Written submission to the *2026 Review of the Privacy Act: Policy Approaches*

July 10, 2026

Introduction

We welcome the opportunity to provide comments on the Treasury Board of Canada Secretariat's ***2026 Review of the Privacy Act: Policy Approaches*** paper ("the paper")***.*** These submissions are made by ***an ad hoc working group*** composed of labour and labour lawyers, academics, trade union representatives, and labour movement leaders. Ad hoc working group members are listed in Appendix A of this submission.

Our members bring diverse professional and practical experience representing workers, advising bargaining representatives, conducting research on privacy and labour relations, and advocating for fair and equitable workplaces. While we do not speak on behalf of any single organization, we share a common interest in ensuring that Canada's federal privacy framework adequately protects workers in the face of rapidly evolving technologies and data practices.

We support the comprehensive review of the *Privacy Ac*t ("the Privacy Act" or "the Act") and welcome the Government's recognition that technological developments continue to expose gaps in the existing legislative framework. We also appreciate the opportunity to provide comments on policy themes that have been the subject of previous consultations by the government and the privacy commissioners, particularly given the pace at which technologies, data practices, artificial intelligence systems, and workplace surveillance tools continue to evolve.[1]

Changing data and privacy practices in federal workplaces

In the federal workplace context, the proposed reforms arrive at a time when federal institutions increasingly rely on digital systems and automated decision-making systems, including Artificial Intelligence (collectively "digital systems") to collect, analyze, and act on worker information. The use of digital systems in connection with personal information is the common structure underlying most of the proposals in the paper. We take this underlying structure as a given, and we take it as a fundamental principle that these systems must be subject to ***continuing governance*** as opposed to one time compliance obligations.

Advances in workplace monitoring, algorithmic management, artificial intelligence, and automated decision-making systems have significantly expanded the volume and sensitivity of personal information collected about workers. While the use of these new technologies may offer seemingly efficient and productive workplaces, they also create new risks to workers' fundamental rights including privacy, equity, equality (including bias, discrimination, and assumptions), autonomy, dignity, and procedural fairness. In our view, modernization of the *Privacy Act* should respond to these realities by establishing clear, enforceable protections that ensure workers retain meaningful privacy rights in the modern workplace.

---

[1] Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight. "Protecting Worker Privacy in the Modern Workplace." Oct. 2023, Québec, QC. https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_02/; Office of the Privacy Commissioner of Canada. (2008, March). *Radio Frequency Identification (RFID) in the Workplace: A Consultation Paper on Recommendations for Good Practices*. Ottawa, ON: Office of the Privacy Commissioner of Canada Online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/rfid/

Recent Supreme Court of Canada jurisprudence under section 8 of the Charter has significantly expanded constitutional protection for informational privacy, particularly in digital environments. The Court has increasingly recognized that privacy harms arise not merely from isolated disclosures of personal information, but also from the aggregation, analysis, and inferential capabilities of modern data systems.[2]

Further, there is a growing body of both Canadian and non-Canadian policy and academic research examining the expansion of workplace surveillance during and after the COVID-19 pandemic.[3] For example, a 2021 report documented how remote-work technologies enabled new forms of worker monitoring and highlighted significant gaps in existing privacy and employment law protections.[4] More recently, a survey of Canadian employers found that the use of worker monitoring technologies ("bossware") expanded significantly alongside remote work, with employers increasingly relying on tools such as time tracking, website monitoring, and keystroke logging. The study concludes by noting that "while these technologies might be justified on rationalized grounds of 'care' for the wellbeing of workers, they also find direct use for coercive control and disciplining of worker behaviours."[5]

In our view, the proposed reforms should include explicit statutory protections governing worker surveillance, algorithmic management, workplace analytics and automated decision-making affecting federal workers. Absent such protections, the proposed changes particularly the cross-system data integration within federal public sector risks facilitating data practices that are inconsistent with evolving constitutional privacy principles and the fundamental values that underpin democratic governance and individual and collective rights.

The proposed reforms also arrive as federal institutions increasingly rely on digital systems to collect, process and act on the information of public service users. The use of automated decision-making systems in public services might offer the allure of efficient public service delivery, but also increase risks to the fundamental rights of public service users including equity, equality, dignity and procedural fairness. Many public sector automated decision systems have been challenged, paused, withdrawn, or subjected to major remediation, and/or subsequently cancelled after causing or risking harm to public service users[6]. The updated

---

[2] See: *York Region District School Board v. Elementary Teachers' Federation of Ontario*, 2024 SCC 22 (CanLII), Referencing the SCC's decision in Cole, the SCC at para 140 held that the information in "Internet-connected devices, normatively, tends to reveal one's "specific interests, likes, and propensities", and as such it is "at the very heart of the 'biographical core' protected by s. 8".

[3] Bernhardt, Annette, Lisa Kresge, and Reem Suleiman. *Data and Algorithms at Work: The Case for Worker Technology Rights*. UC Berkeley Labor Center, 3 Nov. 2021, ; Aloisi, A., & De Stefano, V. (2022). Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon. International Labour Review, 161(2), 289-314. DOI: 10.1111/ilr.12219; Moore, Phoebe V et al. *Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations*. Luxembourg: Publications Office of the European Bargaining representative, 2021.

[4] Masoodi, M.J., Abdelaal, N., Tran, S., Stevens, Y., Andrey, S. and Bardeesy, K. (2021, September). "Workplace Surveillance and Remote Work: Exploring the Impacts and Implications Amidst Covid-19 in Canada." Retrieved from https://www.cybersecurepolicy.ca/workplace-surveillance;

[5] Thompson, Danielle E., and Adam Molnar. "Workplace Surveillance in Canada: A Survey on the Adoption and Use of Worker Monitoring Applications." *The Canadian Review of Sociology*, vol. 60, no. 4, 2023, pp. 801–19, https://doi.org/10.1111/cars.12448.

[6] Redden, J., Brand, J., Sander, I., Warne, H., (2022, September). "Automating Public Services: Learning from Cancelled Systems." Retrieved from https://carnegieuk.org/wp-content/uploads/2024/10/Automating-Public-Services-Learning-from-Cancelled-Systems-Final-Full-Report-2.pdf

Privacy Act should respond to these risks by establishing clear, enforceable protections to protect the rights of public service users.

For each proposed reform addressed in this submission, we have adopted a consistent structure. We begin by summarizing the proposed reform, followed by an analysis of our concerns from a worker and workplace privacy perspective. We then identify key questions that, in our view, require further consideration by the Government, and conclude with specific recommendations intended to strengthen the proposed framework and better protect the privacy rights of workers. We offer these comments with the objective of enhancing transparency, accountability, and meaningful privacy protection while supporting legitimate operational needs within federally regulated workplaces and the federal public sector.

Privacy protections must encompass the collection, analysis, processing, use and sharing of personal information. They must encompass meaningful procedural provisions as described in these submissions. At the same time, they must also recognize and incorporate the full protections offered by collective bargaining and collective agreement administration, and not be exempt from them. Where collective agreements provide protections that exceed the requirements of the *Privacy Act*, those enhanced protections should be maintained and respected. The two systems, privacy and collective bargaining, must be mutually reinforcing of the protections they offer.

Privacy is a fundamental right. The right to be free from discrimination is a fundamental right. The right to free collective bargaining and to strike are fundamental freedoms. These are all protected by the Charter of Rights and Freedoms. Any review and revision of the *Privacy Act* which touches on workers and their employment, must be informed by and conform to these principles.

Theme 1: Enabling integrated services: only with advice and explicit consent

Proposal 1: Government-wide data sharing — purpose-based approach to data sharing

This proposal would allow the broader sharing and reuse of personal data across government organizations and programs without requiring consent when it is deemed necessary for public purpose or program delivery. It is unclear how worker personal data would be treated under this new proposed change.

Concerns

The Canadian government is not simply a service provider. It is also Canada's largest single employer. A data sharing regime that may (or may not, see other concerns and recommendations in these submissions) be appropriate for delivery of public services raises very different concerns when the same personal information can affect an individual's employment, discipline, discharge, accommodation, security clearance, career progression, or personal financial situation.

Proposal 1 and Proposal 2 are two aspects of the same structural issue. Proposal 1 asks "who may share the data?". Proposal 2 asks "what becomes the authoritative source of that information?" and also "what are permissible sources of data that will be tied to employment?".

Together they create the possibility of a government-wide dossier that both potentially draws on non-employment related government information (personal financial and tax information, individual use of government services, status under different government regimes such as immigration and employment insurance) and also follows a worker throughout their career. Even if that is not the government's intention, the legislation should be drafted to prevent that outcome.

Clarification is needed on how the government plans to treat federal workers' data under this new proposed plan. Wider circulation of worker information across the government may dissolve the boundaries between 'ordinary' data related to work and 'sensitive data' related to their personal situation, including their personal health data, behavioural data, biometric/security data, and their human resource personnel file, including any discipline or discharge file.

For reference, see: Standard personal information banks.

Questions

Will the new proposed plan to share and reuse personal data extend to federal workers' personal data? If so, what specific limits and oversight mechanisms will be put in place to ensure federal workers' personal information is shared responsibly across government institutions?

Will additional protections be established for sensitive employment-related information (i.e., performance evaluations, attendance records, disciplinary files, and accommodation requests)? How will workers be able to challenge, correct, or seek redress if their personal information is reused or shared inappropriately or results in adverse employment consequences?

Recommendations

- Recognize as a core principle informing all legislation and protections enacted in this domain of privacy, that worker and/or bargaining representative consent alone is not sufficient for the collection use, disclosure, sharing, or repurposing of workplace data because of the inherent power imbalance in the employment relationship. There must be meaningful legislative provisions for notice (including the content and the purposes for which the information is intended to be used), informed consent including the ability to withhold consent, challenge, appeal, and redress, all including human review, all capable of being invoked by individual workers and their bargaining representatives (collectively "meaningful procedural protections").
- Exclude employment records by default from government-wide purpose-based sharing unless expressly authorized by legislation.
- Where legislation purports to authorize purpose-based sharing of worker information, such legislation must:
    - demonstrably conform to sections 7, 8 and 15 of the Charter of Rights and Freedoms;
    - demonstrably conform to the *Canadian Human Rights Act*;
    - demonstrably conform to the privacy rights proposed to be embedded in the amendments to the Act;
    - demonstrably conform to procedural fairness;
    - require comprehensive privacy impact assessments, expressly incorporating Gender Based Analysis+ and Equity Impact Analysis, subject to oversight, as set out below before implementation;
    - be subject to oversight by a designated agency or office with a clear mandate, authority, definitions of necessity and proportionality, and powers, including the power to prohibit the collection, sharing and use of worker information where circumstances warrant. In this regard see recommendations under Proposals 15, 19, 20, and 22;
    - require necessity and proportionality tests/justification before any worker information may be shared across institutions — such justification to be subject to publication, review, oversight and challenge by affected workers and/or their bargaining representatives, before any implementation. Such justifications must include consideration of less intrusive alternatives and there must be evidence-based decision-making that the anticipated benefit outweighs the potential harm to privacy, equity, and procedural fairness before such information sharing is authorized to occur;
    - create a special category for sensitive worker information, including health information, accommodation records, discipline and discharge, security screening, biometrics, investigations, performance management, sensitive personal financial information; such category to be subject to either complete exclusion or more stringent safeguards and legislative provisions for workers and/or their bargaining representatives to know of and challenge the collection, analysis, processing, use and sharing of the information;

- provide transparency rights to affected workers and/or their bargaining representatives, including notice of collection of personal data, sensitive data and interdepartmental sharing, and a record of what information is being collected and/or disclosed; such information to be subject to legislative provisions for workers and/or their bargaining representatives to know of and challenge the collection, analysis, processing, use and sharing of personal data;
- create review and correction rights, allowing workers and/or their bargaining representatives to challenge inaccurate or inappropriate collection, analysis, processing, use and sharing before data is used for any purpose, and in particular for purposes involving adverse employment consequences;
- prohibit secondary use of employment data for unrelated human resources or disciplinary purposes unless expressly authorized by law and subject to legislative provisions for workers and/or their bargaining representatives to know of and challenge such secondary use of personal data;
- enact corresponding public law safeguards to address the risks of data re-sharing to the public, either by prohibiting data re-sharing completely, or through clear restrictions on data use and re-sharing beyond the intended use. Any use or re-use of data must conform with ss. 7, 8, and 15 of the Charter and any other relevant legal protections. Any use or re-use must be subject to the same robust meaningful procedural provisions as the original use.

Proposal 2 — Official Sources of Government Digital Data

This proposal requires all programs to obtain personal data from designated official sources rather than collect it again.

Concerns

It remains unclear how a centralized or polycentric government data-sharing framework would operate in federal workplaces. For example, would employment-related decisions such as hiring, promoting, disciplining and termination of workers be subject to this expanded data-sharing regime? The proposal is unclear with respect to how issues related to data accuracy, accountability, and security will be handled by the government. Clarification is needed.

Questions

How will the government ensure that personal information is accurate, up-to-date, and used only for appropriate and intended purposes? What safeguards will be implemented to protect what could become a vast, interconnected database of worker and citizen information collected at different times and for different purposes, particularly where individuals have not consented to interdepartmental, intergovernmental, or interministerial sharing?

Recommendations

- Recognize as a core principle informing all legislation and protections enacted in this domain of privacy, that worker and/or bargaining representative consent is not sufficient for the collection, use, disclosure, sharing, or repurposing of workplace data because of the inherent power imbalance in the employment relationship.
- Ensure there are meaningful procedural provisions.
- Exclude employment-related records and decision-making, especially (but not limited to) algorithmically supported decision — making, from any mandatory centralized data-sharing regime unless such sharing is expressly authorized by legislation, demonstrably necessary and proportional, and accompanied by appropriate procedural safeguards. See recommendations under Proposal 1 in this regard.
- Ensure that any "official source" of personal information is subject to rigorous data governance standards, including requirements that information be accurate, current, complete, and regularly reviewed. Workers and/or their bargaining representatives should have a timely and accessible right to review, correct, and challenge inaccurate information before it is relied upon in any decision affecting their rights or employment.
- Prohibit the use of information collected for one purpose from being repurposed for unrelated employment, disciplinary, performance management, or security decisions unless expressly authorized by law and demonstrably necessary and proportionate.
- Require comprehensive privacy impact assessments before establishing or expanding centralized data repositories, with particular attention to the risks of aggregation, function creep, cybersecurity, and unauthorized secondary use.

- Ensure such centralized data repositories and their functions are subject to oversight by a designated agency or office with a clear mandate, authority, definitions of necessity and proportionality, and powers, including the power to prohibit and/or curtail the scope of such centralized data repositories. See recommendations under Proposal 1 in this regard, as well as recommendations under Proposals 15, 19, 20, and 22.
- Access to centralized government data should be governed by strict role-based access controls, comprehensive audit logging, and independent oversight to ensure that personal information is accessed only by those with a legitimate operational need.
- Notify workers and/or their bargaining representatives where centralized government databases contain worker information and significant new categories of data sharing are to be implemented. Ensure they have access to meaningful procedural provisions, especially where inaccurate or improperly shared information can result in adverse employment consequences. See recommendations under Proposal 1 in this regard.
- Recognize in the Act that while reducing duplicate collection of information may be a legitimate administrative objective, efficiency should not override fundamental privacy rights, Charter and human rights, procedural fairness, or the distinct legal obligations owed by the Government in its capacity as Canada’s largest employer.

Proposal 3 — Mandatory Privacy Impact Assessment

This proposal would make Privacy Impact Assessments (PIAs) a legal requirement whenever personal information is used to make decisions about individuals, including federal workers. For federal workers, this could provide greater transparency and accountability by requiring departments and agencies to assess and mitigate privacy risks before implementing new workplace programs, technologies, or data-driven decision-making processes that affect employment.

The Ad Hoc Working Group agrees with this Proposal. We welcome the mandatory legal requirement for PIAs.

Concerns

The proposed trigger for PIAs is event-based, and assessments would not be required on a periodic or continuous basis. Anything AI-driven is not static. AI-enabled digital systems are inherently dynamic. Their operation may change over time through software updates, retraining, changes to underlying datasets, evolving deployment contexts, or modifications to system parameters. Additionally, the evolution of AI systems and machine learning can alter the way these technologies operate. There could be unplanned, unnoticed or unanticipated changes over time, where the AI gradually shifts in the way it assesses, reasons and makes decisions. This is due to its underlying algorithmic structure which is based on probabilities rather than certainties. These constitute reasons for ensuring that AI systems are assessed at regular intervals and as needed rather than a single evaluation at implementation and when modified. There is a concern that PIAs are only required when personal information is used to make a decision about someone. PIAs are an essential tool for federal institutions to consider the risks associated with the collection, analysis, use, sharing and retention of personal data and they foster a culture of data minimization.

Questions

Will Privacy Impact Assessments (PIAs) be mandatory for all workplace digital systems and other technologies that collect, monitor, analyze, use or share worker data, including surveillance, productivity monitoring, and AI-driven decision-making systems?

Recommendations

- Make Privacy Impact Assessments a mandatory legal requirement whenever personal information is collected or used to make decisions affecting individuals. PIAs must be required for all uses of AI involving personal information, including where an individual's data is used to train, test, profile, categorize, risk rank, or inform broader institutional and/or program decisions, even if the individual is not the direct subject of the final decision or outcome.
- Recognize in the Act that AI-enabled and other data-driven digital systems are dynamic rather than static. For digital systems that collect, monitor, analyze, use, share or make

recommendations using personal information, a single PIA at implementation is insufficient. Therefore:

  - Require periodic review and updating of PIAs throughout the lifecycle of AI-enabled digital systems and other high-risk technologies.
  - Review PIAs whenever there is a significant change to the system, its underlying data, its intended purpose, or its decision-making functions, and at regular prescribed intervals even where no major changes have been identified.
  - Treat a PIA as a continuing governance obligation rather than a one-time compliance exercise.
- Expressly require PIAs for workplace technologies that collect, monitor, or analyze worker information, including productivity monitoring systems, surveillance technologies, automated decision-making tools, and AI systems that influence hiring, promotion, performance management, discipline, accommodation, or termination decisions.
- Expressly require that PIAs should assess privacy risks, and the potential impacts on constitutional rights, human rights, procedural rights, algorithmic bias, data accuracy, transparency, and workers' ability to understand and challenge decisions made or informed by digital systems.
- Require departments and agencies as part of the development of PIAs, to consult and work with affected workers and bargaining representatives in the development of the PIA, to occur before implementing digital systems and other high-risk workplace technologies that rely on personal information.
- Make significant PIAs publicly available, subject only to legitimate security or confidentiality limitations.

Theme 2: Enhancing accountability and transparency

Proposal 5 — Transparency requirement for AI and Automated Decision-Making Systems

This proposal would require federal institutions to inform individuals when AI or automated decision systems are used in a decision that affects them and explain how the decision was made and what personal data was used. Individuals can review the accuracy of their information, request corrections where needed, and seek a human review if they believe the system made an error or relied on incomplete or incorrect data. These requirements would apply only where automated decision systems (ADS) are used to make or support decisions that directly affect a person's access to services, benefits, or legal rights.

Concern

The use of digital systems including automated decision systems and AI (ADS/AI) is a significant concern for federal workers. ADS/AI systems are often opaque and make it difficult for workers to understand how decisions are reached or to effectively challenge errors. Transparency alone will not solve this issue. Existing transparency legislation has already proven to be inadequate to ensure that workers understand what digital systems are used and how. Relevant to this proposal and to Proposal 6, in addition to the need for legislative requirements pertaining to information sharing, the government must take steps to promote democratic participation within the workplace and to ensure that workers and their bargaining representatives are consulted and meaningfully involved in the consideration, development, introduction and use of AI and Automated Decision-Making Systems.

Questions

Will this requirement be for all employment-related decisions affecting federal workers, including hiring, promotion, discipline, accommodation, security clearance, and termination decisions? What safeguards will be implemented to detect and prevent bias or discriminatory impacts when ADS/AI are used in workplace decision-making? What recourse and redress are available for workers? Are review mechanisms accessible to workers? If yes, will these review mechanisms provide full appeal rights to ensure principles of procedural fairness, natural justice, and Charter and human rights are upheld? Will bargaining representatives or bargaining representatives be consulted before ADS/AI are introduced in federal workplaces?

Recommendations

- Require transparency whenever ADS/AI are used to make or materially influence decisions affecting individuals. The overriding principle should be that workers and/or their bargaining representatives have access to timely and effective remedies where an AI-assisted decision is contested as inaccurate, procedurally unfair, discriminatory, or based on inappropriate use of personal information. Acknowledge though that transparency alone is not sufficient to ensure fairness, accountability, or compliance with administrative law and human rights obligations.

- Expressly apply the following legislated requirements to the use of AI or automated employment-related decision-making systems which affect federal workers, including about recruitment, hiring, promotion, performance management, discipline, accommodation, security clearances, workforce management, and termination of employment:
  - Ministries, departments and other government organizations should consult and work with affected workers and bargaining representatives before introducing ADS/AI that monitor workers or influence employment-related decisions. Meaningful consultation should occur early enough to influence system design, implementation, and governance.
  - Where AI or automated systems are used to make, support or influence employment decisions, workers and/or their bargaining representatives should have the right to:
    - be informed that AI or automated decision-making will be used;
    - receive a meaningful, accurate and verifiable explanation of how the system contributed to the decision;
    - know what personal information was relied upon;
    - correct inaccurate or incomplete information before a final decision is made;
    - request meaningful human review by a decision-maker with authority to reconsider the outcome, including being provided with the reviewer's name, position and scope of authority for review.
    - Contest the results of such decision-making through a clear and transparent system informed by the principles of natural justice and fairness, to be either embedded in legislation (for non-represented workers) or mandatory contract provisions subject to grievance and arbitration provisions (for represented workers), with full appeal rights.
- Prohibit federal institutions legislatively from relying primarily on automated decision-making for employment decisions that significantly affect a worker's rights, livelihood, or career progression. Meaningful human oversight must remain mandatory.
- Require federal institutions to conduct regular independent testing and auditing of AI systems for accuracy, bias, discrimination, and disproportionate impacts on protected groups, with appropriate public reporting on the results, and appropriate mechanisms of review and redress for individuals impacted where such impacts are identified. Errors made because of such impacts must be subject to meaningful correction, especially for impacted individuals.

Proposal 6 — Notice Requirement

This proposal makes privacy notices explicit by requiring them to be written in plain language, made it easier to find, and published in a centralized registry so individuals can understand how their personal data is used and shared. It would also require notice when AI enabled automated decision systems (“ADS/AI”) are used to make or support decisions affecting individuals.

Concern

Notice alone will not satisfy the requirement of informed consent. Any framing of notice alone as implied consent risks weakening federal workers’ privacy protections and could be viewed as a form of coerced consent, especially in workplace settings where participation is not optional.

Question

How will the government ensure that privacy notices are understandable and consistent across departments and agencies, given the technical complexity of many programs and AI/ADS tools?

Will federal workers have the ability to meaningfully challenge or seek clarification if they believe the privacy notice does not accurately reflect what of their data and how their data is being used?

What safeguards will ensure that exceptions to providing notice remain narrow, justified, and subject to independent oversight?

Recommendations

- Recognize as a core principle informing all legislation and protections enacted in this aspect of privacy protection, that notice alone is an insufficient safeguard and must be accompanied by meaningful procedural provisions regarding individual protection.
- Specify in the Act that notice alone will not replace the standard of informed consent.
- Ensure exceptions to providing notice must remain narrow, justified and subject to independent oversight.
- Notification of workers and their bargaining representatives must occur *before* workers’ personal data is used in AI/ADS systems in employment contexts. Notice beforehand should also be required for the use of AI/ADS in public service delivery.
- The *Privacy Act* should establish a minimum baseline of privacy protection and notice requirements for federal workers. Where collective agreements provide protections that exceed the requirements of the Act in terms of notice and consultation, those enhanced protections should be maintained and respected.
- Specify in the Act what information must be included in the notice, including the personal data collected, how the personal data will be used, the purpose for collecting the data, what person or department/agency is responsible for oversight of the data, where the data will be stored, how often the data will be reviewed, how long the data will be stored, and when the data will be destroyed.
- Specify in the Act what information must be included in the notice when AI/ADS is being used, including the personal information used to make the decision, the nature, purpose and

scope of the decisions for which the AI/ADS will be used, the logic and key parameters that affect the output of the AI/ADS, the types of outputs the AI/ADS will produce, the individual, vendor or entity that created the AI/ADS, and that workers have the right to appeal the decision and correct the data used by the AI/ADS to make the decision.

Theme 3: Advancing safeguards across the spectrum of data sensitivity

Proposal 7 — Recognize a spectrum of data sensitivity and identifiability in law

This proposal would recognize that different types of personal information require different levels of protection based on their sensitivity and how easily they can be linked to an individual. Sensitivity refers to how harmful it could be if the data were exposed or misused.

Concerns

While the proposal recognizes sensitive data requires stronger protections, it does not clearly limit the collection, analysis, processing, use, or sharing of highly sensitive worker information. Furthermore, the proposal does not outline a comprehensive list of what would constitute sensitive data and excludes mention of such criteria as gender identity, other human rights protected identities, and membership in a trade union or other bargaining representative organization.

Questions

Will worker-specific information including health records, accommodation requests, biometric data, disciplinary files, security clearance information, bargaining representative membership, and equity and diversity information be explicitly recognized as sensitive personal information requiring enhanced protections?

What restrictions will apply to the collection, analysis, processing, use, sharing, and retention of sensitive worker data, and will workers be notified when such information is disclosed or used for purposes beyond its original collection? How will the government prevent de-identified worker data from being re-identified, combined with other datasets, or used to create worker profiles for workforce analytics, performance management, disciplinary or other purposes?

Will bargaining representatives be consulted before departments or agencies introduce new technologies or programs that collect, analyze, process, use or share sensitive worker information, including biometric, behavioural, or demographic data?

What additional remedies and accountability measures will be available when a breach of privacy rights involves sensitive worker information, particularly where the breach could affect a worker's employment, reputation, security clearance, human rights, or security of the person?

Recommendations

- Recognize as a core principle informing all legislation and protections enacted in this aspect of privacy rights, that information does not need to be labelled as sensitive before it has the potential to create harm. Information such as attendance, leave, and accommodation requests should automatically be considered sensitive as a precautionary principle. However, even information that is not so categorized can create individual by revealing or implying the existence of, nature of, and/or the details of an individual's personal circumstances. All personal information must therefore be acknowledged and assessed through the lens of its sensitivity. Failure to do so can lead to breaches of privacy protections, the *Canadian Human Rights Act*, as well as the Charter of Rights.

- Create a special category for sensitive worker information that is subject to the most stringent safeguards. Specific prohibitions and restrictions should apply to the collection, analysis, processing, use, sharing, and retention of this sensitive worker data.
- Strictly limit the collection, use, retention, and sharing of sensitive worker data.
- Explicitly recognize worker-specific information including health records, accommodation requests, biometric data, disciplinary files, security clearance information, bargaining representative membership and equity and diversity data as sensitive personal information requiring enhanced protections.
- Prohibit the collection, use and processing of highly sensitive and invasive worker data including biometric data and technologies including facial recognition and emotion recognition.
- Notify workers and their bargaining representatives when sensitive worker data is disclosed or used for purposes beyond its original collection.
- Prohibit the disclosure of sensitive de-identified worker data due to the risk of re-identification.
- Prohibit combining worker datasets including worker sensitive data with other datasets.
- Prohibit the creation of worker profiles (whether de-identified or not) for workforce analytics, performance management, or disciplinary purposes, especially when such profiles contain sensitive worker information.
- Establish additional remedies and accountability measures when a privacy breach involves sensitive worker information. Remedies should include correction or deletion of the information, cessation of the practice used, deletion of the information from other employment practices, damages, and court-enforceable orders from the Privacy Commissioner.

Proposal 9 — Legal requirement to safeguard personal data stored or processed in foreign jurisdiction

This proposal would make it a legal requirement for federal institutions to use physical, technical, and administrative security measures to safeguard the personal data it holds, including whenever personal data is stored or processed outside Canada, or in any other situation that introduces risk. These measures would need to be appropriate for the level of sensitivity of the data and risks involved.

Concern

This proposal raises significant concerns for workers if federal workers' personal information will be stored, processed, and/or accessed outside of Canada where it could become subject to foreign laws, government access requests, or privacy regimes that do not provide protections equivalent to Canadian standards. We are concerned that data moved outside of Canada may not enjoy the same level of security or protection as data stored domestically. If personal information is stored, processed, and/or accessed outside of Canada, affected workers may be at risk of foreign privacy breaches, profiling, surveillance, discrimination, detention and arrest, criminal or administrative charges, incarceration, deportation, discrimination, retaliation or other misuse. Cross-border data practices may create increased risks for Indigenous, Black and racialized workers, workers with disabilities, 2SLGBTQIA+ workers, women, caregivers, immigrants, workers with family abroad, asylum seekers, refugees, and workers involved in grievances, arbitrations, complaints and bargaining representative activity.

Questions

Should workers' personal information be stored, processed, or accessed outside Canada?

If the proposed change anticipates that workers' personal information would be processed outside of Canada, what protections will be in place to ensure federal workers' personal data is not subject to foreign surveillance, disclosure requirements, or weaker privacy standards?

Recommendations

- Recognize as a fundamental principle that federal workers' personal information should only be stored, processed, and/or accessed in Canada, especially sensitive worker information. Sensitive worker data should be prioritized for storage, processing and access in Canada.
- Limit exceptions to the prohibition of foreign storage of, processing of, and access to worker information to only the narrowest of circumstances, subject to stringent evidence-based justification and necessity. Convenience and efficiency do not constitute justification or necessity.
- Prohibit vendors and contractors should be prohibited from using federal workers' information to train, test, improve, or develop AI systems, analytics, resources and tools unless specifically authorized by law and subject to PIAs.
- Notify workers and their bargaining representatives if worker data is stored or processed outside of Canada and have the right to meaningful procedural provisions, should this occur.

- Ensure robust protections are in place if workers’ personal information is stored or processed outside of Canada, to ensure their personal data is not subject to foreign surveillance, disclosure requirements, or weaker privacy standards. Consideration of the impacts on equity-deserving workers before their information is stored, processed, or accessed outside of Canada must be an explicit consideration in the completion of PIAs or other processes authorizing or refusing the authorization of storage and processing of personal information outside of Canada.
- Provide for the clear right of workers to know where their information is held, who or what institutions have access to it, what laws apply to it in the jurisdiction in which it is held, how it may be disclosed and to whom, and what rights and remedies they have in that jurisdiction regarding their information and data, including if their rights are violated. If workers’ data is transferred to, processed in, stored in, or accessed from a foreign jurisdiction, the risk profile for the individual can change adversely and in the extreme. Protections must be commensurate with the risks.

Proposal 10 — Add necessity test to the threshold for limiting collection

This proposal would add necessity as a threshold test for any use of personal information, so that the collection of personal data is limited to data that is reasonably required to achieve a clearly defined purpose that is directly related to an operating program or activity.

Concern

While a necessity-based collection standard could provide stronger privacy protections, its effectiveness may be limited in practice. Federal workplaces already experience significant levels of worker monitoring, workforce analytics, and broad data collection practices. There is a risk that institutions will interpret "necessity" broadly, allowing extensive collection of worker data to continue. Without robust independent oversight and clear limits, necessity requirements may become a procedural exercise rather than a meaningful safeguard against excessive collection and workplace surveillance.

Questions

How will "necessity" be defined in the context of worker data collection, and what measures will prevent departments and agencies from interpreting the term so broadly that routine workplace surveillance and monitoring continue unchecked?

Will departments and agencies be required to demonstrate that less privacy-invasive alternatives were considered before collecting worker information for workforce analytics, monitoring, productivity measurement, or other workplace management purposes?

What independent oversight or review mechanisms will be established to assess whether the collection of worker data is genuinely necessary, proportionate, and justified?

What limits will be placed on the collection of telemetry, behavioural, productivity, and other workers monitoring data to prevent unnecessary or excessive workplace surveillance?

Recommendations

- Define the term "necessity" in the narrowest terms.
- Require PIA for the collection of personal data, as discussed in Proposal 3. These PIAs should operationalize the necessity test by requiring institutions to explain why the personal data is required to achieve the purpose, evaluating whether a less privacy-intrusive method could reasonably achieve that purpose, and explaining through evidence-based analysis why a less privacy intrusive method was rejected should such occur.
- Establish an independent oversight or review mechanism with meaningful procedural provisions to assess whether the collection of worker data is genuinely necessary, proportionate, and justified.
- Require departments and agencies to demonstrate that less privacy-invasive alternatives were considered before collecting worker information for workforce analytics, monitoring, productivity measurement, or other workplace management purposes.
- Require monitoring and surveillance to be proportionate, justified, and minimally intrusive.

- Place limits on the collection of telemetry, behavioural, productivity, and other workers monitoring data to prevent unnecessary or excessive workplace surveillance.
- Prohibit the collection of biometric data through emotion recognition tools, facial recognition tools or any human behaviour manipulation tools, in the workplace.

Proposal 11 — New requirement to dispose of personal data that is not necessary

This proposal would require federal institutions to dispose of personal information that was collected unintentionally or is no longer needed for its original purpose. This is expected to reduce the risks associated with excessive data retention.

Concern

The requirement to dispose of unnecessary data may conflict with obligations to preserve records for anticipated or ongoing litigation related to workplace matters (i.e., wrongful termination or human rights complaint). This could result in missing records that result in violations to workers' rights.

The requirement to dispose of personal data that is not necessary must be balanced with the requirement to preserve records for anticipated or ongoing workplace matters.

The requirement may be inconsistent or incompatible with normal employer obligations to maintain accurate basic records of employment for workers.

Questions

How will "necessary for the original purpose" be defined in the context of workplace data, and who will determine when worker information must be deleted versus retained?

What independent oversight or audit mechanisms will be in place to ensure that departments and agencies are consistently and promptly disposing of unnecessary worker personal information?

Recommendations

- Ensure the *Privacy Act* requires that records be preserved when necessary for ongoing litigation related to workplace matters such as wrongful termination or human rights complaints.
- Define "necessary for the original purpose" in the context of workplace data and determine in consultation with bargaining representatives which worker data must be deleted versus retained.
- Provide for an independent oversight or audit mechanisms to ensure that departments and agencies are consistently and promptly disposing of unnecessary worker personal information and conversely retaining it when such is required.

Proposal 12 — Recognize privacy as a fundamental right

This proposal would update the *Privacy Act's* purpose clause or preamble to recognize privacy as a fundamental right and strengthen its role in guiding federal data practices, including service delivery, and reconciliation with Indigenous Peoples.

Concerns

We support recognizing privacy as a fundamental right. Privacy is connected to democratic participation, freedom and conditions for self-development within social institutions. However, the proposal locates the recognition of this right only in the preamble. Because preambles are interpretive rather than enforceable, there is a concern that recognizing privacy as a fundamental right will not translate into concrete protections for federal workers in practice. Recognizing privacy as a fundamental right must include an anti-racist and anti-colonialist lens. Surveillance, for example, has never been experienced equally nor does it stop at the workplace door. Indigenous, Black and racialized communities, workers with disabilities, 2SLGBTQIA+ workers, women, caregivers, immigrants, workers with family abroad, asylum seekers, refugees and workers involved in grievances, arbitrations, complaints and bargaining representative activity, have been historically marginalized and surveilled. Indigenous and Black communities continue to be disproportionately policed, monitored and surveilled.

Questions

How will the government ensure that framing personal data as a "strategic asset" does not lead to expanded collection or secondary use of federal workers' personal information for workforce monitoring or performance management?

What concrete, enforceable meaningful procedural protections will flow from recognizing privacy as a fundamental right, beyond interpretive guidance in the preamble or purpose clause? If the provision does not expressly override conflicting legislation or policies, in what meaningful sense will privacy be considered "fundamental" in its legal effect, particularly where other statutory or operational requirements take precedence?

Recommendations

- Recognize in the Act, not just the preamble, that privacy is a fundamental right. This right must be accompanied by concrete, enforceable and meaningful procedural protections, rather than left to interpretive guidance in the preamble or purpose clause.
- Specify how this fundamental right to privacy interacts with conflicting legislation and policies and ensure it is given sufficient, generally overriding weight against competing interests and other legislative provisions.
- Expressly qualify the framing of personal data as a "strategic asset" so that rationale cannot be relied upon to justify expanded collection or secondary use of workers' personal information for workforce monitoring, productivity measurement, or performance management.

Proposal 13 — Incorporate principles into the *Privacy Act* to strengthen privacy practices and align with private sector privacy legislation and other international standards

This proposal would modernize the *Privacy Act* by incorporating widely recognized privacy principles from domestic and international frameworks (i.e., General Data Protection Regulation [GDPR]) including accountability, data minimization, safeguards, and transparency.

Concern

The proposed alignment with international frameworks introduces several key privacy concepts to the Canadian context. While we support modernizing the Act by incorporating recognized privacy principles such as accountability, data minimization, safeguards, and transparency, the proposal also includes several vague and undefined terms. Specifically, concepts like “necessity,” “proportionality,” and “effectiveness” can be interpreted to justify broad collection and continued workplace monitoring unless they are clearly defined and reinforced by meaningful procedural provisions.

Questions

How will concepts such as “necessity,” “proportionality’”, and “effectiveness” be defined so they can be consistently applied in real workplace or program settings, rather than interpreted differently by each organization? What specific meaningful procedural provisions will ensure workers can effectively challenge non-compliance without facing barriers such as cost, complexity, or fear of retaliation?

Recommendations

- Define concepts such as “necessity”, “minimal intrusiveness”, “effectiveness” and “proportionality” in the Act, with criteria specific enough to be applied consistently across institutions rather than left to each organization’s discretion.
- Apply these definitions to the strengthened collection threshold contemplated in Proposal 10.
- Provide workers and their bargaining representatives with accessible and effective enforcement mechanisms and remedies in the Act, which are designed to remove barriers of cost, complexity, and delay, and to protect workers who raise privacy concerns from reprisal.
- Require government institutions to bear the burden of justifying the necessity, minimal intrusiveness, effectiveness and proportionality of proposed worker information collection, not the individual worker.

Proposal 15 Harmonize the request regime by incorporating requests for personal data into the *Access to Information Act (ATIA)*

This proposal considers removing the personal data request process from the *Privacy Act* and incorporating it into the *ATIA*.

Concerns

Moving personal data requests into the *ATIA* could risk weakening the distinct safeguards in the *Privacy Act*, since the *ATIA* is primarily designed for access to government records rather than protecting sensitive personal information. This can create uncertainty for workers about which rules apply to their personal data, potentially leading to uneven application of exemptions or access rights across cases.

Questions

How will the harmonized ATIA-based process ensure that privacy protections for personal data are not weakened compared to those currently provided under the *Privacy Act*? What clear criteria will govern the use of exemptions (such as for medical records or security clearances or other sensitive worker information) to ensure workers' access and correction rights are not overly restricted? How will the government ensure consistency and clarity for individuals navigating a combined access regime so that workers understand their rights and the applicable procedures for personal data requests?

Recommendations

- Clarify the difference between access to information request processes, on the one hand, and challenges to the use of personal information through meaningful procedural provisions, on the other. Clarify which body has oversight for each process. Clarify which regime or set of rules applies to each category.
- Expressly preserve the privacy-protective standards of the current *Privacy Act* in any harmonized regime, with a guarantee that consolidation will not reduce workers' existing access, correction, or safeguard rights.
- Govern the use of exemptions affecting workers' personal information with clear narrowly drawn criteria, so that access and correction rights are not unduly restricted.
- Establish a distinct and clearly identifiable set of rules for personal-data requests within any combined regime, so workers can readily understand which protections and procedures apply to their own information. Information that is incorrect or incomplete or being improperly used must be correctable across any combined regime.

Theme 5: Indigenous Peoples' access to, and protection of, their data

Proposal 17 Define Indigenous personal data as subject to distinct governance considerations

Personal data of Indigenous people that is not categorized as Indigenous personal data would be managed and shared in accordance with the rest of the *Privacy Act*. This would include data that the individual chose not to consent to being designated as Indigenous data (a form of negative option), older data from before this designation and data that belongs to a dataset not related to the key programs identified in proposal 18.

Concerns

Indigenous federal workers' data may be treated differently depending on whether it falls under "Indigenous personal data" or general *Privacy Act* rules, potentially creating gaps in protection for sensitive information. We support distinct governance for Indigenous data but are concerned that classifying some information as "Indigenous personal data," while the remainder is governed by the general *Privacy Act*, may fragment the governance of Indigenous federal workers' employment-related information across two regimes, creating risks of inconsistent handling and uneven protection.

Questions

How will the framework ensure that Indigenous workers' personal information is consistently protected when different parts of their employment-related data are classified differently under "Indigenous personal data" versus the general *Privacy Act* regime? What mechanisms will allow Indigenous workers to understand, review, or challenge how their workplace-related personal data is classified and managed over time, especially for historical or legacy records?

How will the government prevent gaps in protection or uneven privacy standards for Indigenous workers when similar types of employment data are subject to different governance rules?

Recommendations

- Require the framework to provide Indigenous workers with a clear and revocable consent mechanism governing if and how any of their employment-related data may be collected, analyzed, processed, used or shared, and ensure such is not undertaken without their informed consent.
- Provide Indigenous workers with accessible means to understand, review, and challenge how their workplace-related data has been classified and managed over time, including for historical and legacy records predating the designation, with meaningful procedural provisions.
- Require the government to adopt safeguards to prevent gaps or inconsistent standards where similar categories of employment data are governed by different rules, ensuring no Indigenous worker receives lesser protection by reason of how a given record was classified.

- Require that Indigenous workers and their representatives be meaningfully consulted in the design of any classification and governance rules applying to their employment data, and that such consultation occurs before those rules are finalized.

Theme 6: Updating the compliance framework — current enforcement mechanisms are not designed to handle AI

Proposal 19: Grant the Commissioner binding order-making powers for corrective action plan enforcement and provide them with the discretion to discontinue or decline complaints

The proposal would give the Privacy Commissioner binding order-making powers and the ability to require corrective action plans with public reporting and possible Federal Court escalation. It also introduces limited discretion to decline or stop investigating certain complaints.

Concern

The discretion to refuse or stop investigating complaints could reduce workers' ability to have certain privacy issues fully examined, especially if complaints are deemed low priority or not pursued, or even found to be frivolous or vexatious, leaving some workplace privacy harms unaddressed.

While the proposed measures to strengthen institutional oversight, enhance public trust, and increase accountability are welcome, they do not address how the Commissioner determines whether a complaint is "frivolous or vexatious" and therefore subject to dismissal at the Commissioner's discretion. These proposals could be strengthened by increasing transparency around how this discretion is exercised. Furthermore, fundamental labour rights cannot be undermined or overridden by this order-making power.

Greater clarity regarding the exercise of this discretion would promote consistency and transparency, while reinforcing public confidence that all complaints of privacy harms will be assessed fairly, and will not be arbitrarily dismissed or unreasonably delayed.

Questions

How will decisions to refuse or discontinue investigating privacy complaints be guided and reviewed to ensure workers still have meaningful access to remedies for workplace privacy concerns?

Recommendation

- Include clear criteria in the Act, to be used to determine whether a complaint is considered "frivolous or vexatious" and include provisions defining how such complaints will be assessed and processed by the Commissioner's Office.
- Ensure the order-making power of the Privacy Commissioner does not override or replace existing collective agreement procedural and substantive protections that may be provided through superior negotiated agreement provisions and the right to grieve and arbitrate disputes.

Proposal 20: Authorize the Commissioner to collaborate and share information with other jurisdictions

This proposal considers amending the Act to allow the Commissioner to share information, including personal data, with other regulatory and oversight bodies under defined conditions. This would include federal review bodies, provincial and territorial regulators, and international counterparts, where necessary to advance the Commissioner's mandate in the public interest.

Concerns

Expanded sharing of personal data across domestic and international regulators may increase the risk of information being used in ways workers did not anticipate or consent to and may raises questions about how privacy is protected once data leaves the original context. We are concerned this may undermine the ability of workers and their bargaining representatives to engage in meaningful co-governance over these issues.

All of our concerns expressed about Proposals 7 and 9 have application here, as do the recommendations made there.

Questions

What safeguards will ensure that workers' personal information is only shared with other regulators when strictly necessary, and not beyond what is required for a specific investigation or mandate? How will workers be informed about when their personal data is shared across domestic or international oversight bodies, and what recourse will they have if they believe that sharing was inappropriate or excessive?

Recommendations

- Recognize as a fundamental principle that the sharing of worker data with other regulatory and oversight bodies is presumptively prohibited.
- Clearly specify in the *Privacy Act* when exemptions to this principle may be granted and by which oversight body. The requirements to obtain an exemption must include demonstrating that the exemption is necessary and proportionate, and the interests to be advanced are sufficiently important so as to outweigh workers' individual and collective privacy rights, all through cogent, relevant evidence. Convenience and efficiency do not justify obtaining such an exemption.
- Require PIAs and meaningful procedural protections in respect of the use of this power to collaborate and share information with other regulatory and oversight bodies.
- Require worker consent in the *Privacy Act whenever* workers' sensitive and personal data is sought to be shared across jurisdictions.
- Expressly provide for remedies in the *Privacy Act in* conjunction with these increased powers to advance the Privacy Commissioner's mandate, for harms resulting from the sharing of workers' personal information that they did not consent to.

Proposal 21- Offences for attempts to re-identify data, except under specific, limited circumstances

This proposal considers introducing offences for individuals or entities that intentionally re-identify data that has been de-identified, except where re-identification is permitted by law or is necessary as a matter of course for specific purposes such as investigations, national security, or other narrowly defined circumstances in regulations. Incidental or unavoidable re-identification that occurs during legitimate processing would not be considered an offence.

Concern

Workers could be affected by uncertainty around what counts as lawful or “necessary” re-identification, especially in investigations or security contexts, which may broaden exceptions in practice. Further, federal workers may have limited visibility regarding when or why their data is re-identified, making it harder to detect misuse or challenge decisions after the fact.

Questions

How will “necessary as a matter of course” and other exceptions for lawful re-identification be clearly defined to prevent overly broad interpretation in practice? What oversight and audit mechanisms will ensure that permitted re-identification (e.g., for investigations or national security) is not used to justify routine or excessive linking of de-identified worker data? How will individuals be informed when their de-identified data is re-identified, and what avenues will they have to challenge or review that process? How will workers dealing with de-identified data in their work be protected against employment discipline or offence prosecution in the event of accidental re-identification?

Recommendations

- Recognize as a fundamental principle that re-identification of de-identified data without lawful authorization is an offence, but that such an offence must also be subject to meaningful procedural protections.
- Expressly define in the Act when re-identification is “permitted by law” or “is necessary as a matter of course.”
- Ensure the offence is directed at malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit. A worker who accidentally re-identifies a person while performing legitimate duties should generally not be held liable unless their actions meet the elements of malice, intent to harm, or intent to obtain an illegitimate benefit.
- Ensure there are oversight and audit mechanisms in place to safeguard from the unauthorized linking of de-identified worker data with other data which could tend to re-identify the worker.
- Ensure the Act specifies what remedies are available to workers when their de-identified data is re-identified for an unlawful or unauthorized purpose.

Proposal 22 — Expand judicial remedies and clarify Federal Court authority

This proposal considers expanding the Federal Court's authority to allow individuals and the Commissioner to seek remedies for a broader range of privacy violations. It would also clarify further recourse options for the mishandling of personal data, ensuring that institutions are held accountable when they fail to comply.

Concerns

Even with expanded Federal Court authority, federal workers may face persistent obstacles in bringing privacy claims because of issues like cost, time, or legal complexity. These obstacles may limit how readily accessible remedies for privacy violations are.

Questions

What measures will be put in place to ensure workers can realistically access Federal Court remedies, given potential barriers such as cost, complexity, and time? How will "privacy violations" be clearly defined to ensure workers understand when they have grounds to seek recourse and to promote consistent decision-making? What timelines or expedited processes will be established in the Federal Court to ensure that privacy disputes affecting workers are resolved in a timely manner?

Recommendations

- Ensure the expanded judicial remedies are consistent with the recommendations made for Proposals 19, 20, and 21.
- Ensure "privacy violation" is clearly defined in the Act, and examples of privacy offences for which legal remedies can be pursued should be listed non-exhaustively.
- Ensure the court rules provide sufficient guidance and are designed to foster efficient processes to pursue legal recourse for a privacy offence or violation through the Federal Court.
- Establish a dedicated expedited process within the Federal Court to enable workers and/or the Commissioner to seek timely remedies for systemic or broader privacy violations.

Appendix A: List of ad hoc working group members

Susan Ursel, Senior Partner, Ursel Phillips Fellows Hopkinson L.L.P.

Hannah Johnston, Assistant Professor, York University, School of Human Resource Management

Sarah Ryan, Acting Research Director, Canadian Union of Public Employees

Eman Cheema, Barrister & Solicitor, Canadian Union of Public Employees

Jésaël Lisiecki, Research Officer, Canadian Association of Professional Employees

Krista M Devine, General Counsel, Public Service Alliance of Canada

Graham Cox, National Representative, Unifor Research Department

Rubina Boucher, National President, Canada Employment and Immigration Union

SR:ic/cope491