveillance, abuse, violence, or harassment , due to the specific wording of "personal or domestic purposes". Such wording evokes and would cast a shadow rooted in the historical context of family law and gender equality issues, in which intimate partner violence has historically been hidden or

---

Documents Act by Elizabeth Denham Assistant Privacy Commissioner of Canada," PIPEDA Report of Findings #2009-008 (16 July 2009) at paras. 310-11.

[23] *Ibid*. This specific circumstance, however, is expressly listed as an exemption under PIPEDA, in section 7(1)(b), and potentially under BC PIPA in section 12(1)(c), which suggests that an arrangement of providing paid private surveillance services, as stalkerware companies do, in circumstances that are *not* explicitly exempted would be subject to PIPEDA and PIPA.

[24] Alberta Office of the Information and Privacy Commissioner, "Re Engel Brubaker," Order P2008- 010 (30 September 2010), at para 105.

downplayed as a "family matter" or merely constituting "domestic" problems within the private home, in contrast to being recognized as a serious and important public policy issue.[25]

59. To close the potential loophole described above, we **recommend** that the Ontario government follow the reasoning of the Alberta IPC in *Re Engel Brubaker* above, and include in any new privacy legislation explicit affirmation that companies that sell software which can be (re)purposed as stalkerware are subject to PIPEDA, to an equivalent set of obligations, or to any substantially similar legislation. The law must make clear that commercial organizations writ large cannot be exempt from PIPEDA, or from any substantially similar Ontario legislation, for reasons of being used for "personal or domestic purposes"—an exception meant to exclude private individuals, in their capacity of private individuals, alone. (**Recommendation 11**)

C. Spyware Companies Must Not be Permitted to Offload Liability to Customers

60. In the course of the Citizen Lab's examination of stalkerware companies and app vendors whose products can be used as stalkerware, we found that their terms of service and EULAs tend to demonstrate a significant disconnect between the well-documented harmful practices associated with stalkerware as a tool of technology-facilitated gender-based abuse[26] and companies' purposeful attempts to shift the burden of legal liability away from the companies themselves, to their individual customers.[27] Businesses are sometimes permitted to meet their PIPEDA obligations by including compliance and safeguard provisions in contract agreements with third parties, such as when data transfer or third-party data processing occurs in the course of their commercial activities.[28] However, such liability-offloading provisions do not and ought not to apply in the case of a app vendor whose products can be (re)purposed as stalkerware, and the product is used to disclose a targeted individual's personal information without consent to their abuser (i.e., the stalkerware operator).

---

25 "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." Beverly Balos, "A Man's Home Is His Castle: How the Law Shelters Domestic Violence and Sexual Harassment," (2004) 23 St Louis U Pub L Rev 77 at 87.

26 See Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo & Ronald Deibert, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry" (June 2019), The Citizen Lab, at 1; Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, et al, "The Spyware Used in Intimate Partner Violence," Paper delivered at 2018 IEEE Symposium on Security and Privacy (San Francisco, 18-23 May 2018).

27 Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo & Ronald Deibert, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry" (June 2019), The Citizen Lab, at 30, 91 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>.

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

61. Several decisions from the Office of the Privacy Commissioner demonstrate the limits of disclaiming liability for PIPEDA obligations by downloading it to third parties through contractual agreements. In addition, reading decisions where the OPC has permitted such downloading reveals clear distinctions between such situations, where transferring of liability is permissible, and situations involving stalkerware in the context of gender-based abuse. For example, a daycare livestreamed a daily webcam feed of the children in its care, to their parents, and required the children's parents to sign a contract agreeing to not record the webcam feed or disclose their access passwords.[29] However, to meet its PIPEDA obligations, the daycare was additionally required to: ensure an encrypted connection; regularly review system logs for unusual activity and potential abuse; ensure all monitored individuals are fully informed (in this case, children were not permitted to even enroll in the daycare unless their parents consented to the webcam); and terminate the privileges of those found to abuse their access to the webcam feed. Companies whose apps are (re)purposed to facilitate intimate partner surveillance, abuse, violence, or harassment do not appear to engage in many, if any, of these practices, on top of the missing crucial elements of consent and appropriate purpose where the targeted individual is concerned.

62. Other cases—one involving the adware developer Wajam and derelict distributors, the other involving Facebook and third-party app developers—strongly suggest that companies selling software which could be (re)purposed as stalkerware would be unable to escape liability by pointing to clauses, statements, or terms in standardized non-negotiated agreements that in effect merely inform users that the purchased software should only be used legally and with the knowledge and consent of those tracked. The OPC found that Wajam violated its consent obligations under PIPEDA because its efforts to enforce distributors' compliance with privacy obligations were inadequate, given Wajam's knowledge of distributors' violations of agreement provisions, and given the company's failure to obtain meaningful consent from users.[30] Similarly, a joint investigation into Facebook's role in the Cambridge Analytica scandal, by the OPC and the Office of the Information and Privacy Commissioner for British Columbia (OIPC BC), found the following:

> Facebook relied on contractual terms with apps to protect against unauthorized access to users' information, but then put in place superficial, largely reactive, and thus ineffective, monitoring to ensure compliance with those terms. Furthermore, Facebook was unable to provide evidence of enforcement actions taken in relation to privacy related contraventions of those contractual requirements.[31]

63. The above reasoning concerning Wajam and Facebook also apply to the stalkerware context, where stalkerware companies have evidence of potential or actual abuse—in the form of customer support requests for assistance in engaging in intimate partner surveillance, public reviews of their apps used

---

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

30 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

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

or attempted to be used for such purposes, and high-profile media coverage of their software used for intimate partner violence, abuse, and harassment[32]—and yet take little to no action whatsoever to ensure their customers are obtaining consent, respecting targeted persons' privacy and human rights, or adhering to the law in practice.[33]

64. Applying the findings regarding Wajam and Facebook to spyware companies that sell products that can be (re)purposed to facilitate intimate partner surveillance, abuse, violence, or harassment, their practices, and their policy deficiencies with respect to ensuring their products and services are not used towards abusive ends, we **recommend** that Ontario privacy law explicitly declare that spyware companies are not permitted to disclaim or offload their liability and obligations to individual customers (e.g., stalkerware operators) through terms of use or EULAs. (**Recommendation 12**)

D. Technical Mechanisms to Ensure Meaningful Consent or Notice

65. Some spyware app companies advertise themselves as possessing more legitimate purposes, such as parental monitoring of young children or lawful employee monitoring (albeit which respectively generate their own problems for privacy rights). To the extent that some spyware applications may be used for these ostensibly legitimate or legal purposes, or have been truly consented to and opted-in to by the tracked individual, such apps must include technical mechanisms to support an opt-in model by default and informed, ongoing, consent. Examples of such mechanisms include "just-in-time" alerts that inform an individual if certain phone features have been turned on—such a microphone, camera, or GPS location—and persistent notifications, which can take the form of a notice running across the top of the phone's screen so long as the tracking, recording, or monitoring continues.

66. Spyware applications which are principally designed to facilitate intimate partner violence, abuse, or harassment 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 provide targeted individuals with the option to refuse or stop such surveillance if it is discovered. For example, Citizen Lab research found an instance where operators were given the option to turn on a feature that prevents the device user (i.e., the targeted person) from uninstalling the app.

67. Moreover, 'dual use' apps with ostensibly non-malicious purposes are also routinely used to facilitate intimate partner violence, abuse, or harassment, and researchers and media reports have demonstrated that the purveyors of these apps often know of their nefarious uses and are willing to assist in enabling them.[34]

---

32 Cynthia Khoo, Kate Robertson, and Ronald Deibert. "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," Citizen Lab Research Report No 120, University of Toronto, June 2019, at pages 129-130 <https://citizenlab.ca/docs/stalkerware-legal.pdf>.

33 See Section E ("Spyware Companies' Privacy Policies Are Overwhelmingly Deficient and Lack Remedy and Data Access/Deletion Rights for Victims") below.

34 See e.g., Anita Elash, "Makers of spyware deny marketing their apps to stalkers in domestic-abuse cases," CBC (13 June 2019) <https://www.cbc.ca/news/technology/spyware-apps-deny-marketing-for-stalking-1.5174294>; Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, et al, "The Spyware Used in Intimate Partner Violence," Paper delivered at 2018 IEEE Symposium on Security and Privacy (San Francisco, 18-23 May 2018), at 2; and Nicki Dell, Karen Levy, Damon McCoy, and Thomas Ristenpart, "How domestic abusers use smartphones to spy on their

68. In the event there are some apps that are genuinely designed for beneficial purposes—such as finding a lost phone—and without reason to maintain features that militate towards abusive purposes, all apps with the kind of monitoring, tracking, remote access, or surveillance capabilities associated with spyware and stalkerware should be required to have built-in persistent notifications and just-in-time alerts at a minimum. Such design elements would contribute towards ensuring that meaningful consent is obtained, at least in cases outside of abusive situations or where there is no power dynamic or coercion involved between the operator and targeted person.

69. A requirement to facilitate consent through technological features might be compared to the Principle 7 safeguards obligation in PIPEDA, which mandates that companies must implement reasonable physical, administrative, and *technical* safeguards to meet the obligation to protect personal information from unauthorized access (Section 4.7, or Principle 7, in Schedule 1).[35] Technical features to ensure consent is obtained from targeted individuals, in the context of all smartphone apps that could be designed or repurposed to facilitate intimate partner violence, abuse, or harassment are particularly critical, given the sensitive and intimate nature of much of the information that is collected and disclosed. Despite these requirements under PIPEDA, spyware apps persist in secretly collecting and disclosing targeted persons' personal information and, even should a complaint be brought under PIPEDA, the OPC lacks any formal enforcement mechanisms to enforce any recommendations that flow from the complaint.

70. We **recommend** that the Ontario government apply a similar approach as PIPEDA applies for the safeguards requirement, to strengthen consent and notice requirements. Effective mechanisms should make it nearly impossible for a tracked, monitored, or recorded individual to remain unaware of what their device is doing. For mobile apps that allow tracking, monitoring, and surveillance of targeted individuals, provided there is a legitimate or legal purpose, meeting the requirement for meaningful consent should necessitate building in technical features such as persistent notifications and just-in-time alerts. (**Recommendation 13**)

E. Spyware Companies' Privacy Policies Are Overwhelmingly Deficient and Lack Remedy and Data Access/Deletion Rights for Victims

71. Many companies that sell software that can be used for ostensibly legitimate or lawful aims, such as child or employee monitoring but which can be repurposed as stalkerware, claim to adhere to privacy laws and have privacy policies which make reference to respecting their users' privacy and data protection rights.[36] Recent research conducted at the Citizen Lab provided a systematic methodological assessment of a selection of these companies' privacy policies, terms of service

partners," Vox (21 May 2018). <https://www.vox.com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spyware-domestic-abusers-apple-google>.

35 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Schedule 1 at s 4.7, "Principle 7 – Safeguards" (emphasis added).

36 *Ibid*, at 77-94 ("Part 4: Company User-Facing Policy Assessments"). To be clear, app vendors that intentionally and knowingly design, sell, and advertise their apps as stalkeware for the purposes of intimate partner surveillance also provide privacy policies and purport to respect individuals' privacy and data protection rights. Our recommendations in this submission are, for the most part, predicated on the view that such businesses are entirely prohibited by PIPEDA from operating at all, and thus it would be, in a certain sense, moot to attempt to bring them into compliance with obligations that address only secondary concerns.

agreements, and end user license agreements (EULAs) to better understand how these companies' businesses account (or do not account) for privacy and security protections as part of the operation of their products and services. We examined these policies to determine how these companies interpret their legal (and ethical) obligations to customers who use stalkerware on others (operators) or individuals who are victimized (targeted persons) by their products and services. We found that such companies—both those which intentionally design and advertise their products as stalkerware, and those which sell products for ostensibly legitimate or lawful purposes but which are used as stalkerware—largely fail to be explicit in their policies about how, in accordance with obligations under PIPEDA and GDPR, they will provide recourse to 'non-customer' targeted persons or other individuals who have not provided consent to have their data collected.

72. Our systematic evaluation identified a range of policy deficiencies that may exacerbate harm to digital privacy, beyond the harms that apps (re)purposed as stalkerware—and the people who create and use such apps—themselves already engender by nature. Policy deficiencies included lack of information or clarity, including (but not limited to) a lack of: information regarding whether or how a company defined 'personal information'; whether or how companies disclosed collected data to third parties; and whether or how a company has made commitments about data security or data breach notification. The findings were disconcerting.

73. Overwhelmingly, companies failed to make clear how victims of stalkerware abuse can seek access to and/or deletion of their personal information, or other remedies, when they have not meaningfully consented to the collection of their personal information. Companies also routinely failed to fully account for the broader scope of personal information that is captured when operating the software (i.e., information from non-consenting or unsuspecting third parties with whom the targeted person communicates—such as their friends, family, coworkers, or other support systems—whose data is also exfiltrated by the app and disclosed to the app operator, or perpetrator of abuse). Significantly, companies overwhelmingly failed to adopt policies to notify persons targeted by their apps to facilitate intimate partner violence, harassment, or abuse—or to notify their own customers—in the event of a data breach. Overall, research findings revealed that the policies failed to recognize how apps with spyware capabilities can be used for harmful purposes and, by extension, failed to adequately account for the privacy rights of targeted persons of stalkerware that are (to varying degrees) enshrined in federal and provincial laws.

74. We **recommend** that the Ontario government clarify and reaffirm obligations in law that encourage meaningful implementation of data access and deletion policies for all Ontario residents, and notably for individuals subjected to child or employee surveillance apps or other forms of spyware that can be repurposed as stalkerware. Special attention should be given to enacting laws that require such companies to explicitly provide and communicate remedy processes and avenues of recourse to assist victims of illicit surveillance that is used to facilitate intimate partner abuse, violence, and harassment. (**Recommendation 14**)

F. Require Mandatory Breach Notifications from Stalkerware Companies

75. Both stalkerware apps and apps ostensibly designed for child and employee monitoring, and their supporting technical infrastructures, are routinely shown to have significant security vulnerabilities, where highly sensitive personal information is stored or transmitted with insufficient safeguards in violation of PIPEDA's requirement to protect personal information under their custody or control. Technical security analyses conducted by the Citizen Lab and researchers at Deakin University in Australia on such products and services (stalkerware and apps which can often be used as stalkerware) documented numerous vulnerabilities that further accentuate the privacy risks for those targeted by illicit surveillance.[37] Mandatory breach notification is thus particularly important where such apps are concerned, given the highly sensitive information that they collect and store.

76. Additionally, these kinds of companies have been the subject of a number of major data breaches in recent years[38] and, moreover, are often specifically targeted by hackers on the basis that they directly or indirectly encourage intimate partner surveillance and similarly abusive activities. FlexiSPY experienced a data breach that released "email addresses of customers, internal company files, a number of emails, and alleged partial credit card information" to a hacker in 2017;[39] Retina-X (responsible for MobileSpy, PhoneSheriff, and SniperSpy) was hacked in 2016, releasing "customer account logins, alleged GPS locations of surveillance victims, and photos and communications ripped from devices by the malware";[40] and in 2019, Mobiispy "left more than 95,000 images and more than 25,000 audio recordings on a database exposed and publicly accessible to anyone on the internet."[41]

77. On a certain level, it is challenging to meaningfully speak of stalkerware companies' obligations to protect data from unauthorized access when the products these companies are selling constitute a form of malware against which such safeguards are typically intended to protect against. However, for

---

37 See Adam Molnar and Diarmaid Harkin, "The Consumer Spyware Industry: An Australian-based analysis of the threats of consumer spyware," Australian Consumer Communications Action Network Report (August 2019), at 23-28 <http://accan.org.au/files/Grants/2017%20successful%20projects/Deakin%20-%20Consumer%20Spyware%20Industry%20%20-%2030Jul19%20WEB.pdf> and Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo & Ronald Deibert, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry" (June 2019), The Citizen Lab, at 46-54 ("2.2.4 Vulnerabilities in Stalkerware Update Processes") <https://citizenlab.ca/docs/stalkerware-holistic.pdf>.

38 See e.g., Zack Whittaker, "A 'Stalkerware app' leaked phone data from thousands of victims," TechCruch (20 February 2020) <https://techcrunch.com/2020/02/20/kidsguard-spyware-app-phones/.; Joseph Cox, "Hacker Strikes 'Stalkerware' Companies, Stealing Alleged Texts and GPS Locations of Customers," Vice News (22 February 2018) <https://www.vice.com/en_us/article/7x77ex/hacker-strikes-stalkerware-companies-stealing-alleged-texts-and-gps-locations-of-customers>

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

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

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

companies selling so-called 'dual-use' applications that can have ostensibly legitimate or lawful purposes (e.g., child or employee monitoring), they should be forcefully required to adhere to data protection safeguards to protect collected data from unauthorized access by yet more third or fourth parties. It is worth noting, however, that companies which design and sell apps with covert surveillance capabilities may be subjected to criminal prosecution for the kinds of activities they facilitate (i.e., interception of private communications), regardless of their level of compliance with specific privacy law obligations.

78. For ostensibly legitimate app vendors, whose products can be repurposed into stalkerware, as well as for vendors selling software intentionally designed to facilitate intimate partner surveillance, we **recommend** that their safeguard obligations include mandatory notification to impacted individuals whenever there has been a data breach. The app vendor must expressly and directly notify all individuals who were being tracked and monitored prior to and at the time of the breach. Notifying the "user" of the app, when interpreted to exclusively encompass the purchaser or perpetrator of the app-driven surveillance, would not suffice to meet this obligation. Should spyware or stalkerware companies fail to engage in reasonable efforts to notify all affected individuals of data breaches, they should be subjected to significant administrative monetary penalties, at a minimum. (**Recommendation 15**)

3. Focused Privacy Reform: Data Exploitation by Foreign Platforms

A. Foreign Company Surveillance and Repurposing of Canadian Users' Chat Data

79. In a May 2020 report,[42] "We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus," the Citizen Lab used technical experiments to reveal that WeChat communications conducted entirely among non-Chinese accounts—such as between residents of Ontario—are subject to pervasive political surveillance that was previously thought to be exclusively reserved for Chinese accounts. WeChat is a communications platform that is incredibly popular in China, and which is used by Chinese citizens who travel abroad, as well as by non-Chinese citizens to communicate with one another and with Chinese citizens. The Citizen Lab's research found that documents and images which were transmitted entirely among non-Chinese accounts undergo content analysis wherein these files are analyzed for content that is politically sensitive in China. Moreover, upon analysis, any files deemed politically sensitive from these accounts are then used to train and build up WeChat's Chinese political censorship system, which is then applied to Chinese accounts.[43]

---

[42] Jeffrey Knockel, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, & Ron Deibert, "We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus" (May 2020), The Citizen Lab, at <https://tspace.library.utoronto.ca/bitstream/1807/101395/1/Report%23127—wechattheywatch-web.pdf>.

[43] These findings were notable because communications surveillance is generally difficult to measure. In our case, we were able to measure it because of its immediately measurable effects on WeChat's ability to censor images and documents sent to Chinese users. However, when its results may not be immediately measurable, communications surveillance is difficult to impossible to measure. For instance, our methods were unable to test

80. To confirm the findings of our technical research and to additionally determine whether non-Chinese WeChat users' chat *texts* (as opposed to documents and images alone) were under surveillance, we analyzed the terms of service and privacy policy documents provided to Canadian users. Additionally, we made PIPEDA-based data access requests to WeChat's operator, Tencent. However, we found that there was no indication in WeChat's terms of service or privacy policy documents that non-Chinese users' communications were being used to more efficiently politically censor Chinese users. Moreover, our PIPEDA-based data access requests failed to even confirm the existence of the political content surveillance that we had already discovered. Our initial requests received generic responses that did not answer specific questions we posed regarding political consent surveillance, and follow-up requests received no response.

81. We bring up the research we conducted into WeChat's business practices to draw stark attention to the existing limitations of federal commercial privacy legislation—legislation which currently governs in Ontario. One of the objectives of PIPEDA is to enable users to understand how their personal information is being used by companies. In order to choose which Internet platforms to use, users must have the capability to learn how their personal information is being used by each Internet platform. For instance, users, upon understanding that an Internet platform is using the content of their communications to enable the political censorship of another demographic of people, may choose to stop using that Internet platform. From an informed consent perspective, it should not require substantive and long-term technical research to establish the existence of systematic surveillance of users' chat contents by a digital platform company, let alone discovering the existence of new surveillance and a new use of their chat data. However, it was only through such laborious and specialized research that we learned of those surveillance and censorship training systems; such information was not contained in either WeChat's or Tencent's terms of service or privacy policies provided to users outside of China (including those living in Ontario), or provided through making PIPEDA-based data access requests.

82. In light of the above, we **recommend** that the Ontario government grant powers to the IPC which allow it to levy AMPs in cases of user data being used improperly. For example, an AMP should be issued if Ontario residents' personal information is used for purposes not made clear in a digital platforms' publicly available terms of service and privacy policies. Where organizations refuse to respond to, or comply with, a data access request the IPC should similarly be empowered to levy AMPs. (**Recommendation 16**)

83. We further **recommend** that the government establish legislation that is more extensive than PIPEDA, with respect to data access rights. Such legislation should compel both Ontarian and non-Ontarian organizations to disclose to individuals, upon request, information concerning both the specific and actual primary and secondary uses of their personal data, as well as copies of the personal data that the organization in question has collected, processed, retained, or disclosed to third parties. The focus on secondary uses would ensure that Ontarian residents have the opportunity to understand how their information may be used or repurposed—even in an anonymized or pseudonymized format—to

whether the texts of chat messages (as opposed to documents and images) sent among non-Chinese users were similarly analyzed for political sensitivity or whether they were similarly used to improve censorship of Chinese users.

engage in business operations (e.g., aggregate statistics of how a given product or service is used) as well as more contentious activities (e.g., using Ontario residents' personal information, including private communications data, to facilitate censorship practices by repressive governments in other countries). (**Recommendation 17**)

4. Focused Privacy Reform: Algorithmic Policing Technologies

84. Algorithmic policing technologies include a wide range of algorithm-driven or artificial intelligence-driven technologies that are used in the course of carrying out policing and law enforcement functions. They may be divided into two broad categories. The first is what is generally known as 'predictive policing' technology, which includes (a) location-focused predictive policing tools, which algorithmically process historical police data to purportedly predict when and where crime will next occur, before it occurs; and (b) person-focused predictive policing tools, which rely on algorithmic data analysis in an attempt to identify people who are allegedly more likely to be involved in potential criminal activity or to assess an identified person for their purported risk of engaging in criminal activity in the future. The second broad category is algorithmic surveillance technologies, which include facial recognition technology, automated license plate readers, social media surveillance, and social network analysis. These kinds of technologies do not necessarily include a predictive component, but are used for general monitoring and surveillance on a level far beyond traditional policing methods.

85. Algorithmic policing technologies—whether predictive policing software or algorithmic surveillance tools—raise complex questions for both constitutional and private sector privacy law that Canadian legislation and jurisprudence have yet to address directly. This deficit must be addressed with urgency in light of the rise of algorithmic policing technologies used, under development, or being considered by law enforcement agencies at the municipal, provincial, and federal levels across Canada.[44] Commercial vendors of such technologies play a major role in Canadian law enforcement, particularly in circumstances where agencies purchase algorithmic policing tools as opposed to developing them in-house. Research undertaken by the Citizen Lab and the University of Toronto's International Human Rights Program has principally focused on the constitutional and human rights law implications in the context of criminal justice.[45] However, over the course of our research, several significant issues concerning algorithmic policing technology vendors and private sector privacy law

[44] See e.g., Miles Kenyon, "Algorithmic Policing in Canada Explained" (1 September 2020), Citizen Lab <https://citizenlab.ca/2020/09/algorithmic-policing-in-canada-explained/>; and Caroline Haskins, "Dozens of Cities Have Secretly Experimented With Predictive Policing Software," *Vice Motherboard* (6 February 2019) <https://www.vice.com/en_us/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software>.

[45] Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto <https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>.

became apparent. The Citizen Lab flags those issues here for the Ontario government's further consideration and investigation.[46]

86. Algorithmic policing technologies implicate the right to data privacy during the collection of data, use (or processing) of data, and disclosure of data (or data sharing). Data accuracy is an additional key issue of concern where algorithmic decision-making is involved, and one that runs throughout the collection, use, and disclosure stages. Algorithmic policing technologies pose particular problems for data protection law and the right to privacy, for at least two reasons in particular. First, such tools' advanced technological capabilities enable an unprecedented degree of invasive and far-reaching data collection as compared to traditional policing methods and non-algorithmic policing technologies. Second, algorithmic policing technologies introduce a high risk of algorithmic discrimination as a result of relying on biased data that is derived from practices reflecting systemic discrimination against particular groups by the Canadian criminal justice system. These groups include, in particular, Black and Indigenous individuals and communities; the LGBTQ+ community; those who live with mental illnesses or disability; and those who live in poverty, rely on social welfare, or are unhoused.

87. Today, police services in Canada have access to unprecedented and ever-growing amounts of data. The state's surveillance infrastructure and law enforcement's big data ecosystem form the backdrop of, and fuel for, algorithmic policing technologies. In Ontario alone, the Toronto Police Service (TPS) has collaborated with the data broker and data analytics company Environics Analytics since 2016, to engage in "data-driven policing", and has expressed interest in potentially adopting certain forms of 'predictive policing' in the future.[47] The TPS has also used facial recognition technology for more than a year without public notice; it was only following media reports that brought the program to public attention in 2019 that the public was made aware that these technologies were being used.[48] Also in 2019, the Ottawa Police Service (OPS) conducted a three-month pilot program with the facial recognition technology NeoFace Reveal. Both the TPS, OPS, and numerous other police services throughout Ontario admitted to informally using or testing the controversial facial recognition product Clearview AI, only after the *New York Times* revealed the connection.[49] In addition, the TPS, OPS, and RCMP have all engaged, or are engaging, in algorithmic social media surveillance, using products and services procured from commercial vendors.

---

46 We note that this submission to the MGCS is written entirely by members and affiliates of the Citizen Lab; assertions and positions provided in this submission may not wholly reflect those of the International Human Rights Program and, as such, should not be attributed to them unless they have explicitly indicated so elsewhere.

47 *Ibid*, at page 45.

48 Kate Allen & Wendy Gillis, "Toronto police have been using facial recognition technology for more than a year", *Toronto Star* (28 May 2019), <https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html>.

49 "Toronto police admit using secretive facial recognition technology Clearview AI", *CBC News* (13 February 2020) <https://www.cbc.ca/news/canada/toronto/toronto-police-clearview-ai-1.5462785>; Kelly Bennett, "Hamilton police tested controversial facial recognition technology Clearview AI", *CBC News* (20 February 2020), <https://www.cbc.ca/news/canada/hamilton/the-service-says-it-has-not-used-the-tool-for-anyinvestigative-purposes-1.5470359>; Shaamini Yogaretnam, "Ottawa police piloted controversial facial recognition software last year", *Ottawa Citizen* (13 February 2020), <https://ottawacitizen.com/news/local-news/ottawa-police-piloted-controversial-facial-recognition-software-lastyear>.

88. Much of the data that are collected and processed through algorithmic policing results are made possible by way of surveillance technologies that are sold by commercial vendors, and which may remain involved in updating, running, or otherwise facilitating the surveillance even after selling the technology. As a result, these vendors can sometimes maintain at least some custody or control over collected data. Law enforcement actors may have access to smart city data, social media data, mobile device information (including location) obtained remotely, and private sector consumer data (such as surveillance cameras built into "smart home" devices), in addition to personal information collected through facial recognition technology, automated license plate readers, social network analysis, and social media surveillance tools—all commercial technologies sold by private sector entities. The AI Now Institute has stated:

> AI raises the stakes in three areas: automation, scale of analysis, and predictive capacity. Specifically, AI systems allow automation of surveillance capabilities far beyond the limits of human review and hand-coded analytics. ... These systems also exponentially scale analysis and tracking across large quantities of data, attempting to make connections and inferences that would have been difficult or impossible before their introduction. Finally, they provide new predictive capabilities to make determinations about individual character and risk profiles, raising the possibility of granular population controls.[50]

89. Current Canadian privacy and data protection laws may no longer suffice to safeguard the right to privacy, in the face of algorithmic policing technologies' formidable reach and capabilities. Above all, we are concerned with the potential of algorithmic policing technologies, where obtained from, managed by, or operated in conjunction with commercial vendors, to result in uses by law enforcement that circumvent or undermine constitutional protections against unreasonable search and seizure under section 8 of the *Canadian Charter of Rights and Freedoms*. We urge the MGCS to consider carefully the interactions between what commercial algorithmic policing technology vendors may be permitted to do with personal information under Ontario privacy law, particularly without consent, and the corresponding constitutional privacy implications for law enforcement authorities' access to personal information through their use of such technologies.

90. The remainder of this section will raise three specific issues and recommendations for consideration, with respect to algorithmic policing technology vendors and their current obligations under PIPEDA (to the extent that their activities are not governed by constitutional or public sector privacy law as a result of their use by law enforcement).

A. Algorithmic Policing Technology Requires Reevaluation of Consent Exceptions

91. PIPEDA allows for the collection, use, and disclosure of personal information without consent under certain circumstances that involve law enforcement purposes. Such circumstances include if consent would compromise the information and collection relates to investigating a contravention of Canadian law; if the organization has reasonable grounds to believe that the personal information could assist an investigation of illegal activity "that has been, is being or is about to be committed"; if the disclosure is made to a requesting government institution with lawful authority to obtain the

[50] AI Now Institute, AI Now Report 2018 (December 2018) at 12 <https://ainowinstitute.org/AI_Now_2018_Report.pdf>.

information, for enforcing, investigating for enforcement purposes, or gathering intelligence to enforce a law; or if the disclosure is reasonable for investigating illegal activity that "has been, is being or is about to be committed" and consent would reasonably be expected to compromise the investigation.[51]

92. Without careful narrowing and clarification, there is the risk that these provisions may be interpreted in a way that exempts algorithmic policing technology vendors from the obligation to obtain consent before collecting, using, or disclosing data to law enforcement agencies without consent, to a degree that was not contemplated when the legislation was drafted and which would now violate the spirit and purpose of the law. Some of the above-mentioned consent exemptions are additionally concerning given the reference to investigating a contravention of law that is "*about to be* committed" (emphasis added). This raises the spectre of self-styled 'predictive policing' software vendors claiming that they are covered by the exemption by nature of what their technology purports to do—predict criminal activity that is "about to" occur, regardless of their software's reliability or accuracy and whether or not any such activity does occur.

93. The exponential reach associated with the scale, inferential intimacy, and potential invasiveness of algorithmic and big data policing methods raises the urgent question of whether these exemptions still appropriately maintain a balance between the right to privacy and the objectives that these exemptions are meant to achieve. Algorithmic surveillance technologies in particular, such as facial recognition software and social media surveillance, pose formidable threats to the right to privacy. In the case of facial recognition, as an example, such technology threatens to "end [the] ability to walk down the street anonymously".[52] In the case of social media surveillance, such technology enables systematic transformation and repurposing of personal information for law enforcement purposes, without knowledge or consent by users, including personal information concerning individuals' intimate lives, personal relationships, habits, interests, values, and everyday thoughts and activities.[53]

---

[51] Section 7(1)(b) of PIPEDA allows for the collection of personal information without consent if obtaining consent "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". Section 7(2)(a) permits use without consent if "in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention". Section 7(3)(c.1)(ii) allows disclosure without consent to a requesting government institution with lawful authority, if "the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law". Section 7(3)(d.1) permits disclosure without consent to "another organization" if the disclosure is "reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation".

[52] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *New York Times* (18 January 2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

[53] Moreover, there are an increasing number of private companies whose entire business model is mass collection of personal information for the specific purpose of selling access to that information to law enforcement, such as the facial recognition tool by Clearview AI. The company remains directly involved with the collection, use (processing), and disclosure of information ongoingly, far beyond the point of sale, and thus may still be governed by private sector data protection law where police usage does not trigger governance by public sector privacy law instead.

94. The federal privacy commissioner and the courts have recognized some limits on the consent exemptions cited above, and the Ontario government should ensure such limits clearly apply to algorithmic and predictive policing technology vendors under provincial privacy law. For example, the Office of the Privacy Commissioner of Canada has asserted that to rely on section 7(1)(b) (collection without consent), "an organization must have substantial evidence to support the suspicion that the [individual] is engaged in wrongdoing", among other requirements, and moreover stated that "anecdotes do not qualify as substantial evidence", which may be a salient principle in the context of social media surveillance.[54]

95. Regarding the section 7(3)(c.1)(ii) exemption from consent for disclosure to a government institution, the Supreme Court of Canada established in *R. v. Spencer* that reliance on this provision is subjected to the individual's constitutionally protected reasonable expectation of privacy under the *Charter* (which determines if the requesting institution, in this case law enforcement, has lawful authority to obtain the disclosure without consent in the first place).[55] The OPC has also noted that "where requests for disclosure of personal information were concerned, [it is] incumbent upon any private-sector organization not to take the submissions of any government organization at face value, but rather to be vigilant about checking authorities cited."[56]

96. Lastly, in a guidance document regarding section 7(3)(d.1) (disclosure without consent to another organization for investigative purposes), the OPC has warned that the "invisible nature of these disclosures" undermines transparency and accountability, and emphasizes that such exemptions:

    - *Are not* to be applied in an overly broad manner.
    - *Do not allow* for widespread disclosures and casual sharing of personal information.
    - *Are limited* to certain purposes, under defined circumstances, and given specific conditions.[57]

    The OPC document sets out further detailed interpretation guidance and measures that organizations must undertake to ensure due diligence, accountability, and that disclosure of personal information under this exemption is responsible, reasonable, and proportionate, given the stated purpose.

97. The OPC's guidance is limited, however, on the basis that it applies to disclosures to other private organizations, as opposed to disclosures to government institutions such as law enforcement. The Ontario government should implement and enforce similar principles and measures where the latter is concerned. For example, the provincial law should ensure that the investigation or law enforcement

---

54 Office of the Privacy Commissioner of Canada, "Electronic monitoring does not yield any information, but practice is strongly discouraged", PIPEDA Case Summary #2004-268 (16 June 2004) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-268/>.

55 *R v Spencer*, 2014 SCC 43, at para 62.

56 Office of the Privacy Commissioner of Canada, "Airline accused of improper disclosure of travel information to government department", PIPEDA Case Summary #2002-62 (22 July 2002) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2002/pipeda-2002-062/>

57 "Applying paragraphs 7(3)(d.1) and 7(3)(d.2) of PIPEDA", Office of the Privacy Commissioner of Canada (March 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/gd_d1-d2_201703/> (emphasis in original).

activity for which disclosure is sought "pertains to a specific breach of a law or agreement" in all cases, rather than a vaguely forecasted potential future breach of an unspecified law, as may be the case with some predictive policing or algorithmic risk assessment programs.

98. In light of the above, we **recommend** that the Ontario government implement privacy legislation that incorporates the best practices from the OPC's guidance document regarding PIPEDA section 7(3)(d.1) in the context of disclosing personal information without consent to law enforcement authorities. (**Recommendation 18**)

99. We further **recommend** that in enacting new legislation, the Ontario government consult with a range of independent legal, criminal justice, human rights, and racial justice experts, including members of Black and Indigenous communities, to evaluate whether or not current exceptions that permit collection, use, or disclosure of personal information without consent, for law enforcement purposes, are proportionate and necessary in view of the advanced capabilities of algorithmic policing technologies. (**Recommendation 19**)

B. Privacy Law Must Protect Social Media Activity from Algorithmic Surveillance

100. PIPEDA allows for collecting, using, and disclosing personal information without consent if "the information is publicly available and is specified by the regulations", in sections 7(1)(d), 7(2)(c.1), and 7(3)(h.1), respectively. As defined in the *Regulations Specifying Publicly Available Information*, "publicly available" information includes "personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information."[58] This definition may be interpreted to authorize private organizations to either capture the social media activity of specific individuals or conduct dragnet surveillance on social media users on a mass scale. Both these forms of surveillance pose a grave threat to the rights to privacy, equality, and freedom of expression in the context of algorithmic policing technology.

101. Professor Teresa Scassa has pointed out the dangers of interpreting the provisions described above to mean that all public social media data is exempt from consent obligations. Specifically, and in reference to a report by the Standing Committee on Access to Information, Privacy, and Ethics ("ETHI") concerning reforms to PIPEDA, she has stated:

> The scope of ETHI's proposed change [to exempt use, collection, and disclosure of social media data from consent obligations] is particularly disturbing given the very carefully constrained exceptions that currently exist for publicly available information. A review of the Regulations should tell any reader that this was always intended to be a very narrow exception with tightly drawn boundaries; it was never meant to create a free-for-all open season on the personal information of Canadians.
>
> The Cambridge Analytica scandal reveals the harms that can flow from unrestrained access to the sensitive and wide-ranging types and volumes of personal information that are found on social media sites. Yet even as that scandal unfolds, it is important to note that everyone

[58] *Regulations Specifying Publicly Available Information*, SOR/2001-7, s 1(e).

> (including Facebook) seems to agree that user consent was both required and abused. What ETHI recommends is an exception that would obviate the need for consent to the collection, use and disclosure of the personal information of Canadians shared on social media platforms. This could not be more unwelcome and inappropriate.[59]

102. We agree. A social media consent exemption would be even more alarming and untenable in the context of algorithmic social media surveillance software used by police services, where criminal jeopardy is at stake, including potential state interference with individuals' liberty and equality rights and their fundamental freedoms, in addition to their right to privacy. ETHI's position as described in paragraph 97—which is shared by the Royal Canadian Mounted Police (RCMP)[60]—oversimplifies the privacy interests at stake. When individuals use social media they do not expect to have their information systematically collected by third-party private companies for the purpose of passing that information to law enforcement and, for instance, algorithmically processing their social media content to assess their purported risk level for future involvement in certain kinds of activity that the state considers to be criminal. Moreover, social media surveillance tools do not simply collect discrete pieces of data as one-off requests, but instead tend to be designed to systematically and ongoingly collect social media data over time and analyze it to generate ever more revealing and intimate portraits of surveilled individuals and populations.

103. Exempting personal information that is collected through social media activity from consent obligations is also problematic when examining the roles that public protest and social media—which can be instrumental in organizing such demonstrations—have played in facilitating historically oppressed groups' freedom of expression, combined with the knowledge that such groups have already been repeatedly targeted by law enforcement as a result of advocating for their equality rights and civil liberties.[61] In at least one known case, such targeted social media surveillance was assisted and encouraged by a commercial vendor based in London, Ontario: the company, Media Sonar, marketed itself to law enforcement agencies in the United States as a way to monitor hashtags related

---

[59] Teresa Scassa, "Open Season on Social Media Data (ETHI's Report on PIPEDA Reform - Part II)" (22 March 2018) <https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=273>.

[60] Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto, at page 77 <https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>

[61] See e.g., Stephen Davis, "Police monitored Black Lives Matter Toronto protesters in 2016, documents show", *CBC News* (3 May 2018) <https://www.cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628>; Hillary Beaumont, "Canadian police spied on Indigenous protesters on Parliament Hill", *VICE* (10 November 2017) <https://news.vice.com/en_ca/article/a3jjxa/canadian-police-spied-on-indigenous-protesters-on-parliament-hill>; Hillary Beaumont, "Canada's spy agency has been watching Standing Rock and thinks it has Canadian implications", *VICE* (15 March 2017) <https://news.vice.com/en_ca/article/evaw3w/canadas-spy-agency-has-been-watching-standing-rock-and-thinks-it-has-canadian-implications>. In 2014, the RCMP established Project SITKA to collect information about prominent Indigenous activists and assess their levels of "threat" (assessed as a likelihood that the individual has committed or will likely commit criminal activity): Sean Craig, "RCMP tracked 89 indigenous activists considered 'threats' for participating in protests", *The National Post* (13 November 2016) <https://nationalpost.com/news/canada/rcmp-tracked-89-indigenous-activists-considered-threats-for-participating-in-protests>.

to social movements protesting police brutality, including #BlackLivesMatter.[62] In theory, the same surveillance practices could easily be applied to protests or demonstrations on other issues, such as taxation or government corruption. Social media surveillance tools are a threat to legitimate political protest and public demonstrations of dissent, regardless of the issue being protested. This kind of activity should not be permitted or encouraged under contemporary privacy law that takes the expanded capabilities of algorithmic policing technologies into account, in Ontario or elsewhere.

104. For the reasons above, we **recommend** that the Ontario government, in enacting new legislation, re-evaluate current PIPEDA exceptions that permit collection, use, or disclosure of personal information from public spaces or public sources, including social media and public demonstrations and protests. Any new Ontarian privacy legislation must ensure that any such exemptions are proportionate and necessary, in view of the advanced capabilities of algorithmic surveillance technologies, and relative to human rights at stake such as the right to liberty, equality, and freedom of expression, in addition to the right to privacy. (**Recommendation 20**)

C. Provide GDPR-Level Due Process Rights in Automated Decision-Making

105. Articles 13 and 14 of the GDPR state that whenever an individual's personal data is obtained, and to "ensure fair and transparent processing in respect of the data subject [i.e., the individual concerned]", that individual is entitled to be informed of "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[63] Such a right should also be included in any forthcoming Ontario privacy legislation, given the rise of algorithmic policing technologies and other forms of automated decision-making throughout the country, as well as the need for Ontarian law to be best situated to be deemed adequate under the EU's assessment of provincial privacy law.

106. The joint research conducted by the Citizen Lab and the University of Toronto's International Human Rights Program into algorithmic policing technologies revealed a wide range of due process concerns, including the overarching issue of algorithmic transparency and the right of impacted individuals to make full answer and defence in the context of criminal proceedings where an algorithmic forecast or algorithmic risk assessment tool played a role in a decision concerning that individual. Commercial vendors who provide such technologies in a way where they are ongoingly involved in the collection, use or processing, and/or disclosure of data to law enforcement should be required to inform individuals, upon request, of the existence and details of any algorithmic or automated decision-making or profiling as mandated in Articles 13(2)(f) and 14(2)(g) of the GDPR, as a part of their data accuracy and data access obligations.

---

[62] Andrew Margison, "Twitter and Instagram ban London, Ont., company for helping police track protesters", *CBC News* (19 January 2017) <https://www.cbc.ca/news/canada/toronto/twitter-bans-firm-police-protesters-1.3942093>; and ACLU Northern California, "This Surveillance Software is Probably Spying on #BlackLivesMatter" (15 December 2015) <https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter>.

[63] Articles 13(2)(f) and 14(2)(g), General Data Protection Regulation (GDPR) (EU) 2016/679 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>.

107. Beyond technology vendors, the Ontario government must also adhere to its own transparency obligations where such technologies are used for criminal justice purposes. This obligation takes the form of a defendant's right to procedural fairness, due process, Crown disclosure, and the ability to make full answer and defence, where they are charged with a crime on the basis of evidence obtained through one or more types of algorithmic policing technologies.

108. In light of the above, we **recommend** that the Ontario government enact law with contents similar to Articles 13, 14, and 22 of the GDPR, which provides a level of transparency to individuals with respect to how their data is processed, where algorithmic or automated decision-making is involved. Transparency obligations concerning automated decision-making that affects an individual's legal or similarly significant interests should apply to both commercial vendors and the government itself, particularly in the context of algorithmic policing technologies. (**Recommendation 21**)

109. To reiterate, the points raised in this section of our submission, regarding algorithmic policing specifically, are neither exhaustive nor comprehensively explored here or in our report on algorithmic policing technologies. They are issues that emerged in the course of the research and analysis conducted by the Citizen Lab and the University of Toronto's International Human Rights Program (IHRP), and which we—members and affiliates of the Citizen Lab, without presuming to speak for IHRP—considered warranted flagging for the MGCS's attention and further investigation. The relevant provincial ministries and the Ontario IPC should work with the federal privacy commissioner, other provincial / territorial privacy commissioners, and relevant federal and provincial /territorial ministries and agencies, in a coordinated effort to establish robust oversight and accountability measures to protect the privacy rights of those subjected to algorithmic policing technologies. This may involve working with municipal, provincial, and federal law enforcement agencies and implementing or strengthening requirements such as Privacy Impact Assessments, as part of more comprehensive Algorithmic Impact Assessments, for any law enforcement agency considering using a given algorithmic policing technology.

Conclusion

110. Ontarians are increasingly concerned about their privacy, and in how private organizations collect, retain, process, and disclose their personal information. Unfortunately, successive federal governments have failed to table, and pass, meaningfully and comprehensive privacy reform over the past decade. The Ontario government now has the opportunity to assess what it can do to better protect the interests of its residents, while simultaneously enabling organizations in Ontario to better understand how best to protect the information that is in their custody.

111. We appreciate the efforts that are being undertaken through the Ministry of Government and Consumer Services consultation process, and the attention being paid to pressing privacy and data protection issues. The Citizen Lab looks forward to seeing the consultation unfold, and would be pleased to discuss our recommendations in more depth as the consultation progresses, at the Ministry's convenience.

Signed (alphabetical order):

Lex Gill, Lawyer at Trudel Johnston & Lespérance in Montreal and a Citizen Lab Research Fellow

Cynthia Khoo, Research Fellow at the Citizen Lab and technology and human rights lawyer

Jeffrey Knockel, Research Associate at the Citizen Lab

Adam Molnar, Assistant Professor of Sociology and Legal Studies at the University of Waterloo and a member of the Waterloo Cybersecurity and Privacy Institute

Christopher Parsons, Senior Research Associate at the Citizen Lab

Kate Robertson, Criminal Defence Lawyer at Markson Law in Toronto and a Citizen Lab Research Fellow

Primary Contact:

Cynthia Khoo <cynthia@citizenlab.ca>

Appendix I: List of Recommendations

1. Overarching Principles to Guide Privacy Reform in Ontario

Recommendation 1: The government should adopt a principles-based approach to privacy legislation, in order to ensure that the law may more easily adapt to future technological advances while providing equivalent levels of privacy protection in Ontario regardless of the specific technical nature of such future technologies. This framework should be supplemented by charging the IPC with an educational mandate to help organizations to comply with their privacy law obligations, which may evolve alongside the world's evolving technological context. Any such framework should be backstopped by a strong enforcement regime to ensure effectiveness, such as providing the IPC with the ability to issue significant AMPs.

Recommendation 2: The government should ensure that there is consistency in how private organizations are expected to protect personal information in their care and that, to accomplish this, organizations be compelled to apply either the public or private sector regulations that would maximally protect the class(es) of personal information in question. Ensuring consistency may, in addition to reforming private sector privacy legislation, also entail updating or supplanting public sector legislation where private sector regulations are found to be more protective. Such reforms will ensure that the privacy protections that apply to private sector treatment of both private sector and public sector data both are more easily complied with and will provide Ontarians with the highest standard available of privacy protection.

Recommendation 3: Transparency reporting templates should be generated in consultation between government, industry, civil society, and academia.

Recommendation 4: Where information has been disclosed to government agencies, organizations should be required to notify individuals of such disclosures unless pressing public interest reasons militate against such notification. Organizations should additionally be compelled to publish annual reports that disclose the frequency of, and rationales for, any disclosures to government agencies, including law enforcement authorities.

Recommendation 5: In reforming its privacy laws, the province should require private organizations to specifically disclose the information that is being collected (i.e., stating precisely what particular information is in fact collected, as opposed to stating that particular information "may" be collected) and for what specific purpose, and with whom that information has been specifically disclosed to and under what terms.

Recommendation 6: The government of Ontario should include all private organizations—including businesses, charities, non-profit organizations, and political parties—in any new privacy or data protection legislation that emerges from its consultations. However, the law must exercise the utmost care to ensure any such regime applied to non-governmental or non-commercial organizations is contextually appropriate and proportionate to the particular purpose and activity of the regulated organization, especially where public interest activities and purposes are concerned.

Recommendation 7: The creation of any statutory remedy in Ontario in the nature of a "right to be forgotten" should ensure that all requests for removal or de-indexing be subject to rigorous constitutional scrutiny—including the principles of minimal impairment and proportionality—by an independent and impartial court or tribunal.

Recommendation 8: The government should carefully review the GDPR and ensure that any legislation that is passed to protect Ontario residents' personal information and privacy rights are compliant with the GDPR. Compliance with the GDPR will ensure that the legislation will be deemed adequate by the European Union, so as to provide both Ontarians and Europeans with a commensurate high level of data protection.

Recommendation 9: The government of Ontario should ensure that any proposed legislation facilitates a range of remedial avenues for complainants and litigants to seek recourse for breach of their privacy rights. Recourse should be available both on an individual basis and to those seeking systemic redress for unlawful practices that violate the collective privacy rights of a particular defined group or community. This should include robust investigation and enforcement powers provided to the Ontario IPC, sufficient to deter illegal conduct and to encourage the proactive adoption of best practices.

2. Focused Privacy Reform: Consumer Spyware and Stalkerware Apps

Recommendation 10: In enacting new privacy legislation, the Ontario government should make clear that the individual from whom consent is required, in all cases, is the individual whose personal information is being collected, used, or disclosed, whether or not they are termed the "user" or "customer" of a particular app. To comply with this requirement, companies' privacy policies must explicitly protect and apply to individuals whose data is being collected, used, or disclosed by their product or service—whether or not that individual is considered the official "user" or "customer"—regardless of app purchase, device ownership, or whether or not the individual is the one who paid for or is controlling the surveillance software in question.

Recommendation 11: The Ontario government should follow the reasoning of the Alberta IPC in *Re Engel Brubaker*, and include in any new privacy legislation explicit affirmation that companies that sell software which can be (re)purposed as stalkerware are subject to PIPEDA, to an equivalent set of obligations, or to any substantially similar legislation. The law must make clear that commercial organizations writ large cannot be exempt from PIPEDA, or from any substantially similar Ontario legislation, for reasons of being used for "personal or domestic purposes"—an exception meant to exclude private individuals, in their capacity of private individuals, alone.

Recommendation 12: Ontario privacy law should explicitly declare that spyware companies are not permitted to disclaim or offload their liability and obligations to individual customers (e.g., stalkerware operators) through terms of use or EULAs.

Recommendation 13: The Ontario government should apply a similar approach as PIPEDA applies for the safeguards requirement, to strengthen consent and notice requirements. Effective mechanisms should make it nearly impossible for a tracked, monitored, or recorded individual to remain unaware of what their device is doing. For mobile apps that allow tracking, monitoring, and surveillance of targeted individuals, provided there

is a legitimate or legal purpose, meeting the requirement for meaningful consent should necessitate building in technical features such as persistent notifications and just-in-time alerts.

Recommendation 14: The Ontario government should clarify and reaffirm obligations in law that encourage meaningful implementation of data access and deletion policies for all Ontario residents, and notably for individuals subjected to child or employee surveillance apps or other forms of spyware that can be repurposed as stalkerware. Special attention should be given to enacting laws that require such companies to explicitly provide and communicate remedy processes and avenues of recourse to assist victims of illicit surveillance that is used to facilitate intimate partner abuse, violence, and harassment.

Recommendation 15: Spyware and stalkerware apps vendors' safeguard obligations should include mandatory notification to impacted individuals whenever there has been a data breach. The app vendor must expressly and directly notify all individuals who were being tracked and monitored prior to and at the time of the breach. Notifying the "user" of the app, when interpreted to exclusively encompass the purchaser or perpetrator of the app-driven surveillance, would not suffice to meet this obligation. Should spyware or stalkerware companies fail to engage in reasonable efforts to notify all affected individuals of data breaches, they should be subjected to significant administrative monetary penalties, at a minimum.

3. Focused Privacy Reform: Data Exploitation by Foreign Platforms

Recommendation 16: The Ontario government should grant powers to the IPC which allow it to levy AMPs in cases of user data being used improperly. For example, an AMP should be issued if Ontario residents' personal information is used for purposes not made clear in a digital platforms' publicly available terms of service and privacy policies. Where organizations refuse to respond to, or comply with, a data access request the IPC should similarly be empowered to levy AMPs.

Recommendation 17: The government should establish legislation that is more extensive than PIPEDA, with respect to data access rights. Such legislation should compel both Ontarian and non-Ontarian organizations to disclose to individuals, upon request, information concerning both the specific and actual primary and secondary uses of their personal data, as well as copies of the personal data that the organization in question has collected, processed, retained, or disclosed to third parties. The focus on secondary uses would ensure that Ontarian residents have the opportunity to understand how their information may be used or repurposed—even in an anonymized or pseudonymized format—to engage in business operations (e.g., aggregate statistics of how a given product or service is used) as well as more contentious activities (e.g., using Ontario residents' personal information, including private communications data, to facilitate censorship practices by repressive governments in other countries).

4. Focused Privacy Reform: Algorithmic Policing Technologies

Recommendation 18: The Ontario government should implement privacy legislation that incorporates the best practices from the OPC's guidance document regarding PIPEDA section 7(3)(d.1) in the context of disclosing personal information without consent to law enforcement authorities.

Recommendation 19: In enacting new legislation, the Ontario government should consult with a range of independent legal, criminal justice, human rights, and racial justice experts, including members of Black and

Indigenous communities, to evaluate whether or not current exceptions that permit collection, use, or disclosure of personal information without consent, for law enforcement purposes, are proportionate and necessary in view of the advanced capabilities of algorithmic policing technologies.

Recommendation 20: The Ontario government, in enacting new legislation, should re-evaluate current PIPEDA exceptions that permit collection, use, or disclosure of personal information from public spaces or public sources, including social media and public demonstrations and protests. Any new Ontarian privacy legislation must ensure that any such exemptions are proportionate and necessary, in view of the advanced capabilities of algorithmic surveillance technologies, and relative to human rights at stake such as the right to liberty, equality, and freedom of expression, in addition to the right to privacy.

Recommendation 21: The Ontario government should enact law with contents similar to Articles 13, 14, and 22 of the GDPR, which provides a level of transparency to individuals with respect to how their data is processed, where algorithmic or automated decision-making is involved. Transparency obligations concerning automated decision-making that affects an individual's legal or similarly significant interests should apply to both commercial vendors and the government itself, particularly in the context of algorithmic policing technologies.