Brief in support of witness presentation at The House of Commons of Canada's Standing Committee on Industry and Technology on 5 February 2024 on Bill C-27

Ignacio Cofone

Introduction

Thank you for the invitation to share my thoughts on Bill C-27 with the Standing Committee on Industry and Technology. I was invited to participate in my personal capacity on 5 February 2024. I am the Canada Research Chair in Artificial Intelligence Law & Data Governance at McGill University, Faculty of Law, where I teach Privacy Law and AI Regulation. My work in privacy law and AI regulation has been published in books and law journals including the University of Toronto Law Journal, the Stanford Technology Law Review, and the Harvard Journal of Law & Technology. Among other work in the field, in 2020, I worked with the Office of the Privacy Commissioner of Canada to write its "Policy Proposals for PIPEDA Reform to Address AI" report, and last year I published a book with Cambridge University Press on legislative design for privacy under AI. This Brief provides support and further detail to my presentation.

AI promises to transform the Canadian economy and society during the next decade. It promises to improve Canadians' wellbeing, efficiency, and sustainability. It already affects people's daily lives in fields as critical as pandemic responses, healthcare, finance, housing, employment, and incarceration. It also contains significant risks of harm that are often hidden from popular view. It is crucial that Canada has a legal framework that fosters the enormous benefits of AI and data while preventing its population from becoming collateral damage. Canada needs a new legal framework for AI and privacy such as the one Bill C-27 proposes.

Conditional on maintaining the general characteristics and approach of Bill C-27 as proposed, I believe there are three important and interrelated opportunities for further improving it: one for AIDA, one for the CPPA, and one for both of them.

Recommendation 1: An improved definition of harms in AIDA

AIDA is an accountability framework.[1] And the effectiveness of any accountability framework depends on what it holds entities accountable for. Currently, AIDA recognizes

[1] Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Sess, 4th Parl, 2022, cl 39(4)(b) (second reading 24 April 2023) ("to prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests").

property, economic, physical, and psychological harms.[2] In recognizing psychological harm, AIDA takes an important step towards moving past outdated frameworks that focused only on physical and economic harms. But for it to be effective at preventing AI harms, the Act needs to go a step further.

Consider the harms to democracy that were imposed during the Cambridge Analytica scandal. Consider the meaningful, but diffuse and invisible, harms that are inflicted every day through intentional misinformation that polarizes voters and misrepresentation of minorities that disempowers them.[3] These go unrecognized by the current definition of harm.[4]

AIDA would significantly improve by recognizing intangible AI harms beyond individual psychological ones, which it can do with two minor changes. First, AIDA would significantly improve by recognizing harms to groups, such as harms to democracy, as AI harms often affect communities rather than individuals.[5] Second, it would significantly improve by recognizing dignitary harms, like those stemming from misrepresentation and the growing of systemic inequalities, which AI can inadvertently create.[6]

This fuller account of harms would put Canada up to international standards. For example, compare the language proposed here with the recently released text of the European Union AI Act, which already in its Recital 4 considers harm to public interests, to rights protected by European Union law, to a plurality of persons, and to people in a vulnerable position;[7] and later in the Act gives special consideration to impact on “a plurality of persons” and whether they are in a vulnerable position.

Moreover, this fuller account would increase the consistency within Canadian law, as the Directive on Automated Decision-Making, when defining impact assessment levels,

[2] *Ibid* cl 39(5)(1) (“harm means (a) physical or psychological harm to an individual; (b) damage to an individual’s property; or (c) economic loss to an individual. (*préjudice*)”).

[3] See e.g. Soroush Vosoughi, Deb Roy & Sinan Aral, “The Spread of True and False News Online” (2018) 359:6380 Science 1146; Nicholas Diakopoulos, *Automating the News: How Algorithms are Rewriting the Media* (Cambridge, MA: Harvard University Press, 2019); Ignacio Cofone, “Algorithmic Discrimination is an Information Problem” (2019) 70:6 Hastings LJ 1389 at 1404–1406.

[4] See Ben Delaney, “Bill C-27 and AI in Content Moderation: The Good, The Bad, and The Ugly” (3 January 2023), online: <mcgill.ca/business-law/article/bill-c-27-and-ai-content-moderation-good-bad-and-ugly>.

[5] See e.g. U.S. Department of Commerce & National Institute of Standards and Technology, *AI Risk Management Framework* (2023) at 1 online: <nist.gov/itl/ai-risk-management-framework> (“pose risks that can negatively impact individuals, groups, organizations, communities, society, the environment and the planet”); Teresa Scassa, “Explaining the AI and Data Act” (21 March 2023), online: <teresascassa.ca/index.php?option=com_k2&view=item&id=369:explaining-the-ai-and-data-act&Itemid=80>.

[6] See Kate Crawford, “The Trouble with Bias” (2017) Conference on Neural Information Processing Systems 2017 Keynote Address.

[7] See European Commission, *Proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act)*, 2021 (recital 4: “artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law. Such harm might be material or immaterial”).

repeatedly refers to “individuals or communities.” It would also better comply with AI ethics frameworks, such as the Montreal Declaration Responsible AI,[8] the Toronto Declaration,[9] and the Asilomar AI principles.[10]

For those reasons, I ask the committee, when doing clause by clause review, to consider incorporating these intangible harms to individuals and communities by amending Section 5(1) of AIDA to say: *“harm means: (a) tangible harm to an individual or community, such as physical harm, harm to property, or economic loss; (b) intangible harm to an individual or community, such as psychological or emotional; or (c) dignitary harm to an individual or community, such as through discrimination.”*

Recommendation 2: CPPA explicitly recognizing inferences as personal information

What people listen to on Spotify can be used to infer their ethnicity.[11] The type of coffee people order can be used to infer their political convictions.[12] Text messages can be used to infer people’s income bracket.[13] These are just some examples of the thousands of ways companies have significantly more information about people than the information collected from them.[14] Inferences exponentially increase the risk of harm because they collate seemingly inoffensive pieces of information into sensitive information to form individual profiles and group trends.[15]

Inferences are a type of information that can both harm people at an individual level and cause social harms because identifying patterns uncovers group insights, such as shared preferences and identifying features.[16] Risks posed by inferences are impossible to anticipate because the information inferred is disproportionate to the sum of the information disclosed.[17] It is impossible to know what piece of information will be the one that completes

[8] Consider its principle of responsibility paired with non-individual principles of solidarity, democratic participation, equity, and diversity and inclusion.

[9] It recognizes collective interests with language such as “protecting the rights of all individuals and groups” and highlights people’s right to an effective remedy.

[10] See its ninth principle on responsibility of designers and builders for all harms or discrimination caused by systems.

[11] Shantal R. Marshall & Laura P. Naumann, “What’s Your Favorite Music? Music Preferences Cue Racial Identity” (2018) 76 J Research in Personality 74 at 88.

[12] Daniel DellaPosta, Yongren Shi & Michael Macy, “Why Do Liberals Drink Lattes?” (2015) 120:5 Am J Sociology 1473 at 1474–1475.

[13] Yannick Leo et al, “Socioeconomic Correlations and Stratification in Social-Communication Networks” (2016) 13:125 J Royal Society Interface 1 at 2.

[14] Przemyslaw Palka, “Data Management Law for the 2020s: The Lost Origins and the New Needs” (2020) 68:2 Buffalo L Rev 559 at 564–566.

[15] Ignacio Cofone, *The Privacy Fallacy: Harm and Power in the Information Economy* (Cambridge, UK: Cambridge University Press, 2023) at 49–50 [*Privacy Fallacy*].

[16] *Ibid* at 47–48.

[17] Katherine J. Strandburg, “Free Fall: The Online Market’s Consumer Preference Disconnect” (2013) 2013 U Chicago Leg Forum 95 at 131.

an inferential sequence that leads to new information.[18] Inferences can even be harmful when incorrect, as the TransUnion class action in the United Stated showed, when the credit rating agency mistakenly inferred that hundreds of people were terrorists.[19]

By supercharging inferences, AI has transformed the privacy landscape.[20] Canada cannot afford to have a privacy statute that focuses on disclosed information because doing so builds a back door into privacy law that strips the law of its power to create meaningful protections in today's inferential economy. To protect Canadians in the coming decade, Canada needs a privacy statute that considers how, through inferred information, AI changes the privacy landscape.[21] Proposing the CPPA and AIDA together through Bill C-27 presents a unique opportunity because, while AI changed the privacy landscape, privacy law is one of the most effective tools to govern AI, as privacy law is the body of law that regulates the data that fuels it.

Enforcers across the world recognize the importance of inferences for privacy. In California, the Attorney General recognized the importance of inferences and ruled they are personal information for access requests.[22] European courts, similarly, include some inferences in these requests, such as comments on examinations.[23] Once one recognizes the importance of inferred information, it becomes apparent that there is no legal or conceptual reason to stop at access requests. The Office of the Privacy Commissioner has also argued that inferences are personal information for all purposes, as have international data protection authorities, such as those of Australia. Modern privacy laws also increasingly recognize inferences as personal information. Amendments to the California Consumer Privacy Act, for example, expand protections over inferred information.[24]

The CPPA, in its current language, does not rule out inferences being personal information, but it does not incorporate them explicitly either.[25] It must. The CPPA is ready to acknowledge the importance of inferences because, by having a legitimate business

[18] Ignacio Cofone & Adriana Robertson, "Consumer Privacy in a Behavioral World" (2018) 69:6 Hastings LJ 1471 at 1489–1490.

[19] See *TransUnion LLC v Ramirez*, 141 US 2190, 594 (2021).

[20] Cofone, *Privacy Fallacy, supra* note 15 at 5–7, 10.

[21] Ignacio Cofone, *Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report*, Office of the Privacy Commissioner of Canada (Ottawa: OPC, November 2020) at 2.c, online: <priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011> [*Policy Proposals*].

[22] Rob Bonta, *Opinion No. 20-303* (California: Office of the Attorney General, 2022) at 10; Jordan M. Blanke, "Protection for 'Inferences Drawn': A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act" (2020) 2 Global Privacy Law Review 81 at 90.

[23] *Peter Nowak v Data Protection Commissioner*, C-434/16, [2017] ECLI:EU:C:2017:994.

[24] *California Civil Code* § 1798.100 (a)(3), 1798.100 (c), 1798.105 (d)(2), 1798.140 (e), 1798.140 (e)(2); Jordan M. Blanke, "The CCPA, 'Inferences Drawn,' and Federal Preemption" (2023) 29:1 Richmond JL & Tech 53 at 67–73; Anupam Chandler, Margot Kaminski & William McGeveran, "Catalyzing Privacy Law" (2021) 105 Minnesota L Rev 1733 at 1752–1753.

[25] Bill C-27, *supra* note 1, cl 2(2)(1) ("personal information means information about an identifiable individual. (*renseignement personnel*)" / "renseignement personnel Tout renseignement concernant un individu identifiable. (*personal information*)").

interest provision, it could incorporate inferences into its framework without unrealistic expectations that each of them will be explicitly consented to.[26]

For those reasons, I ask the committee, when doing clause by clause review, to consider amending the definition of personal information in Section 2(1) of the Act to say "*personal information means disclosed or inferred information about an identifiable individual or group* (*renseignement personnel*)."

Recommendation 3: mixed enforcement

The third recommendation follows from the first two. Enforcement is necessary for any privacy or data protection legislation to be effective.[27] But authorities face challenges in enforcing laws that cover thousands of activities by private actors, many of them by tech giants who hold significant power.[28] The European Union has been successful at converging public and private enforcement to the benefit of individuals by having neither of them depend on the other.[29]

Both public and private enforcement mechanisms are needed in practice to overcome the enforcement challenges that exist in data and AI.[30] Private rights of action alleviate regulatory burden on administrative agencies, reduce the risk of agency capture, and pressure companies to comply with the law.[31] Lawsuits can become a significant deterrent to breach in addition to public enforcement.[32]

[26] See *ibid*, cl 2(18)(3) ("[a]n organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and (a) a reasonable person would expect the collection or use for such an activity; and (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.").

[27] Marc Rotenberg & David Jacobs, "Enforcing Privacy Rights: Class Action Litigation and the Challenge of Cy Pres" in David Wright & Paul De Hert, eds, *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Switzerland: Springer, 2017) at 307; Janet Walker, "Douez v Facebook and Privacy Class Actions" in Ignacio Cofone, ed, *Class Actions in Privacy Law* (London: Routledge, 2020) at 67–72.

[28] Jutta Gurkmann, "Data Protection Violations by Meta and Co: ECJ Confirms Extensive Right of Consumer Organisations to Take Legal Action to Enforce GDPR" (28 April 2022), online: <vzbv.de/en/data-protection-violations-meta-and-co-ecj-confirms-extensive-right-consumer-organisations-take>.

[29] Johanna Chamberlain & Jane Reichel, "The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation" (2020) 89:4 Mississippi LJ 667 at 694–696.

[30] Lauren Henry Scholz, "Private Rights of Action in Privacy Law" (2022) 63:5 William & Mary L Rev 1639 at 1646–48, 1655–63; Becky Chao, Eric Null & Claire Park, "A Private Right of Action Is Key to Ensuring That Consumers Have Their Own Avenue for Redress" (20 November 2019).

[31] See Danielle K. Citron & Daniel J. Solove, "Risk and Anxiety: A Theory of Data Breach Harms" (2018) 96 Texas L Rev 737 at 781–782.

[32] Sanna Toropainen, "The Expanding Right to Damages in the Case Law of CJEU" (2019) Maastricht Faculty of Law, Working Paper No 2019/03; Walker, *supra* note 27 at 68–69.

Regulators and courts have different institutional advantages.[33] Public enforcement is better positioned than courts to address systemic problems when granted investigatory and sanctioning powers; it can address harms to public goods, such as harms to democracy.[34] However, we do not always know how to determine effective procedures in advance that will prevent future harm, so it is helpful to let private enforcement align entities' capacity to reduce risk with incentives for them to do so.[35] The process of discovery is an information benefit of private rights of action, as fact-finding uncovers whether data practices are in breach, helping increase transparency for enforcing agencies.[36]

As AI and data-mediated interactions continue to seep into more aspects of Canadians' social and economic lives, one regulator for each act with limited resources and personnel will not be able to have their attention on every activity that either of these acts cover.[37] They will have to prioritize. Inevitable budget constraints render it impossible for public enforcement authorities to investigate everything, making it wise to have a mixed enforcement system where they can focus resources on aspects courts cannot address.[38]

If Canada does not want all other harms to fall through the cracks, both parts of the Act need a combined public and private enforcement system taking inspiration from GDPR, where each Commissioner granted with public enforcement (or the Tribunal), issues fines without preventing the court system from compensating for tangible and intangible harms done to individuals and groups.[39]

The CPPA currently incorporates a mitigated private right of action in Section 107(1).[40] However, the section only allows individuals to exercise a private right of action if the Commissioner or the Tribunal already made a finding that the organization has contravened the Act, as PIPEDA currently does.[41] This mechanism makes private rights of action repetitive of, and not complementary to, public enforcement.

Incorporating a private right of action in AIDA would similarly improve its efficacy. The draft bill designates a central authority for initiating legal proceedings for breach of the Act.[42] However, given the growing number of entities involved in high-risk AI development and applications, an exclusively centralized approach to enforcement will encounter substantial obstacles in ensuring compliance.[43] Facilitating private individuals and organizations to initiate legal actions when AI systems inflict harm would alleviate

[33] Cofone, *Privacy Fallacy, supra* note 15 at 153–154.

[34] See Omri Ben-Shahar, "Data Pollution" (2019) 11 J Leg Analysis 104 at 105.

[35] Ignacio Cofone, "Certifying Privacy Class Actions" (2024) 37 Harvard JL & Tech __.

[36] James Dempsey et al, "Breaking the Privacy Gridlock: A Broader Look at Remedies" (2021) at 28–32.

[37] Cofone, *Policy Proposals*, *supra* note 21 at 2.e.

[38] Cofone, *Privacy Fallacy, supra* note 15 at 154–155.

[39] Cofone, *Policy Proposals, supra* note 21 at 2.e.

[40] Bill C-27, *supra* note 1, cl 2(107)(1).

[41] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 14.

[42] Bill C-27, *supra* note 1, cl 39(33)(1).

[43] Derek Brown, "Canada's Proposed Artificial Intelligence and Data Act (AIDA): A Critical Review" (2023).

governmental burden.[44] The threat of litigation from those directly affected, or from organizations acting on their behalf in representative actions, would thus serve as a preventive measure by creating better incentives for compliance. The result would be a more responsible and ethical AI landscape.

For those reasons, I ask the committee, when doing clause by clause review, to consider amending Section 107(1) of the CPPA to say "*An individual who is affected by an act or omission by an organization that constitutes a contravention of this Act has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the contravention*," removing the two conditions currently present, and to add a Section 30(5) in AIDA to incorporate identical language, saying "*An individual who is affected by an act or omission by an organization that constitutes a contravention of this Act has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the contravention*."

Summary

I recommend the committee to make three amendments during clause by clause review.

1. Amend Section 5(1) of AIDA to say: *"harm means: (a) tangible harm to an individual or community, such as physical harm, harm to property, or economic loss; (b) intangible harm to an individual or community, such as psychological or emotional; or (c) dignitary harm to an individual or community, such as through discrimination."*
2. Amend Section 2(1) of the CPPA to say "*personal information means disclosed or inferred information about an identifiable individual or group* (*renseignement personnel*)."
3. Amend Section 107(1) of the CPPA to simply say "*An individual who is affected by an act or omission by an organization that constitutes a contravention of this Act has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the contravention*" and add an amendment in AIDA as Section 30(5) to incorporate identical language.

[44] *Ibid.*