February 29, 2024

Mr. Joël Lightbound
Chair
Standing Committee on Industry and Technology
House of Commons

Dear Mr. Chair,

Re: Submission regarding Bill C-27

Thank you for the opportunity to provide my input regarding Bill C-27. This is my first time making a submission to the Committee.

My background

I have recently earned my PhD in Law from the University of Western Ontario in the area of privacy law. In my PhD dissertation, I argued that there was an "electronic surveillance gap" in privacy legislation generally, and that it was important to narrow the scope and begin examining this gap in the employment context because: the employment relationship was the most suitable setting for studying and understanding electronic surveillance technologies as they affected relationships of power imbalances; there was a rich body of case law stemming from workplace privacy cases that could provide significant insights about how to best create an effective privacy regime pertaining to electronic surveillance technologies; and the centrality of paid work to the lives of individuals made the study of workplace privacy a high priority.[1]

More specifically, I dealt with surveillance and the privacy laws of Canada, the United States, and the European Union.[2] In this comparative socio-legal analysis, I synthesized privacy legislative provisions, privacy cases, and social theories of privacy and surveillance[3] to propose new provisions in Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)*.[4] In particular, I proposed closing the electronic surveillance gap with novel legislative data protection provisions in a new workplace privacy regime by modifying and adding provisions to *PIPEDA*.[5]

I am currently working as a consultant (self-employed)—my comments reflect my personal opinions and are only made in attempt to help Canada create provisions for new and improved federal private sector privacy and artificial intelligence laws. In this document, I will discuss my thoughts concerning both privacy and artificial intelligence (AI) provisions contained in Bill C-

[1] Christina Catenacci, "Privacy and Surveillance in the Workplace: Closing the Electronic Surveillance Gap" (2020) at 5–12, online (pdf): *Scholarship@Western* <https://ir.lib.uwo.ca/etd/7117/> [Electronic Thesis and Dissertation Repository: 7117] [Christina Catenacci, "Privacy and Surveillance in the Workplace"].
[2] *Ibid* at 13–22.
[3] *Ibid*.
[4] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].
[5] Christina Catenacci, "Privacy and Surveillance in the Workplace", *supra* note 1 at 290–328.

27.[6] More specifically, I will address the *Consumer Privacy Protection Act* (CPPA), the *Personal Information and Data Protection Tribunal Act* (PIDPTA) and the *Artificial Intelligence and Data Act* (AIDA).

My Thoughts

1. Privacy

Given that this part of the bill has gone through a couple of iterations beginning with the proposed Bill C-11,[7] and a great deal of time has passed since the bill has been introduced, it is safe to say that Canadians have been patiently waiting for a fresh draft of a modern federal private sector privacy law. In fact, since I graduated at the end of 2020 with a doctoral dissertation that proposed *PIPEDA* provisions to protect vulnerable employees from the harmful implications of surveillance technologies in the workplace, no federal law has been enacted and we still have *PIPEDA*.

I agree with many of the previous submissions on Bill C-27. However, I would like to highlight five main concerns:

1. The proposed privacy provisions contained in the *CPPA* would not protect the most vulnerable individuals—employees—in federally regulated employment. I argued this point in my dissertation when trying to improve *PIPEDA*; however, the *CPPA* looks very similar when it comes to providing privacy protections for federally regulated employees. More precisely, when examining the privacy provisions in the employment context, there are again no provisions that explicitly protect employees from employers' use of overly intrusive and excessive surveillance technologies that employers may use when exercising their management rights. This is problematic since employees are not in a position to consent to the collection of their personal information; that is, employees are not able to freely consent to employer monitoring because they are concerned about the consequences of saying "no" and they depend on their employers to earn a living.[8]

    - I would like to suggest that new provisions be created in order to protect the privacy rights of employees. I have drafted several suggestions in my proposed privacy regime that aims to create a healthy balance of privacy rights of employees with the management rights of employers, by modifying, reworking, and creating new privacy provisions[9].

---

[6] 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 amendments to other Acts*, 1st Sess, 44th Parl, 2022 (currently in the House in the Industry and Technology Committee) [Bill C-27].
[7] Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential amendments and related amendments to other Acts*, 2nd Sess, 43rd Parl, 2020 (died on the Order Paper due to the election and never reached the Committee).
[8] Christina Catenacci, "Privacy and Surveillance in the Workplace", *supra* note 1 at 154–178.
[9] *Ibid* at ch 6.

2. The proposed provisions in the *CPPA* would not protect the privacy rights of young persons in the consumer context. The surveillance gap that I highlighted in my doctoral dissertation exists in like manner for young consumers. This can be seen with the monitoring, targeting, manipulating, and bullying of young people on social media. As with employees, children are not in a position to consent (they are minors) or appreciate the implications of their decisions when using social media. Simply put, there are insufficient protections in place to protect the privacy of children.

    - I would like to suggest that new privacy provisions be created to protect the privacy rights of children. This would include adding features that would protect children from being bullied or manipulated on social media

3. The provisions in the *CPPA* would not protect women, politicians, and other people who are in the public eye from the dangerous and damaging implications of deepfake technology. Technologically speaking, it is quite easy to create a deepfake, put it on a social media platform, and have cause it to be viewed millions of times. The problem is serious, and I believe that we are not ready for this kind of technology whatsoever.

    - As I discussed in a recent article,[10] Canada needs some strong privacy protections to protect the privacy rights of the victims of deepfakes. I would like to suggest that Canada create provisions similar to British Columbia's recently created legislation, and place it in the *CPPA*.

    - I would also like to suggest the addition of criminal provisions to deter deepfake creators and distributors from making, posting, or sharing deepfake images or videos on the internet.

4. Privacy is not characterized as a fundamental right. As I explained in my dissertation, the problem is that without the human right to privacy, the autonomy of individuals would be threatened.[11]

    - There should be a provision in the *CPPA* in the purpose section so it is made clear form the outset that privacy is a fundamental human right—the law needs to adapt to evolving societal values and embrace rights-based language.

5. There is some question as to whether it is necessary to have the Tribunal as established in the *PIDPTA* (Part 2 of Bill C-27). This could be problematic because it would add another level of privacy governance, creating time delays, confusion, and additional costs.

---

[10] Christina Catenacci, "The problem with deepfakes, and British Columbia's solution" (23 February 2024), online: <https://blog.firstreference.com/the-problem-with-deepfakes-and-british-columbias-solution/>.
[11] Christina Catenacci, "Privacy and Surveillance in the Workplace", *supra* note 1 at 145.

- I would like to suggest that the Office of the Privacy Commissioner of Canada be granted order-making powers, with the orders having the same effect as a court order from the Federal Court of Canada. This would eliminate the need for the Commissioner to recommend penalties to the Tribunal, since the Commissioner would be able to make the order itself. By removing the Tribunal, the process would be more expeditious.

2. Artificial Intelligence

Firstly, it is worth noting that the confusion that came with the first version of *AIDA*,[12] the subsequent amendments that attempted to provide some clarifications to the skeletal *AIDA* provisions,[13] the companion document,[14] and the Minister's letter to the Committee,[15] there have been major concerns that we are not creating a strong, clear, and modern AI law that is aligned with Canadian values.

Disappointingly, the recent rush to catch up to other jurisdictions like the European Union[16] or the United States[17] has left us pushing to pass an AI law before we have properly considered the implications or asked ourselves some important questions about our intentions as a society, the incentives associated with the use of AI, the potential unintended consequences, and what we would do to prevent those consequences.

For the most part, I agree with many of the submissions that have previously been made. That said, I would like to highlight five main concerns:

1. The provisions in *AIDA* (and amendments mentioned above) would still not be sufficient to address the serious implications of AI, and does not even come close to what is contained

---

[12] Bill C-27, supra note 6.
[13] Committee Minister of Innovation, Science and Industry, "Correspondences from the Honourable François-Philippe Champagne to the Standing" (November 2023) online: <https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12633023/12633023/MinisterOfInnovationScienceAndIndustry-2023-10-20-e.pdf>; see also <https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12600809/12600809/MinisterOfInnovationScienceAndIndustry-2023-10-03-e.pdf>.
[14] Government of Canada, "The Artificial Intelligence and Data Act (AIDA)—Companion document" (13 March 2023), online: <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document>.
[15] Committee Minister of Innovation, Science and Industry, "Correspondences from the Honourable François-Philippe Champagne to the Standing" (November 2023) online: <https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12600809/12600809/MinisterOfInnovationScienceAndIndustry-2023-10-03-e.pdf>.
[16] European Parliament, "EU Act: first regulation on artificial intelligence" (19 December, 2023), online: <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>.
[17] See The White House, "Executive Order on the Safe, Secure, Trustworthy Development and Use of Artificial Intelligence" (30 October, 2023), online: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> [White House, "Executive Order"].

in the EU's *Artificial Intelligence Act*.[18] In my view, it is unacceptable to push forward with something that is not ready because "something is better than nothing". The problem is that Canadians need and deserve meaningful AI protections, and it might be useful to be prudent and take the time that is required to properly deal with AI.

- I would like to suggest that Canada not move forward with the current version of AIDA, and instead take some time to carefully and thoughtfully draft provisions that can be more aligned with what is in the EU's *Artificial Intelligence Act*. This would entail separating Bill C-27 into two parts: the *CPPA* and *AIDA*. The *PIDPTA* would not be included.

2. The definition of "high-impact system" was initially missing and left to the regulations. Now, with the amendments, we see that the proposed schedule would set out a list of classes that describe certain uses. There is a lack of detail and clarity about what the requirements would be; for example, the first use involves employment, recruitment, promotion, and other employment decisions. The problem, as it seems to me, is that there is not enough information to properly tackle the problem and address the implications of using AI with this use case.

    - In a recent article,[19] I examined Ontario's attempt to govern the use of AI in hiring, and I noted that the bill was virtually a skeleton with no substance whatsoever. I recommended examining New York's law with the following requirements: conducting a bias audit before using any AI tools; posting a summary of results of the bias audit on the company website; notifying job candidates and employees that the AI tool would be used to assess them (and include instructions regarding accommodations); and posting on the employer's website a notice about the type and source of data that is used for the tool and the employer's data retention policy. Further, in Biden's Execuitve Order on AI,[20] there was a commitment to supporting workers and this would entail ensuring that AI was not deployed in ways that undermine rights, worsen job quality, encourage undue worker surveillance, lessen market competition, introduce new health and safety risks, or cause harmful labour-force disruptions.

    - I would like to suggest that Canada incorporate some of these ideas and add more extensive provisions with respect to the list of classes for high-impact systems

[18] EC, *Proposal for a Regulation pf the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union Legislative Acts*, [2021] [*AI Act*].
[19] Christina Catenacci, "Bill 149: a focus on hiring employees and employers' use of AI" (19 January 2024), online: <https://blog.firstreference.com/bill-149-a-focus-on-hiring-employees-and-employers-use-of-ai/>.
[20] White House, "Executive Order", note 17.

3. Technology moves quickly—just take ChatGPT and Bard. Already, Bard has become Gemini.

    - It is necessary to add a requirement that there be a regular review of the legislation and periodic amendments as required to keep up with the pace of technology.

4. There seems to be some confusion regarding the entity that would be dealing with bias and discrimination

    - I would like to suggest that this task be assigned to the Canadian Human Rights Tribunal, not ISED.

5. It appears that the addition of anonymized data in *AIDA* has created some inconsistencies with what is in the *CPPA*.

    - I would like to suggest that provisions be added in order to provide some clarification in this regard.

Thank you, and please do not hesitate to contact me if you have any questions.

Christina Catenacci
BA, LLB, LLM, PhD