CUPE

Canadian Union of Public Employees

Submission to the Standing Committee on Industry and Technology

Study of Bill C-27, Digital Charter Implementation Act, 2022

January 29, 2024

1375 boul. St. Laurent
Ottawa, ON K1G 0Z7
613-237-1590
scfp.ca

The Canadian Union of Public Employees (CUPE) is Canada's largest union, with over 740,000 members. CUPE members take great pride in delivering quality services in communities across Canada in sectors representing a broad cross-section of the economy including health care, education, municipalities, early learning and child care, libraries, universities and colleges, social services, public utilities, emergency services, transportation, airlines, ports, and communications.

Consumer Privacy Protection Act

The Consumer Privacy Protection Act (CPPA) regulates the collection, use, and disclosure of personal information by private sector organizations. In this regard, the legislation affects all workers in Canada. The CPPA also addresses the personal information of private sector employees in federally regulated sectors. This legislation will affect workers who CUPE represents in the telecommunications, ports, and airline sectors.

CUPE has long advocated to uphold and strengthen the right to privacy and protect individuals' private lives. Through lobbying, collective bargaining, and legal proceedings, CUPE has organized to curtail electronic surveillance and monitoring of workers and to safeguard the personal information of all residents of Canada from private interests.

Issue 1: Equal weight given to individual privacy and commercial interests

CUPE recognizes the amendment proposed by Minister Champagne to explicitly acknowledge the fundamental right to privacy in section 5 of the CPPA.[1] However, the "purpose" of the CPPA remains flawed as it places an individual's right to privacy and commercial interests on the same footing. An individual's right to privacy must supersede commercial interests.

Recommendation: Amend the purpose of the CPPA to explicitly recognize privacy as a fundamental right that prevails over commercial interests.

Issue 2: Businesses given carte-blanche for personal data

Under the proposed CPPA, organizations themselves are to determine whether the manner and purposes of collecting, using, or disclosing personal information are appropriate. The factors to consider include "whether the purposes represent legitimate business needs of the organization" [s 12(2)(b)], "the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs" [s 12(2)(c)] and "whether the individual's loss of privacy is proportionate to the benefits in light of the measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual" [s 12(2)(e)]. Missing from this list is consideration of an individual's right to privacy. Moreover, not only is "legitimate business need" not defined, but this entrusts businesses to decide whether a loss of privacy is permissible. Problems with self-regulation are well-known. Private actors with profit motives will prioritize commercial interests over societal considerations like safety, economic security, and human rights.

[1] Champagne, F. P. (2023, October 20). *Correspondence from the Honourable François-Philippe Champagne - 2023-10-20, Minister of Innovation, Science and Industry.* House of Commons. https://www.ourcommons.ca/DocumentViewer/en/44-1/INDU/related-document/12633023

Recommendation: Amend section 12 to include an individual's right to privacy as a factor that must be considered when determining appropriate purposes of the collection, use or disclosure of personal information. Define what is a reasonable "legitimate business need".

Issue 3: Dangerous exceptions to requirement for consent

The CPPA creates a new exception that allows for the collection, use, or disclosure of personal information without the individual's knowledge or consent if it is for the purpose of a "business activity". The list of business activities includes "an activity that is necessary for the organization's information, system or network security" [s 18(2)(b)] and "an activity that is necessary for the safety of a product or service that the organization provides" [s 18(2)(c)] and "any other prescribed activity" [s 18(2)(d)]. CUPE is concerned that these exceptions to consent are overly nebulous and could be exploited, leading to privacy abuses. This exception to consent for "business activity" is not in the Personal Information Protection and Electronic Documents Act, the existing federal law that regulates how businesses handle personal information.

Even more vague is the exception to consent "for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual" [s 18(3)]. The legislation once again leaves it up to the private organization to make this calculation on its own. There is also no requirement for the organization to be transparent with affected individuals about the fact that an exception to their consent has been engaged. In CUPE's view, an organization's interest in the collection, use, or disclosure of personal information must always be superseded by an individual's right to privacy.

CUPE is also opposed to the exception which allows an organization to transfer personal information to a service provider without individuals' knowledge or consent. Workers must be informed and provided an opportunity to consent to their personal information being transferred to a service provider, which may include contractors or subcontractors with whom the individual has no direct relationship and third-party corporations based in other jurisdictions.

Consent is fundamental to privacy. Any exceptions to consent for data use and collection of personal data must be tightly regulated and need to be exclusively in the public interest. These three exceptions prioritize commercial interests over the right to privacy and human autonomy.

Recommendation: Remove the exceptions to consent for business activities, legitimate interest, and transfer to service provider.

<u>Artificial Intelligence and Data Act</u>

Artificial intelligence (AI) will soon permeate every sector and industry and impact nearly every job classification. CUPE members, including those in the municipal, health, communications, and port sectors, are already experiencing applications of AI in their workplaces. CUPE has seen that the adoption of AI has had significant implications for job design, workers' privacy, human resources decision-making (e.g. hiring, discipline), and public service delivery.

CUPE has been attentive to technological change in our workplaces and public services since our founding 60 years ago. CUPE's concerns with the use of artificial intelligence, as with all new technologies, are the protection of workers' rights, ensuring economic prosperity for the working class, and enhancing public services.

Whether AI will improve our standard of living significantly depends on the legislation that governs its deployment. A legislative framework that bends toward the profit-maximizing interests of AI developers and managers or fails to require the necessary safeguards to mitigate harm, could be disastrous for Canadian society. In CUPE's view, the consequences of getting this wrong could include the widespread violation of privacy and human rights, depressed wages, proliferation of precarious work and job displacement, job losses, exacerbated income inequality, cuts to public services, perpetuation of historical biases and discrimination, aggravated disinformation campaigns and manipulated content, and the loss of human autonomy.

Unfortunately, the proposed Artificial Intelligence and Data Act (AIDA) – the Government of Canada's first attempt to regulate artificial intelligence – fumbles the opportunity. CUPE acknowledges Minister Champagne's extensive proposed amendments sent to the committee on November 28, 2023, in response to widespread stakeholder criticism of the initial scant drafting of the legislation. Minister Champagne's amendments could be characterized as an attempted rewrite, as the proposed amendments are longer than the original Act. The vast majority of the INDU committee's witnesses and briefs occurred before Minister Champagne submitted extensive proposed amendments. The Committee should allow sufficient time for stakeholders to analyze and provide additional commentary on these new amendments. Still, what is before the committee is a deeply flawed legislative framework on a pivotal matter for all Canadians.

Issue 1: Non-application to the federal government

One of the most egregious issues with the proposed legislation is that it does not apply to any government department, ministry, institution, or Crown corporation [s 3(1)]. Further, non-application extends to "a product, service or activity that is under the direction or control of the Minister of National Defense; the Director of the Canadian Security Intelligence Service; the Chief of the Communications Security Establishment" [s 3(2)]. The near-total exemption of the federal government is far beyond that of the European Union's Artificial Intelligence Act, which limits non-application to AI systems developed or used exclusively for military purposes.[2]

In our view, the highest-impact AI systems with the greatest risk of serious harm would be those deployed in the public sector. For example, AI systems could be deployed to make decisions or recommendations related to defense and the military, the provision of income supports, taxation, energy regulation, refugee claims, and transportation safety. In a November 28, 2023, letter to INDU, Minister Champagne has made limited concessions on this point.

[2] (2023, October 20). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

The Minister stated, “If a high-impact system is made available in the course of international and interprovincial trade for use by police, courts or healthcare authorities, then the AIDA will apply.”[3] In our view, any and all situations concerning access to, or delivery of public services should be classified as high impact and subject to AIDA.

With a sweeping non-application clause in the AIDA, the federal government is setting a double standard for protection, ethical use, and accountability. Rather than lead by positive example, the federal government is setting a dangerous precedent for provincial governments who will also inevitably develop legislation to regulate AI. Rather than subject the government to the law, the Treasury Board Secretariat has penned a “Directive on Automated Decision-Making” internal policy and a voluntary guidance document entitled “A Guide on the Use of Generative AI,” both with limited enforceability, recourse, and accountability.

Recommendation: The AIDA should apply to all government institutions, and all matters of access or delivery of public services should be classified as high impact.

Issue 2: Limited definition of harm

Harm is only defined on an individual level in the AIDA [s 5(1)]*:*

(a) physical or psychological harm to an individual;
(b) damage to an individual’s property; or
(c) economic loss to an individual.

There is no mention of collective or societal harm in this definition or the stated purposes of the Act [s 4(b)]. In CUPE’s view, harm to the environment, democracy, human rights, critical infrastructure, and more could all be omitted in the risk management requirements because of this overly narrow definition in the legislation. Minister Champagne chose not to propose any amendment to the definition of harm, ignoring the calls of many stakeholders.

Recommendation: Expand the definition of harm and the purposes of the Act to include collective and societal harm.

Issue 3: Lack of independence for Artificial Intelligence and Data Commissioner

The Act allows the Minister to designate a senior official of Innovation, Science and Economic Development Canada (ISED) to be the Artificial Intelligence and Data Commissioner (AIDC), tasked with administering and enforcing the Act. It would be inappropriate for a commissioner tasked with supervision and regulatory oversight of AI systems to be housed within ISED. ISED’s mandate includes improving conditions for investment and helping businesses grow.[4] As proposed, there is a risk of undermining public trust in the commissioner and raising the potential for conflicts of interest. Like other commissioners, the AIDC should be appointed by the Governor in Council after consultation with the leaders of every recognized party in the Senate and House of Commons and report directly to Parliament. Minister Champagne has

[3] Champagne, F. P. (2023, November 28). *Correspondence from the Honourable François-Philippe Champagne, Minister of Innovation, Science and Industry - Amendments to AIDA*. House of Commons. https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/
[4] Innovation Science and Economic Development Canada. (2010, April 19). *Mandate* [About Us]. https://ised-isde.canada.ca/site/ised/en/about-us/our-organization/mandate

acknowledged concerns with the proposed design of the AIDC.[5] Still, the Minister's proposed amendments fail to provide the necessary arms-length distance from ISED.

Recommendation: The AIDC should be an independent officer of Parliament.

Issue 4: Missing "high-impact" classes and unacceptable risk category

Minister Champagne proposes an amendment to define a "high-impact system" as one of seven classes in a newly-created schedule, amendable by regulation. In our view, several additional classes of high-impact systems have been overlooked, including AI systems in telecommunications, education, housing, critical infrastructure, transportation, immigration, and border security.

Unlike the EU AI Act, the AIDA does not contain an "unacceptable risk" category for AI systems. In CUPE's view, this is a mistake. Certain AI systems ought to be banned. Banned applications in the EU AI Act include cognitive behavioural manipulation, untargeted scraping of facial images, emotion recognition in the workplace and educational institutions, social scoring, and biometric identification and categorisation of people.[6] Notably, Canada's proposed AIDA would permit AI systems to process biometric information as a "high impact" system whereas this is prohibited under the EU AI Act. The Office of the Privacy Commissioner defines biometric information as "people's physical and behavioural attributes, such as facial features, voice patterns, fingerprints, palm prints, finger and palm vein patterns, structures of the eye (iris or retina), or gait".[7] Subject to the regulatory requirements of high-impact systems, Minister Champagne's amendments would allow AI technologies to identify individuals based on their biometric information and assess their behavior or state of mind.[8]

Recommendation: Expand the classes of high-impact systems to cover all public services and create an unacceptable risk category to prohibit certain AI systems

Issue 5: Lacking protections for workers' rights

Under the Minister's proposed amendments, the use of AI systems in "matters relating to determinations in respect of employment" would be rightly classified as high impact because these systems could impact workers' livelihoods, and right to privacy.[9] Class 1 should be amended to include task allocation, monitoring, and evaluation. This is a more comprehensive definition of the ways in which AI systems can impact employment and would make the classification consistent with the EU AI Act.

---

[5] Champagne, F.-P. (2023, October 3).
[6] (2023, December 9). *Artificial Intelligence Act: Deal on comprehensive rules for trustworthy AI*. New European Parliament. https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai
[7] (2011, February 1). *Data at Your Fingertips Biometrics and the Challenges to Privacy*. Office of the Privacy Commissioner. https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/
[8] Champagne, F.-P. (2023, November 28).
[9] *Ibid*.

Obligations related to the operationalization of AI systems must include a requirement to consult impacted workers and their unions before the introduction of AI systems in their workplaces or in any way that will affect their jobs, privacy, or personal data. This fundamental protection for workers is enshrined in the EU AI Act.[10] Employers ought to be required to disclose to workers and their unions any contracts with third parties for AI systems. This is necessary to ensure workers have a clear understanding of the AI technologies being implemented in their workplaces. Moreover, it ensures that unions can engage in discussions about the impact of AI technologies on employment conditions in an informed way. If a collective agreement is in force, the use of AI systems should be negotiated prior to the implementation of new technology.

Lastly, the AIDA would better fulfill its purpose with a whistleblower protection clause for workers involved in the design, development, and deployment of AI. Whistleblowers should be encouraged to report instances of misconduct, unethical decision-making, or violations of the Act without fear of reprisal. Often whistleblowers bring issues to light that allow for early intervention to address problems before they escalate. This is especially important in a legislative regime like the AIDA which is based on industry self-reporting.

Recommendation: Amend Class 1 high-impact systems to include task allocation, monitoring, and evaluation. Require that workers and their unions be consulted when AI systems are deployed in the workplace or in any way affecting their jobs, privacy, or personal data. Add whistleblower protection.

EN:cc/cope491

[10] European Trade Union Confederation. (2023, June 14). *AI: Parliament protects workers' rights – but new directive needed* [Press Release]. ETUC | European Trade Union Confederation. https://www.etuc.org/en/pressrelease/ai-parliament-protects-workers-rights-new-directive-needed