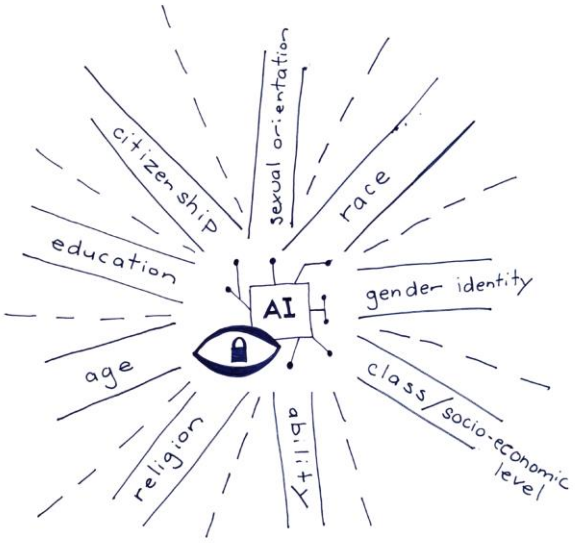


Submission to The Standing Committee on Industry and Technology on Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*

November 2023

Prepared by

Sara Bannerman, B.Mus., MA, PhD
Professor and Canada Research Chair in Communication Policy and Governance
Department of Communication Studies & Media Arts
McMaster University

Karen Louise Smith, PhD
Associate Professor
Department of Communication, Popular Culture and Film
Brock University

Joanna Redden, PhD
Associate Professor
Faculty of Information and Media Studies
University of Western Ontario

Opeyemi Akanbi, PhD
Assistant Professor
The Creative School
Toronto Metropolitan University

Sana Maqsood, PhD
Assistant Professor
Department of Electrical Engineering & Computer Science
York University

Jonathan A. Obar, PhD
Associate Professor
Department of Communication and Media Studies
York University

Tom Streeter, PhD
Professor
Faculty of Information and Media Studies
Western University, Ontario

All graphics: Karen Louise Smith

Endorsed by

Tamara Shepherd, PhD
Associate Professor
Department of Communication, Media, and Film
University of Calgary

Summary

To better uphold the privacy and dignity of individuals and communities, we argue for the inclusion of privacy as a fundamental human right and for the insertion of an intersectional lens throughout the draft Bill C-27. Our argument is backed by research on the social impacts and potential harms of digital systems and recent patterns of behaviour in the digital industries, which suggest broader definitions of harms, inclusion of intersectionality, expansion of mitigation measures, and more robust, transparent, and autonomous oversight are necessary to achieve the goals of C-27. While some of our recommendations align with suggestions made by others, especially prior submissions by Bailey, Burkell, and McPhail, LEAF, and the CCLA; we further advise adding language that includes “groups with intersecting identities” where appropriate. We recommend the requirements and procedures for various parties to assess and mitigate harms should be developed by an independent regulator through public proceedings mandated to include relevant and most-affected groups, and involve intersectional analysis capable of recognizing group, intersectional and cumulative, rather than “high impact,” harms. Towards these ends, we recommend that data collection by government institutions and political parties be included as subject to oversight, and that passage of AIDA be delayed to enable a full public consultation that brings intersectionality to the forefront.

1. Introduction

We, as a group of Communications Policy and Privacy scholars, support the strengthening of privacy, personal data protection, and regulation of autonomous and algorithmic processes under 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*.

This submission suggests ways the language and spirit of the bill can prioritize privacy as a fundamental human right. This submission also suggests inserting intersectional analysis throughout the bill so as to better uphold the privacy and dignity of individuals and communities, and especially for those that are multiply marginalized. As data collection practices expand to include the increased processing of personal information within artificial intelligence (AI) systems, including intersectional considerations can improve the effectiveness of the policymaking processes outlined in the proposed legislation.

1.1 What intersectionality is, and why it is fundamental

In 2018, Buolamwini and Gebru famously noted that facial recognition technology more frequently misrecognizes Black women's faces than it does those of Black men's or white women's faces. If one had been using the categories of only gender, or only race, that discrepancy might have gone unnoticed. Intersectionality involves formal recognition of the fact that categories like gender, race, ability, age, and class overlap. They rarely if ever occur in isolation from each other. Building this fact into the bill and ensuring that a diversity of experiences are considered in the formation of policies will ensure that the full diversity of experiences in Canada are considered in relation to privacy and emerging AI uses.[1]

For example, the participation of groups representing *women* and *Black Canadians* would be positive and appropriate in a consultation on the potential harms in an AI system, or as part of a periodic policy review process related to privacy or AI. However, if the two groups were dominated by white women and Black men respectively, *Black Canadian women* could be accidentally eclipsed. Further, the experiences of Black women is not a simple matter of adding the two identity positions together; it is a unique positionality.[2] Consideration of additional intersecting identity points, such as citizenship status, religion, age, ability, housing status, or other attributes, could create even greater nuance in the understanding of the intersectional experiences of Canadian citizens, residents or visitors in relation to privacy or AI.[3]

---

[1] For a discussion of how social justice and rights might be better achieved with intersectionality see Collins, P. H. (2019). *Intersectionality as critical social theory*. Duke University Press.

[2] The example of Black women being potentially excluded was selected because it is foundational to Kimberlé Crenshaw's (1989) scholarship that helps to coin the term of intersectionality. See Crenshaw, Kimberlé. "Demarginalizing the intersection of race and sex: A Black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics." In *Feminist legal theories*, pp. 23-51. Routledge, 2013. Available at: https://scholarship.law.columbia.edu/faculty_scholarship/3007/

[3] The term Canadian may be limited to citizens of Canada, but we recognize that privacy and AI issues are relevant more broadly to residents, visitors and even individuals applying to enter the country. For example, how AI was applied has been critically questioned in relation to temporary resident visa applications in China and India

Evidence of the importance of intersectionality was found, for example, in the above mentioned fact that facial recognition technologies are most inaccurate for darker-skinned females.[4] Intersectional analysis and research also shows how the use of AI and automated systems leads to differential and harmful experiences across areas of application, for example when a nonbinary trans femme tries to travel through an airport,[5] in the creation of recidivism scores in a criminal justice system, in hiring practices, in housing and employment opportunities, when risk assessing parents for the likelihood of abuse and neglect, and within welfare fraud detection systems.[6]

A consideration of intersectionality makes a systematic analysis of the differential impacts of AI possible. Previous research demonstrates that people who are already marginalized are far more likely to experience harm as a result of applications, while people in positions of privilege may benefit from particular kinds of applications or at minimum escape the harms being experienced by others. For example, researchers have documented how algorithmically mediated insurance rates meant that people living in minority neighborhoods paid more for car insurance than people living in predominantly white neighborhoods, despite similar accident and risk rates.[7] Automated hiring systems have been found to discriminate on the basis of gender, mental health, disability, and ethnicity.[8] Further, researchers have identified how attempts to mitigate bias in hiring systems fail to take intersectionality into consideration, despite its importance to anti-discrimination.[9]

---

to Immigration, Refugee and Citizenship Canada. See: https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/committees/cimm-nov-29-2022/question-period-note-use-ai-decision-making-ircc.html

[4] Joy Buolamwini and Timnit Gebru identified the poor functioning of FRT systems for women with darker skin tones in 2018 research titled 'Gender Shades" Intersectional Accuracy Disparities in Commercial Gender Classification" See: https://proceedings.mlr.press/v81/buolamwini18a.html The Coded Bias documentary illustrates racial and gender biases in facial recognition technology (FRT) systems, which draw upon AI and the documentary features researcher Joy Buolamwini. These systems were also illustrated to impact people differently in contexts relevant to employment, justice and the criminal justice system. See: https://www.ajl.org/spotlight-documentary-coded-bias

[5] Costanza-Chock, S. (2018). Design justice, AI, and escape from the matrix of domination. *Journal of Design and Science*, *3*(5).

[6] Benjamin, R. (2019). Race After Technology: Abolitionist Tools for the New Jim Code. Cambridge: Polity Press; Eubanks, V. (2018). Automating Inequality. New York: Macmillan; Lum, K. and Isaac, W. (2016). To Predict and Serve. Significance. 13(5): 14-19. Retrieved from https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x; Gangadharan, S. P., Eubanks, V., and Barocas, S. (2014). Data and discrimination: collected essays. Open Technology Institute and New America. Retrieved from https://www.ftc.gov/system/files/documents/public_comments/2014/10/00078-92938.pdf (9 Sept. 2015); Hu, M. (2015). Big Data Blacklisting. Florida Law Review, 67: 1735-1809; O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. NewYork, NY: Crown Publishing; Keddell, E. (2015). The Ethics of Predictive Risk Modelling in the Aotearoa/New Zealand Child Welfare Context: Child Abuse Prevention or neo-Liberal Tool? Critical Social Policy, 35 (1): 69–88. doi:10.1177/0261018314543224; Stark, L. (2018). Algorithmic Psychometrics and the Scalable Subject. Social Studies of Science. 48(2), 204–231; Redden, J., Brand, J. and Terzieva, V. (2020) Data Harm Record, Data Justice Lab, https://datajusticelab.org/data-harm-record/

[7] Angwin, J. et al. (2017) Minority neighborhoods pay higher car insurance premiums than white areas with the same risk, ProPublica, https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk

[8] Whitaker, M. et al. (2019) Disability, Bias, and AI, AI Now, https://ainowinstitute.org/wp-content/uploads/2023/04/disabilitybiasai-2019.pdf

[9] Sánchez-Monedero, J. et al. (2020) What does it mean to 'solve' the problem of discrimination in hiring? Social, technical and legal perspectives from the UK on automated hiring systems, In Proceedings of the 2020

In the Canadian policy context, there are numerous groups and communities with intersectional identities at the nexus of race, Indigeneity, age, gender identity, religion, ability and a range of other social locations that are usefully foregrounded as privacy and AI policy are developed. Canada's responsibility to consider intersectionality in privacy and AI policy can be rooted in its Action Plan on Gender Based Analysis [GBA] (2016-2020), where GBA is taking an intersectional turn, by layering in consideration of additional diversity factors through GBA Plus.[10]

Our submission on Bill C-27 addresses a targeted range of issues contained in Bill C-27, and we have focused many of our comments in areas where there is overlap with the concept of intersectionality.

1.2 Privacy as a Fundamental Right

We endorse the calls by many others to recognize privacy as a fundamental human right in the purpose statements of the Bill, and we welcome the Minister's proposed amendments to the CPPA. However, more is required.

The briefs of LEAF, and Bailey, Burkell and McPhail emphasize that substantive equality, as well as privacy, is at stake in many of the data collection and algorithmic systems and practices to be regulated under C-17.[11] We therefore endorse the call by LEAF to recognize the right to substantive equality in the preamble of the bill.

Recognizing substantive equality issues in the preamble of the bill will show increased acknowledgement of intersectional approaches to privacy and the governance of AI. An intersectional commitment to substantive equality can assist to better instantiate privacy as a fundamental right, amongst other human rights in Canada.[12]

> Recommendation: Amend the preamble to Bill C-27, section 5 of the CPPA, and section 4 of AIDA, to recognize privacy as a fundamental right.
>
> We endorse LEAF's call to amend the preamble as follows: "And whereas this Act aims to support the Government of Canada's efforts to foster an environment in which Canadians can seize the benefits of the digital and data-driven economy and to establish a regulatory framework that supports and

conference on fairness, accountability and transparency, https://dl.acm.org/doi/abs/10.1145/3351095.3372849#sec-cit

[10] Government of Canada Action Plan on Gender Based Analysis (2016-2020). https://women-gender-equality.canada.ca/en/gender-based-analysis-plus/resources/action-plan-2016-2020.html

[11] All of the briefs referred to in this document can be found on the INDU committee web site at https://www.ourcommons.ca/Committees/en/INDU/StudyActivity?studyActivityId=12157763

[12] For discussion of intersectionality in relation to human rights see for example: Bakan, A., & Abu-Laban, Y. (2017). Intersectionality and the United Nations world conference against racism. *Atlantis: Critical Studies in Gender, Culture & Social Justice*, *38*(1), 220-235. Intersectionality has been considered in relation to the Open Government Action plan in Canada, see: Canada. (2018). Canada's 2018-2020 National Action Plan on Open Government. Available online: https://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government

protects Canadian norms and values, including the right to privacy and substantive equality." We add that substantive equality requires integrated intersectional analysis to "ensure equality for all, rather than just the relatively privileged minority within a category."[13]

2. *Consumer Privacy Protection Act*

2.1 Intersectionality and the *Consumer Privacy Protection Act*

The *Consumer Privacy Protection Act* (CPPA) is described in Bill C-27 as legislation to protect personal information that is collected to support the processing of commercial transactions and other activities. We call upon policy-makers to recognize that intersectional identities (e.g., gender combined with race, age, etc.) are pertinent to the CCPA and citizens' experiences in their digitally mediated lives, throughout processes including the collection of consent for data collection and understanding of the implications of data processing that happens now, and in the future.

To begin with an example related to intersectionality and age, we concur with UNICEF Canada's submission on Bill C-27 that there are distinct experiences of child users to consider in terms of processes to ensure meaningful consent is obtained before their data is collected or processed.[14] Similarly, Beauvais and Shade call for the need to define a minor, to define capacity to consent, and to add an age threshold for consent. Beyond the age-based issues facing children, there are also numerous other examples where the complexities of intersectional identities impact commercial data processing. Social media platforms are widely understood as sites for commercial data processing: personal information is collected by platform owners and advertising is targeted at consumers as part of the market-based exchange that occurs.

Facebook as a social media platform is helpful to illustrate a convergence of complex factors. The platform Facebook is well known for a real name policy, where government issued identification, or mail received by the account holder, can be required to confirm a user's identity that is displayed on the platform.[15] A member of the 2SLGBTQI+ community who has adopted a new name, but also domestic violence survivors or political dissidents, may be severely challenged to provide authentic meaningful consent, by platform rules that require their 'real' name to be verified to continue to have a presence on the platform.[16]

---

[13] Smith, Ben. "Intersectional discrimination and substantive equality: a comparative and theoretical perspective." *The Equal Rights Review* 16, no. 1 (2016): 75. Available at: https://www.equalrightstrust.org/ertdocumentbank/Intersectional%20Discrimination%20and%20Substantive%20Equality%20A%20Comparative%20and%20Theorectical%20Perspective.pdf

[14] Unicef Canada. (2023, May). Digital Charter Implementation Act 2022 [INDU submission]. Available online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12448397/br-external/UNICEFCan-e.pdf

[15] Facebook. (n.d.). Types of ID that Facebook Accepts. Available online: https://www.facebook.com/help/159096464162185

[16] Rodley, C. (2014, Sept. 25). Facebook's real name policy won't stop queers getting bullied. Available online: https://theconversation.com/facebooks-real-name-policy-wont-stop-queers-getting-bullied-32205

Intersectional identities are also relevant to Facebook in terms of how microtargetting of political advertising on the platform was conducted by Cambridge Analytica. In the Cambridge Analytica scandal, widespread collection of 50 million user profiles occurred, users were categorized with psychometrics, and political advertisements were targeted to profile users during a US election amongst political events.[17]

Furthermore, intersectional identities are also pertinent in relation to a recent investigation by the Office of the Privacy Commissioner of Canada (OPC). The OPC found that the Tim Horton's app was collecting "'vast amounts' of sensitive location data" and they stated that locational data is "highly sensitive because it can be used to infer where people live and work, or reveal trips to medical clinics. It can be used to make deductions about religious beliefs, sexual preferences, social political affiliations and more."[18]

With greater awareness of intersectionality, especially for the multiply marginalized, the CCPA needs to be nuanced in how meaningful consent is obtained. The CPPA should also be broadened to apply to political parties.

2.2 Broaden to include Political Parties

The text of the CCPA is currently limited to electronic commerce and commercial activities. The text of the CCPA does not currently make any mention of federal political parties. In light of the Cambridge Analytica scandal, we believe that information about who supports or communicates with the various political parties in Canada, as well as the political opinions of electors, is highly sensitive information-- the protection of which is essential to democracy. All personal information in the hands of political parties should be encompassed under Bill C-27 or substantially similar privacy legislation. In his submission on Bill C-27, Bennett called "the absence of proper privacy standards for federal political parties (FPPs)...unjustifiable and untenable" and we agree.[19]

Recommendation: Amend Bill C-27 to cover personal information collected by federal political parties. We endorse Colin Bennett's suggested approach of adding a new subsection to 6(1) of the CPPA as follows:[20]

> 6 (1) This Act applies to every organization in respect of personal information that
> (a) the organization collects, uses or discloses in the course of commercial activities; or
> (b) is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business; or

[17] Cadwalladr, C. and Graham-Harrison, E. (2018, 17 Mar). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Available online: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
[18] Office of the Privacy Commissioner of Canada. (2022, June 1). Tim Hortons app violated privacy laws… Available online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220601/
[19] Colin J. Bennett, SUBMISSION ON BILL C-27, DIGITAL CHARTER IMPLEMENTATION ACT TO HOUSE OF COMMONS STANDING COMMITTEE ON INDUSTRY AND TECHNOLOGY, OCTOBER 26, 2023, 3.
[20] Colin J. Bennett, SUBMISSION ON BILL C-27, DIGITAL CHARTER IMPLEMENTATION ACT TO HOUSE OF COMMONS STANDING COMMITTEE ON INDUSTRY AND TECHNOLOGY, OCTOBER 26, 2023, footnote 8.

(c) is collected, used or disclosed by a federal political party, a candidate, an electoral district association, or a nomination contestant in connection with electoral activities.

2.3 Strengthening Consent

We endorse the calls by others to strengthen the consent provisions of Part I of the Bill. Specifically, we endorse the calls by Bailey, Burkell and McPhail to strengthen Bill C-27's consent-related provisions enumerated in part 3 of their brief.

Recommendation: Amend CPPA as per the list of amendments enumerated under item 3 on pp. 13-14 of Bailey, Burkell, and McPhail's brief.

2.4 Deceptive Design

Section 16 of the proposed CCPA states, "An organization must not obtain or attempt to obtain an individual's consent by providing false or misleading information or using deceptive or misleading practices. Any consent obtained under those circumstances is invalid."

We recommend strengthening section 16 to prevent the use of deceptive design practices in obtaining meaningful consent from users. Harry Brignull, defines deceptive design patterns (also known as "dark patterns") as "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something."[21] Indeed, the term 'deceptive design' can refer to user interface designs that can manipulate, coerce, and even exploit individuals.[22] When applied to privacy, these designs may be used by organizations to deceive users into making less privacy-preserving choices (e.g., providing more data than necessary), which are advantageous to the organization but compromise users' privacy. An example of a privacy deceptive design pattern is "*Forced Action*",[23] which describes how users might be forced to complete a secondary action in order to complete their primary task (e.g., nudging the user to accept all terms and conditions in order to purchase an item). Deceptive design patterns may also lead to user interface elements and language that might manipulate the user's emotional state. For example, the "confirmshaming" design pattern[23] could make users feel guilty for not opting into a choice or for opting out of something. Language can be used in the user interface that may nudge users into making an undesired choice (e.g., using *"No, I do not want to help others"* to shame users from opting out of a choice).

[21] Brignull, H. Deceptive design. https://www.deceptive.design

[22] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1-14.

[23] Swedish Consumer Agency. Tech report. (2021). Barriers to a well-functioning digital market. Effects of visual design and information disclosures on consumer detriment. https://www.konsumentverket.se/globalassets/publikationer/produkter-och-tjanster/ovriga-omraden/underlagsrapport-2021-1-barriers-digital-market-konsumentverket.pdf; Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32.

We recommend the government interpret Section 16 as applying to deceptive user interface designs present during online consent processes. Problematic designs like clickwrap agreements can distract and dissuade individuals from engaging in meaningful consent processes.[24] Commercial organizations should be discouraged from using deceptive designs, and encouraged to improve consent user interfaces to better-support meaningful consent processes, aligned with the Office of the Privacy Commissioner of Canada's "Guidelines for Obtaining Meaningful Consent".[25] This should extend beyond sign-up processes and should be applied to cookie consent scenarios. The government should follow the lead of France's *Commission Nationale de L'informatique et des Libertés (CNIL)*, which fined Facebook, Google, and TikTok for deceptive cookie consent user interfaces[26], and the Federal Trade Commission in the United States that is also addressing deceptive user interface designs.[27]

The use of deceptive design patterns has already been included in other jurisdictions, such as the European Directive 2005/29/EC on unfair commercial practices (UCPD) and the California Consumer Privacy Act (CCPA). The following text is included in Chapter 20 of the California Consumer Privacy Act Regulations:

> "A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out. Illustrative examples follow:
> (1) The business's process for submitting a request to opt-out shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.
> (2) A business shall not use confusing language, such as double-negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt-out.
> (3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.
> (4) The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request.
> (5) Upon clicking the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or

---

[24] Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media + Society*, July-September 2018, 1-14.
[25] Office of the Privacy Commissioner of Canada. (2018, May). Guidelines for obtaining meaningful consent. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/
[26] Commission Nationale de l'Informatique et des Libertés (2022, January). Cookies: The CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation. https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance; Commission Nationale de l'Informatique et des Libertés (2023). Cookies: the CNIL fines TIKTOK 5 million euros. https://www.cnil.fr/en/cookies-cnil-fines-tiktok-5-million-euros
[27] Federal Trade Commission (2022, September). Bringing dark patterns to light. Staff report. https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

webpage to locate the mechanism for submitting a request to opt-out."[28]

Recommendations have also been made to include them in the GDPR. Given the negative impact of deceptive design practices on users' privacy, we recommend including them in the CPPA.

Recommendation: Amend section 16 of the CCPA to prevent the use of deceptive designs, and interpret the term "deceptive" to include deceptive user interface designs.

3. *Personal Information and Data Protection Tribunal Act*

An intersectional approach must be core to a Data Protection Tribunal in Canada. In the UNICEF Canada brief on Bill C-27, the authors recommended the development of "specific strategies and processes to ensure that the accountability mechanisms proposed under Bill C-27 are accessible and understandable to children and young people, and actively promote their participation." Indeed, making the Data Protection Tribunal processes, and any accountability mechanism accessible to children, or any group or community that is harmed or negatively impacted must be considered carefully.

In their submission on C-27, Bailey, Burkell and McPhail recommend, "creating an arms-length, independent public tribunal with full investigatory and enforcement powers to carry out the functions determined to be necessary through public consultation."

Recommendation: as recommended by Bailey, Burkell and McPhail, we advocate to "create an arms-length independent public tribunal with full investigatory and enforcement powers to carry out the functions determined to be necessary through public consultation" where consultations explicitly address intersectional lived experiences with data collection, processing and privacy issues.

4. The *Artificial Intelligence and Data Act* (AIDA)

4.1 Consultation

Multiple submissions regarding AIDA have identified that consultation with diverse stakeholders is significant and necessary.

[28] California Consumer Privacy Act Regulations, Available at: :https://oag.ca.gov/system/files/attachments/press-docs/CCPA%20March%2015%20Regs.pdf

In particular, we note that OpenMedia and 45 civil society and academic signatories identified they are "gravely concerned that shoehorning AI regulation into Privacy Bill C-27 [which] will not allow for adequate consideration of AIDA."[29] Bailey, Burkell and McPhail recommend, "delaying passage of AIDA pending full public consultation and amendments aimed at reducing the number of important matters left to be dealt with via regulation." We endorse these recommendations.

We concur that the issues associated with AIDA are too complex to embed in the multi-faceted Bill C-27, and call for AIDA to be separated and dealt with in a robust manner, which truly consults Canadians in a manner that brings intersectionality to the forefront. Any policies that are developed to govern AI in Canada should be thoughtful, thorough, comprehensive, and responsive to the rights based issues that are at stake.

Recommendation: The passage of Part 3, the *Artificial Intelligence and Data Act* should be delayed to enable a full public consultation that brings intersectionality to the forefront.

4.2 Ongoing public input and review

Should AIDA continue through in the current process, we recommend adding robust mechanisms for ongoing review.

Recommendation: We endorse the CCLA's call to amend "AIDA to add periodic Parliamentary review and annual reporting so AIDA can keep abreast of rapid technological developments" (recommendation 23, p 5). We endorse LEAF's call to amend s. 35(1) of AIDA as follows: ""Advisory committee 35 (1) The Minister may establish a committee to provide the Minister with advice on any matters related to this Part. The committee should reflect a range of perspectives, ensuring public input and consultation particularly from communities most affected by the use of AI systems."" (p. 15) We add that committee consultation should be inclusive of intersectional identities and analysis.

[29] https://openmedia.org/press/item/advocates-demand-proper-consideration-for-ai-regulation

4.3 Intersectional analysis

Greater awareness and integration of intersectionality theory will potentially allow the Government of Canada to craft policy that better responds to impacts experienced by communities of individuals living in Canada (e.g., children and young people, racialized communities, diversely abled citizens, etc.).

- Utilize intersectional approaches throughout policy making and regulation process for AI
    - Consultation and public engagement on AI related issues that reaches and involves intersection communities is necessary;
    - Categorization of AI systems (if applicable) should consider the intersectional experiences that are probable for Canadian citizens or residents;
    - Algorithmic impact assessments, algorithmic audits and consideration of harms of AI systems should include the most impacted communities and draw from intersectional analysis;
    - The policy review cycle for any AI relevant laws in Canada should include intersectional analysis.

Add a new s. 35.1 stating "Analysts and advisory committee members shall undertake robust intersectional analysis of the impacts of artificial intelligence systems and the operations of this act, to encompass ways of including and assessing impacts on groups with intersecting identities."

As above, we endorse LEAF's call to amend s. 35(1) of AIDA as follows:
""Advisory committee
35 (1) The Minister may establish a committee to provide the Minister with advice on any matters related to this Part. The committee should reflect a range of perspectives, ensuring public input and consultation particularly from communities most affected by the use of AI systems."" (p. 15)

To this, we add:
35 (1) The Minister may establish a committee to provide the Minister with advice on any matters related to this Part. The committee should reflect a range of perspectives, ensuring public input and consultation particularly from communities most affected by the use of AI systems, including those with intersecting identities and those adopting intersectional analysis.""

4.4 Scope

Public sector, government, and national security organizations

We endorse the calls by LEAF; the CCLA; Bailey, Burkell and McPhail; and others to expand the scope of AIDA to encompass the public sector and government organizations, including national security products, services, and activities.

The fact that AIDA does not apply to government institutions means that it is already outdated, inadequate, and dangerously out of step with the needs of Canadians as well as the legislative and regulatory approaches taken by other AI leading nations. For example, both the recent EU AI Act and the White House Executive Order on AI apply to uses of AI by government institutions. There is an extensive body of research documenting the ways government uses of AI and automated systems have already led to harm.[30] Previous research has also documented the strain placed on individuals, communities and review bodies to stop the use of harmful AI practices once in place, reinforcing the importance of oversight to ensure investigations of impact and extensive review before implementation and that such efforts should be put in place and apply to government uses of AI.[31]

While the Government of Canada has not yet provided a registry of AI systems in use, our own work in developing such a registry has identified at least 249 applications of AI across federal government institutions and agencies.[32] The widespread use of AI and the risk and harm that can come with AI, demonstrate the need for AIDA to apply to government applications.

Recommendation: We endorse LEAF's recommendation to "Remove section 3 of AIDA so the Act and subsequent regulations apply to government institutions."

We endorse the CCLA's recommendations to "Amend language throughout the bill—including the name of Part 1, "Regulation of Artificial Intelligence Systems in the Private Sector"—to account for public sector and national security actors" and "Amend AIDA to add periodic Parliamentary review and annual reporting so AIDA can keep abreast of rapid technological developments." (Recommendations 22 & 23, p 6).

Political parties and activities

The act defines regulated activity (s 5(1)) as:

[30] For example, see work cited in note 6.
[31] Redden, J. et al. (2022) Automating Public Services: Learning from Canceled Systems, Carnegie UK Trust and Data Justice Lab, https://d1ssu070pg2v9i.cloudfront.net/pex/pex_carnegie2021/2022/09/21101838/Automating-Public-Services-Learning-from-Cancelled-Systems-Final-Full-Report.pdf
[32] Redden J. and Sahoo, S. (forthcoming) Mapping Canadian Government Uses of AI for Social Services. Starling Centre.

any of the following activities carried out in the course of international or interprovincial trade and commerce:
(a) processing or making available for use any data relating to human activities for the purpose of designing, developing or using an artificial intelligence system;
(b) designing, developing or making available for use an artificial intelligence system or managing its operations.

We endorse the calls of other organizations calling for the expansion of the Act beyond international or interprovincial trade or commerce, and we specifically call for political activities--particularly the activities of federal political parties--to be encompassed.

Recommendation: Amend s 5(1) as follows:

regulated activity means any of the following activities carried out in the course of international or interprovincial trade and commerce or in connection with electoral activities:
(a) processing or making available for use any data relating to human activities for the purpose of designing, developing or using an artificial intelligence system;
(b) designing, developing or making available for use an artificial intelligence system or managing its operations.

4.5 Harm and significant harm

The bill currently deals with harms that impact individuals; s. 4(b) of AIDA (Purposes) states that the purpose of AIDA is "to prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests" (emphasis added). The bill creates an offense of making an AI system available for use, knowing or being reckless as to whether it "is likely to cause serious physical or psychological harm to an individual or substantial damage to an individual's property," where the use of the system causes such harm or damage (s 39).

By focusing solely on harm at an individual level, AIDA does not address the kinds of collective harms being experienced at community or societal levels. Legislation and regulation that focus solely on individual harm ignores AI harms that affect groups of people and can be an impairment and setback for societal interests. For example, an individualized understanding of harm may leave AI applications that involve spreading misinformation, voter manipulation, wrongful denial of services or discriminatory sorting on the basis of group or collective identifiers. Legal scholars have argued for data harms to be understood as the adverse effects caused by uses of data that may impair, injure, or set back a person, entity or society's interests.[33]

[33] For discussions of the need to expand legal definitions of harm in connection with AI applications see: Citron, Danielle Keats and Solove, Daniel J., Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793

Many commentators, including LEAF (p 5), the CCLA (p. 14), the International Civil Monitoring Group (p 12), and Bailey, Burkell and McPhail (p 11), have suggested amending the definition of harm in section 5 to include harms to an identifiable group and other collective concepts. We agree.

Recommendation: We endorse LEAF's recommendation, endorsed by the International Civil Monitoring Group (p 12), to amend s 5 as follows:

"Harm means
(a) physical or psychological harm to an individual or identifiable group;
(b) damage to an individual's property, collectively owned property, land or buildings held on behalf of a group or collective, or public property or public spaces; or
(c) economic loss to an individual or identifiable group."

We recommend further adding to (a) and (c):
(a) physical or psychological harm to an individual or identifiable group, including groups with intersecting identities;
(b) damage to an individual's property, collectively owned property, land or buildings held on behalf of a group or collective, or public property or public spaces; or
(c) economic loss to an individual or identifiable group, including groups with intersecting identities."

Minister Champagne, in his communication following his September 25, 2023 appearance before the committee, proposes to clarify, with future amendments, the responsibilities of developers, persons making available, and persons managing the operation of high-impact systems. This communication seems to relegate responsibility for assessing and mitigating risks of harm to 'developers'. This is entirely inadequate. Developers are likely to be employed by or contracted to those who stand to profit from algorithmic and machine learning systems. They do not necessarily have the skills, capacity, resources, or positioning to identify individual, group, or societal harms.

Recommendation: The requirements and procedures for various parties to assess and mitigate should be developed by an independent regulator through public proceedings mandated to include relevant and most-affected groups, and intersectional analysis capable of recognizing intersectional and cumulative harms.

4.6 Impacts ("high impact")

The bill defines a *high-impact system* as:

> "an artificial intelligence system that meets the criteria for a high-impact system that are established in regulations."

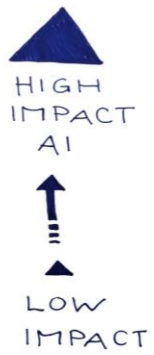
(2022), Available at SSRN: https://ssrn.com/abstract=3782222 or http://dx.doi.org/10.2139/ssrn.3782222; D. Solove and D. Citron (2016) Risk and Anxiety: A Theory of Data Breach Harms, *Texas Law Review,* 737, Solove, Daniel J. and Citron, Danielle Keats, Risk and Anxiety: A Theory of Data Breach Harms (December 14, 2016). 96 Texas Law Review 737 (2018), GWU Law School Public Law Research Paper No. 2017-2, GWU Legal Studies Research Paper No. 2017-2, U of Maryland Legal Studies Research Paper No. 2017-3, Available at SSRN: https://ssrn.com/abstract=2885638 or http://dx.doi.org/10.2139/ssrn.2885638

Those responsible for high-impact systems must, under the bill, in accordance with the regulations, "establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system" (s 8) and "establish measures to monitor compliance with the mitigation measures they are required to establish under section 8 and the effectiveness of those mitigation measures" (s 9). Public posting of plain-language descriptions of high-impact systems (s 11) and notification to the Minister of likely material harms (s 12) is also required.

The relegation of duties to assess, monitor, mitigate, publish, and notify to a narrow class of systems identified as "high-risk" is problematic for several reasons. First, harms cannot be easily categorized in a hierarchical manner from "high" to "low" impact. Second, a narrow definition of "high-impact systems" assumes a homogeneous definition of risk or harm. Different communities may experience systems differently, and equitable approaches to mitigating associated risks and harms must not assume that only systems labeled "high-risk" are potentially problematic. Furthermore, the cumulative effect of so-called "low-risk" systems that contribute to harms for people across different sectors could be greater than the harms experienced in so-called "high-risk" scenarios that may not even be relevant to the same individual. An equitable approach to protections must acknowledge the unique and nuanced needs of members of marginalized and vulnerable communities in Canada, and not assume to know the answers to the questions before they are even asked.

Problems with hierarchical assumptions

Rating AI systems in any hierarchical manner, such as a 'low' to 'high impact' AI systems, potentially reduces awareness of:

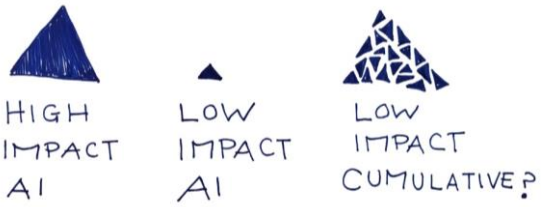


- The shifting contexts of AI's deployment and use. As Bailey, Burkell, and McPhail note, "future uses of one's data can be very difficult to predict" (p. 5). Particularly in a context where the general public and, at times, industry and professional groups, may be often unaware of the actual and potential uses of their data, current and future potential impacts can be difficult to identify. Members of the public and organization outsiders may be unaware of current or future algorithmic processing and its implications, while organizations may be unaware of the effects of such processing, and without robust mechanisms and situatedness for becoming aware.
    - Privacy as contextual integrity[34] is an important scholarly idea that is relevant to any attempts to govern or regulate AI, where contextual integrity is also likely to be relevant
- Miscategorization of systems (e.g., something deemed low impact initially, that can cause significant harm because it is misunderstood or the context of use shifts)
- Non-uniform or standardized experiences of AI in the lives of citizens
- Possible interplay between citizens' experiences of multiple AI systems
- It is possible that attempts to anonymize or aggregate data may

[34] Nissenbaum, Helen. "Privacy as contextual integrity." *Wash. L. Rev.* 79 (2004): 119.

result in a label of “low-risk”. The academic literature suggests that re-identification by combining supposedly anonymized data sets is possible.[35] With the lack of oversight due to the “low-risk” label, this scenario might go unchecked.

One possible interplay between citizens’ experiences of multiple AI systems is that exposure to many ‘low’ impact systems could add up to a low impact cumulative effect that equals or exceeds a ‘high impact AI’ system.



We are concerned that “low impact” systems may be excluded from careful scrutiny or audit. For example, algorithmic impact assessments may be conducted on systems that are perceived as high impact, with low impact systems, and situations of a low impact cumulative effect, not receiving appropriate scrutiny.

Given the difficulty of hierarchizing impacts from “high” to “low”, a number of approaches have been suggested. LEAF, in its brief to the Industry committee, notes that:

> unless “high impact” is defined so broadly as to include almost any system with social valence (which would call into question the need for such a category in the first place), it will not sufficiently address the real concern at the heart of this legislation - mitigating harm and discriminatory bias.
>
> Instead, all systems should be required to adhere to some degree of oversight and mitigation measures. (LEAF, pp 11-12)

LEAF recommends removing “high-impact” from ss. 8 (identify, assess, and mitigate risks), 9 (monitor compliance under s8), 11 (publication of description), 12 (notification of material harm), and 36 (regulations to define ‘high-impact system’).

The International Civil Liberties Monitoring Group recommends, in their brief, both removal of the term ‘high-impact’ from ss 8, 9, 11, 12, and 36, and leaving it to the Governor in Council to further define categories of AI systems to be subject to oversight (p 11).

The CCLA recommends not only the adoption of multiple levels of impact, following the model of the EU’s AI Act (recommendation 15), but also amending s.7 “to shift the responsibility of assessing whether an AI system is high impact to an independent third-party assessor” (recommendation 18). It notes that determination of level of impact is, under the current wording, left to corporations; it would shift this burden to an independent regulator.

---

[35] Sweeney, Latanya. “Simple demographics often identify people uniquely.” Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000

Recommendations: We endorse LEAF's approach of removing the language of "high-impact" from the relevant provisions ss. 8 (identify, assess, and mitigate risks), 9 (monitor compliance under s8), 11 (publication of description), 12 (notification of material harm), and 36 (regulations to define 'high-impact system').

We recommend that the definition and determination of applicability of categories of impact be tasked to an independent regulator through public proceedings mandated to include relevant and most-affected groups, and intersectional analysis capable of recognizing intersectional and cumulative impacts. Consultation, engagement and impact assessment processes need to be resourced to facilitate widespread community participation.

Excluded impacts

Minister Champagne, in his communication following his September 25, 2023 appearance before the committee, proposes to adopt a relatively broad definition of "high impact AI systems" that includes contexts of employment, training, the processing of biometric information in limited contexts, content moderation and others (p. 2-3). We welcome the articulation of this list and a broad definition of "high impact." However, the proposed list does not include several important categories such as systems used:

- to identify, predict, or make inferences about political opinions and orientations;
- in political communication, including systems used to target or influence electors with political messages, communications, or advertisements;
- for education,
- for worker management,
- to control access to public and essential private services,
- in border control,
- in the provision of legal services,
- and many other categories.

The proposed list of classes has not been subject to robust public consultation. As above, those impacts deemed "high impact" or those otherwise defined as subject to the bill's provisions must be open to adaptation and change so that impacts initially deemed low or outside the scope of robust regulation, cumulative impacts, and unexpected or unanticipated impacts can be brought under greater regulation as needed.

Recommendations:

Regulations setting out a list of "high impact systems"--or systems encompassed by the AIDA regime-- should be created through a process involving public consultation encompassing diverse groups that includes intersectional identities.

Any list of "high impact systems"--or systems encompassed by the AIDA regime--should be subject to

annual public consultations, review, and revision, encompassing diverse groups that includes intersectional identities.

Any list of “high impact systems”--or systems encompassed by the AIDA regime--should include systems used :

- to identify, predict, or make inferences about political opinions and orientations;
- in political communication, including systems used to target or influence electors with political messages, communications, or advertisements;
- for education,
- for worker management,
- to control access to public and essential private services,
- in border control, and
- in the provision of legal services.

4.7 Mitigation Measures

In light of the foregoing concerns about the narrow definition of harms and the absence of intersectional considerations, the mitigation obligations imposed on persons responsible for artificial intelligence systems ought to be more robust than currently outlined in section 8, 9 and 11 of the AIDA. If recent developments in AI have taught us anything, it is that companies in the AI space have a tendency to move faster than their ability to guarantee the safety and dignity of people affected by these technologies. Invariably, the role of government is to ensure a delicate balance between the expansion of the digital economy and the safety of people across various identity groups.

The facial recognition example we cited in the introduction to this brief is instructive. IBM decided to retract its facial recognition software in response to concerns about the tendency of the technology to mis-identify people of colour and women. While this was celebrated, the bigger question is whether it is prudent to leave these kinds of decisions to companies. We suggest that periodic transparency reports and mandatory access for academic researchers and civil society groups to training data for algorithmic systems might provide more impactful pathways for ensuring accountability and mitigation measures. Specifically, given the history of the development of intersectionality, academic researchers and civil society groups are more likely to identify associated harms than corporate compliance officers. The Stanford University Center for Research on Foundation Models and Ranking Digital Rights are already working on standards for evaluating AI providers.

5. Endorsements of Related Briefs

We strongly endorse the recommendations made in the briefs submitted to the Standing Committee on Industry and Technology by 1) LEAF, the Women’s Legal Education & Action Fund; and 2) Jane Bailey, Jacquelyn Burkell, and Brenda McPhail. Numerous additional briefs continued to be posted as we

drafted our submission, we find many synergies with the briefs by UNICEF Canada, Beauvais and Shade, and Bennett, The International Civil Liberties Monitoring Group, and Canadian Civil Liberties Association submitted to INDU.

About the authors

Sara Bannerman, Canada Research Chair in Communication Policy and Governance, is a Professor of Communication Studies at McMaster University. She is the author of *Canadian Communication Policy and Law* (Canadian Scholars, 2020) and co-editor, with James Meese, of *The Algorithmic Distribution of News: Policy Responses* (Palgrave, 2022). She has published two books on international copyright: *International Copyright and Access to Knowledge* (Cambridge University Press, 2016) and *The Struggle for Canadian Copyright: Imperialism to Internationalism, 1842-1971* (UBC Press, 2013)—a history of Canadian international copyright. She has published in journals such as *New Media & Society, Communication Theory*, *New Political Economy*, the *Canadian Journal of Communication*, *Futures*, and *Information, Communication & Society*.

Karen Louise Smith, is an Associate Professor in the Department of Communication, Popular Culture and Film at Brock University. Her research has focused on public interest issues associated with the internet and emerging technologies since the early 2000s. Dr. Smith has worked extensively in community based settings to explore topics including universal access, privacy, and citizen service encounters. Her work is published in academic journals including *Surveillance & Society, Big Data & Society, Computer Supported Cooperative Work, Studies in Social Justice, and The Canadian Journal of Law & Society.*

Joanna Redden is an Associate Professor in the Faculty of Information and Media Studies at Western University. She co-directs Starling: Research Centre for Just Technologies, Just Societies at Western University and the UK-based Data Justice Lab. Her research focuses on the social justice implications of AI and automated decision making systems. This work involves mapping government uses of AI, documenting data harms and learning from people trying to redress and prevent data harms as well as working to advance greater civic participation in response to datafication. Recent publications include the co-authored *Data Justice* as well as *Automating Public Services: Learning from Canceled Systems*.

Opeyemi Akanbi is an Assistant Professor in The Creative School at Toronto Metropolitan University. Her research lies at the intersection of law and communication and she has published in academic journals such as *Media Culture and Society*, *International Journal of Communication*, *Canadian Journal of Communication* and *Yale Law Journal Forum*. Her teaching includes courses in Political Economy, Privacy and Organizational Communication.

Sana Maqsood is an Assistant Professor in the Department of Electrical Engineering & Computer Science at York University. Her research is at the intersection of human-computer interaction, cybersecurity and privacy. Recent publications include *Security and Privacy perceptions of mental health chatbots* and *Usability of Paper Audit Trails in Electronic Voting Machines*. Her latest project involved developing a security and privacy literacy game for tweens (A Day in the life of the JOs) in partnership with MediaSmarts, and the game has been deployed in over 500 Canadian elementary schools.

Jonathan A. Obar is an Associate Professor in the Department of Communication and Media Studies at York University. Recent academic publications address big data and privacy, online consent processes, corporate transparency, deceptive user-interface designs, and network neutrality. Publications appear in academic journals such as: *Big Data & Society*, *Telecommunications Policy*, *Information Policy*, *Information Society*, *Social Media + Society*, and *Information, Communication & Society*. He recently launched www.biggestlieonline.com, a knowledge mobilization site funded by the Office of the Privacy Commissioner of Canada to engage stakeholders in meaningful online consent research.

Tom Streeter is a Professor in the Faculty of Information and Media Studies at Western University. He received the C. Edwin Baker Award for the Advancement of Scholarship on Media, Markets and Democracy, at the International Communications Association in 2017. His publications include *The Net Effect: Romanticism,*

Capitalism, and the Internet (NYU Press, 2011), *Selling the Air*, a study of the cultural underpinnings of the creation of the US broadcast industry and its regulatory apparatus (Chicago UP, 1996), and, with Zephyr Teachout, an edited volume *Mousepads, Shoe Leather, and Hope* (2007). He has published articles and chapters in outlets ranging from the *Cardozo Arts and Entertainment Law Journal* to the *Journal of Communication* to *Critical Inquiry*.