BC CLA BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION | ASSOCIATION DES LIBERTÉS CIVILES DE LA COLOMBIE-BRITANNIQUE

Submissions to the House of Commons Standing Committee on Human Resources, Skills and Social Development and the Status of Persons with Disabilities regarding the Implications of Artificial Intelligence Technologies for the Canadian Labour Force

November 22, 2023

Prepared by Aislin M. Jackson, Policy Staff Counsel

British Columbia Civil Liberties Association
306 - 268 Keefer Street
Vancouver, BC, Canada V6A 1X5

Tel 604.687.2919
Fax 604.687.3045
Toll-free 866.731.7507

info@bccla.org
www.bccla.org

Introduction

Artificial Intelligence ("AI") is a category of technology that seeks to replicate human-like decision making, make predictions, or perform other analytical tasks through software models trained on large datasets. These software models, once so trained, are able to analyze a large volume of information to make a decision or prediction much more quickly than a human could.

AI's ability to quickly analyze large volumes of information promises great leaps in productivity and innovation and will surely revolutionize the Canadian workplace. At the same time, its emphasis on automation, appetite for data, and distance from human decision-makers enable workplace surveillance of a scope and depth that was not previously possible. These attributes of AI also raise the spectre of workers being subjected to discriminatory decision-making for which no human being can be held responsible. Further, AI creates novel issues of worker health and safety. As AI reshapes the workplace, it is vital that Canada face these risks with clear eyes and craft appropriate legislation to protect against these harms.

Workers' Privacy

Privacy is a fundamental human right as well as a necessity for the meaningful participation of citizens in a democratic state. The importance of this right is emphasized by the inclusion of section 8 in the *Charter*[1], which guarantees our privacy rights by protecting us from unreasonable search or seizure by the state and its agents.

The privacy interests of Canadians do not stop at the office or shop door. Employers exercise a high level or power and control over their workers, and it is natural to desire – and reasonable to expect – that workers be free of this power and control in the private sphere. In our submission, AI's ability to facilitate surveillance and data collection makes it possible for employers to invade the privacy of workers on an unprecedented scale, turning the workplace into an effective panopticon.

Further, following the COVID-19 popularization of remote work, the workplace itself does not stop at the office or shop door. It follows us to those most private and personal spaces, our homes. The caselaw that interprets section 8 of the *Charter* has recognized that we have an elevated expectation of privacy in our homes, owing to the private, personal, and intimate nature of the activities that take place there.[2] Accordingly, information about activities inside the home is afforded a high level of constitutional protection when and to the extent that it can reveal intimate, personal information about the biographical core of an individual.[3] Any form of surveillance that captures images of the interior of an employee's home – including objects and decoration that the worker has chosen and information about other residents of the home – could

[1] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.
[2] See e.g. *R v Gomboc*, 2010 SCC 55, [2010] 3 SCR 211 at paras 45 and 79.
[3] See *ibid* at para 50.

represent an intrusion of the employer into a sphere of privacy that the state is constitutionally required to respect.

The boundary between workplace surveillance and state surveillance is porous. Section 487.0195 of the *Criminal Code*[4] permits police to make informal requests for voluntary disclosure of computer data and documents, as long as the disclosure is not prohibited by law. This section also protects entities that voluntarily disclose information under the provision from any civil or criminal liability that may otherwise flow from their disclosures.

One major concern resulting from the above *Criminal Code* provision is that, where applicable privacy legislation allows disclosure to law enforcement, evidence that the police obtain in this way can be used as evidence in criminal cases.[5] Whether these cases are against the specific worker or as evidence in a case against someone else, the circumvention of *Charter* rights regarding privacy and liberty is a clear concern.

It is particularly concerning that information may be included in police and national security databases through this type of surveillance and voluntary disclosure. Information in these databases has been used to further state surveillance within Canada, and is often shared across government departments and even with foreign governments.[6] As workplace surveillance can operate as a 'back door' for the state to gather information about individuals, the issue is not only a labour relations concern but a civil liberties one as well.

Employers have sought to surveil their workers since long before the advent of AI, and workers have resisted this surveillance for just as long.[7] Employer surveillance may be motivated by concerns about productivity, misuse of resources, and worker honesty. Employers can use a variety of surveillance technologies in the workplace, ranging from video surveillance to geolocation tools that identify the location of employees, attention trackers that use webcams to monitor the worker's biometric features like eye gaze, or keyloggers that capture every keystroke. Even without AI, these tools are invasive and can reveal details about an employee's daily habits, personal relationships, and even capture passwords to any personal accounts that the worker may check on their work devices.[8]

As powerful as these surveillance tools are on their own, monitoring and analyzing their outputs would be extremely, perhaps prohibitively, resource-intensive without AI assistance. Because of

---

[4] RSC 1985, c C-46.
[5] See *R v Kurucz*, 2023 ABKB 353 at paras 320-328.
[6] See Greg McMullen, "Pulling Back the Curtain on Canada's Mass Surveillance Programs – Part Two", *BC Civil Liberties Association*, (16 March 2023), online: <https://bccla.org/2023/03/pulling-back-the-curtain-on-canadas-mass-surveillance-programs-part-two-the-cse-secret-spying-archive/>.
[7] See e.g. *Re Lornex Mining Corporation Ltd. and United Steelworkers, Local 7619*, 14 LAC (3d) 169, 1983 CanLII 4887 (BC LA).
[8] Darrell M West, "How employers use technology to surveil employees" (January 5, 2021), online: *The Brookings Institution* <https://www.brookings.edu/articles/how-employers-use-technology-to-surveil-employees/> [https://perma.cc/JM55-DDH2].

this, the availability of AI incentivizes the expansion of workplace surveillance by enabling more surveillance for the same or fewer resources. As AI is a data-hungry technology, expanding use will also provide an incentive for an employer to store more data for longer than they otherwise might in the hopes that it could become useful for future AI training and analysis.

More expansive storage of information about workers necessarily increases the risk to the workers' privacy: data that is not retained cannot be voluntarily provided to law enforcement, nor can it be stolen by malicious actors. In this way, the use of AI to assist workplace surveillance amplifies the risks and invasiveness of all other workplace surveillance techniques and technologies.

Automated Bias

AI models are only as good as their training data: they have no knowledge or insight into the world beyond what is included in that data, and no independent judgment or sense of ethics. The goal is to make human-like decisions, decisions that fit into the statistical patterns it teases from the training data, rather than normative or legal principles. If discriminatory bias is present in the dataset that the AI model is trained on – whether in the underlying data itself or in the way the data has been packaged and formatted to render it intelligible to the program – the AI will replicate this pattern. As forms of bias that give rise to discrimination are all-too present in Canadian society, and were historically prevalent, training datasets must be carefully selected and encoded to prevent the resulting AI model from expressing these biases. There is also a risk that bias will be introduced if an AI model is used for a different purpose than it was trained for, as the new context may raise forms or expressions of bias that were not considered or controlled for in the preparation of the training dataset.[9]

The decision-making and analysis of AI models are often opaque, functioning as a proverbial 'black box': the inputs and outputs are known, but the actual workings, the precise algorithms being used, are obscure. This opacity it difficult for end-users of AI tools, including employers, to evaluate whether the models they're using has bias. End-users are often not the developers of the AI tools that they use, which are created by specialized firms and then sold as a finished product, and do not have access to the source code or training dataset.

Without examining the code and data that produced the model, bias can only be evaluated by examining the outputs of the AI model, a process which requires not only a substantial sample of outputs but also technical and statistical expertise.[10] Even entities that create their own AI tools can have difficulty identifying bias within their models before it has real-world effects: Facebook, for example, had to apologize in September 2021 after users viewing a news clip that featured Black men were asked if they wanted to "keep seeing videos about Primates"..[11]

The insidious nature of discriminatory bias in AI is an obvious obstacle to preventing human rights violations in employment. It also raises fundamental questions about accountability when an employer makes a discriminatory employment decision with the aid of an AI tool: must employers of all sizes bear the expense of generating and analyzing the output of a commercial AI product before they can use it? If not, can they escape liability for discrimination if they rely in good faith on the AI model? Can an AI developer be held responsible for discrimination that flows from their tools' biased outputs, even though they do not have control over the decision-making of the employer or the context in which their product is used?

---

[9] See e.g. Xavier Ferrer et al, "Bias and discrimination in AI: a cross-disciplinary perspective" (2021) 40:2 IEEE Technology and Society Magazine 72 at 72.
[10] See *ibid* at 73-74.
[11] See Ryan Mac, "Facebook Apologizes After A.I. Puts 'Primates' Label on Video of Black Men", *The New York Times* (3 September 2021), online: <https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html> [https://perma.cc/V86E-M7R3].

If neither the employer who uses the AI tool nor the developer of the AI is responsible, individuals who experience AI-assisted discrimination may be left without a remedy even if they can establish that the AI model contains an inherent bias. This is, in our submission, unacceptable, both because of the injury to the individual's human dignity and economic interests and because it would license employment discrimination more broadly.

Although commercial applications of AI are still evolving, preliminary data from the United States of America indicates that AI tools are attractive to human resources professionals and are already being widely used. A survey conducted by the Society for Human Resources Management in February 2022 found that almost 1 in 4 respondent organizations already used automation and/or AI in their human resources activities.[12] 79% of these organizations use these tools for recruitment and hiring,[13] which is a particular concern as the nature of the hiring process makes hiring discrimination especially difficult to evaluate and prove in a tribunal or court even with only human decision-makers.

Unlike humans, AI generates no notes and has no discussions with others that can provide insight into whether and how the worker's protected characteristics were considered in the decision-making process. This evidence, or the lack of it, is often necessary for the complainant to discharge their burden to prove that an employer's non-discriminatory explanation for their conduct is pretextual.[14] Even if courts or tribunals accept evidence of algorithmic bias in the AI tool that the employer relies on as sufficient to discharge the complainant's burden, individuals without the resources of even small business organizations will have to pay for experts to conduct this analysis. Unlike the businesses that are using these tools, individual complainants do not have access to the tool itself and cannot generate large sets of output data for examination. In this way, AI facilitated discrimination is inherently more expensive and challenging to prove, making it more difficult to get redress for human rights violations.

Workplace Health and Safety Standards

One clearly harmful and dangerous form of AI usage is identified in draft legislation prepared by the European Union (the "EU"); namely, the *AI Act*.[15] The EU noted that employers could use AI to subliminally manipulate their workers. For example, an inaudible sound in a truck driver's cabin could keep the driver awake beyond the limits of their health and safety.[16] To address this issue without placing the legal burden of proof on vulnerable workers, the EU proposes to ban this type of AI usage outright. Notably, the draft AI legislation that is currently being considered

---

[12] "Automation & AI in HR" (2022) at 3, online (pdf): *Society for Human Resources Management* <https://advocacy.shrm.org/SHRM-2022-Automation-AI-Research.pdf>, [https://perma.cc/4BVJ-JU6F].
[13] *Ibid* at 4.
[14] See *Wilson v Canada Border Services Agency*, 2015 CHRT 11 at paras 19-21. See also *Dulce-Crowchild v Tsuut'ina Nation*, 2020 CHRT 6 at paras 64 and 94.
[15] *Artificial Intelligence Act*, European Commission, 2021/0106 (COD) at pages 38-88, online: <https://artificialintelligenceact.eu/the-act/> [*AI Act*].
[16] *Ibid* at Art. 5.

by the Standing Committee on Industry and Technology as part of Bill C-27 contains no analogous provision.

The EU's draft *AI Act* identifies five categories of prohibited AI usage altogether, with the caveat that additional categories may be added as AI technology continues to develop.[17] Like any other technology, it is likely that AI will create new health and safety risks for employees that have yet to be imagined. For this reason, it is imperative that AI's potential dangers to worker health and safety are prohibited or strictly regulated.

Summary

The BC Civil Liberties Association ("BCCLA") recommends that this committee's study clearly identify the potential harms of AI in the workplace in the following areas of impact:

- Workers' privacy interests, through increasing surveillance and data collection that may be disclosed to law enforcement;
- Workers' human rights in employment, as obscure decision making and the prospect of bias in AI models makes discrimination more difficult to identify, prevent, and prove; and
- The possibility that AI tools will allow novel health and safety risks through the manipulation of worker behaviour.

About the BC Civil Liberties Association

The BCCLA is the oldest civil liberties and human rights group in Canada, advancing litigation, law reform, community-based legal advocacy, and public legal education for the last 60 years.

[17] *Ibid*.