

## **Comments on Preliminary Discussions with the Government of Canada on Council of Europe Treaty Negotiations on Artificial Intelligence**

Ana Brandusescu, PhD Candidate, McGill University  
Renée Sieber, Associate Professor, McGill University

*The following response is part of the preliminary discussions with the Government of Canada on the Council of Europe (CoE) Treaty Negotiations on Artificial Intelligence. In developing Canada's negotiating positions, the Core Departments representing Canada in these negotiations -- co-led by Global Affairs Canada and the Department of Justice, with strong support by the Treasury Board of Canada Secretariat and Innovation, Science and Economic Development Canada -- wish to solicit the views of Canadian experts and stakeholders with an interest and expertise in AI and human rights. To this end, we have prepared answers to questions from the Core Departments based on a draft of the treaty known as the "Consolidated Working Draft". This is the most recent draft of the treaty, as prepared by the CoE Secretariat and the Chair of the CoE's Committee on Artificial Intelligence and published on July 7, 2023. This draft has been provided by the CoE to serve as the basis for further negotiations. It does not yet reflect the final outcome of the negotiations, which are expected to conclude in early 2024. The authors consent to having their name, the name of the organization they represent, and their title within the organization published in association with their comments.*

### **Abstract**

This response answers questions posed by Canada's Core Departments *in developing Canada's negotiating positions for the Council of Europe Treaty Negotiations on Artificial Intelligence*. We propose the treaty should adopt harm-based and rights-based approaches. This includes rights mechanisms that move beyond risk as well as include a strong role for participation by civil society, proportionate redress mechanisms, arms-length monitoring and supervisory authorities that do not have dual mandates in the commercial and regulatory aspects of AI, as well as moratoria or bans to address AI systems that are high-harm and pose an unacceptable level of risk. The treaty excludes trans and gender non-conforming individuals. AI has induced differential harms to various marginalized groups that cannot be captured in ambiguous language.

We discuss (1) the use of biometrics (including facial recognition technology) for access to essential services; (2) the development and use of autonomous weapons systems; and (3) the treatment of AI workers, especially those in low and middle income countries. AI systems like facial recognition technology and autonomous weapons systems merit special treatment in the treaty because of discrimination based on race and gender, exemptions often granted to national security agencies and law enforcement, and challenges with government accountability.

Canada has a special role as observer in this treaty, both in terms of Canada's value to the global AI discourse and Canadian values. Canada is recognized as an international leader in responsible

AI with best practice policy instruments Canadian values and case law reveal strong support for Indigenous rights, environmental protection, and peacekeeping. During these negotiations, Canada has the opportunity to advocate for a focus on actual and current harms of existing AI systems instead of future existential risks, and assert collective privacy beyond simple personal data protection.

**1. What are the key outcomes that you would like to see from this treaty? This may include considerations in relation to:**

**The application of the treaty to the public and private sectors:** To the degree possible, Canada should be able to develop more stringent policies and standards, if it chooses, related to the development and use of AI within its boundaries (e.g., around opting out of datasets used to train facial recognition technology). This would include no repercussions for government agencies should a country, for example, remove a company from its preferred vendors' list.

**The use of risk-based approaches to the regulation of AI:** Instead of a risk-based approach, the focus of the treaty should be on harm-based and rights-based approaches. Risk-based approaches can over-emphasize software performance (e.g., the risk of inaccurate results or lack of currentness of inputs) as well as reputational risk to the public/private sector. For example, a system that accurately predicts a pregnant person's menstrual cycles and likelihood of pregnancy can endanger them, should that accurate prediction be used in another application that shows the persons' nearness to a political boundary or an abortion centre. In this and other cases, a private sector firm may assert proprietary control over the model because identifying the source of training data may discomfit the firm, that is risk damage to their reputation.

We note calls for risk-based approaches,<sup>1</sup> which argue, among other things, that the focus must be on the application of AI and algorithms. However, as we have seen, there are fundamental problems with some foundational technologies. For example, false arrests from predictive policing may reveal deeply embedded bias in generative pre-trained transformers (GPTs) that cannot be removed when an application is built atop the model. These flaws exceed mere calls to document or explain but require the need to regulate what is becoming the underlying core infrastructure of AI.

We strongly support Article 6 on the protection of governments from undue influence from AI and respect for judicial independence. We also support the potential to decommission AI systems. We support Items 4-7 in the treaty preamble, although the text of Item 6 should be broadened to include the protection of trans and gender non-conforming individuals.

---

<sup>1</sup> Gerlach, N. (2023, March 23). The case of the EU AI Act: Why we need to return to a risk-based approach. *International Association of Privacy Professionals*.  
<https://iapp.org/news/a/the-case-of-the-eu-ai-act-why-we-need-to-return-to-a-risk-based-approach/>

There needs to be refinement of the consequences of the good but quite broad definition of AI. Decisions around rights, redress, monitoring and supervisory authorities will be vastly different when considering, for instance, logistic regression compared to reinforcement (neural network) learning.

We would like to see strong AI worker protections in this treaty, for example, service availability (e.g., substantial worker protections for mental health),<sup>2</sup> unionization,<sup>3</sup> class action lawsuits,<sup>4</sup> and whistleblower protection.<sup>5</sup> This includes workers in low and middle income countries, whether inside and outside the participating member states, who may be fundamental to AI systems development in participating countries.

**Rights mechanisms:** Rights mechanisms should include a right to public participation (of impacted individuals and groups as well as the general public) in the choices to develop and use/decommission AI. The right for participation should occur as early as possible in the development stage. There are proven methods to involve the public and/or affected people in the AI design and development process (e.g., participatory design).<sup>6</sup>

**Redress mechanisms:** Redress mechanisms should include the ability to ban AI companies or decommission specific AI systems. We would like to see the treaty support regulatory and judicial regimes that can deliver monetary and other damages proportionate to the harm caused. Compensation should accrue both to the government and to the affected individual(s). The treaty also should enable class action lawsuits (e.g., harm to Black people as a consequence of false arrests due to predictive policing and/or facial recognition technology).

**Monitoring and supervisory authorities:** We seek accountability in a supervisory authority body that is independent and has enforcement power. The independence must be at arm's length, free of undue influence by the public and private sectors. The supervisory authority body also must have mechanisms to address conflicts of interest amongst those who sit on the body and experts who come before the body. As we have learned from the nuclear regulatory bodies,<sup>7</sup> the supervisory authority body cannot be both involved in the commercial and regulatory aspects

---

<sup>2</sup> Arsht, A., & Etcovitch, D. (2018). The Human Cost of Online Content Moderation. *Harvard Journal of Law and Technology (JOLT)*. <https://jolt.law.harvard.edu/digest/the-human-cost-of-online-content-moderation>

<sup>3</sup> Perrigo, B. (2023, May 1). 150 African Workers for ChatGPT, TikTok and Facebook Vote to Unionize at Landmark Nairobi Meeting. *TIME*. <https://time.com/6275995/chatgpt-facebook-african-workers-union/>

<sup>4</sup> Ibid.

<sup>5</sup> Brown, S. (2021, October 6). Ex-Google researcher: AI workers need whistleblower protection. *MIT Management Sloan School*.

<https://mitsloan.mit.edu/ideas-made-to-matter/ex-google-researcher-ai-workers-need-whistleblower-protection>

<sup>6</sup> Lee, M. K., Kusbit, D., Kahng, A., Kim, J.T., Yuan, X., Chan, A., See, D., Noothigattu, R., Lee, S., Psomas, A., & Procaccia, A. D. (2019). WeBuildAI: Participatory Framework for Algorithmic Governance. *Proceedings of ACM Human-Computer Interaction* 3, (November 2019), 1–35. <https://doi.org/10.1145/3359283>

<sup>7</sup> Johannson, P. R., & Thomas, J. C. (1981). A Dilemma of Nuclear Regulation in Canada: Political Control and Public Confidence. *Canadian Public Policy / Analyse de Politiques* 7, 3 (Summer, 1981). <https://doi.org/10.2307/3549641>

of AI. That is, a supervisory authority body should not simultaneously create policies that promote AI/deliver services related to AI and develop/enforce regulations of AI.<sup>8</sup>

**Proposed moratoria or bans to address AI posing an unacceptable level of risk:** The treaty should include the possibility of moratoria or bans on certain AI systems that are high-harm. Government entities large and small have called for a ban on the use of facial recognition technology across the US and the EU. Some organizations in the public and private sector have already declared moratoria on facial recognition technology, which is core to numerous AI systems. The moratoria should extend to autonomous weapons systems.

## **2. Do you see additional risks to the development and use of AI in relation to the protection of human rights, democracy and rule of law other than those already addressed in the draft treaty?**

We see three omissions that should be addressed: (1) the use of biometrics (including facial recognition technology) for access to essential services (e.g., banking); (2) the development of autonomous weapons; and (3) the treatment of AI workers, especially those in low and middle income countries.

**On the use of biometrics:** We note that the treaty covers data protection, safety, and security. However, the treaty should contain greater specificity on responsibility for data breaches as well as impacts of increased surveillance afforded by facial recognition technology. Here we raise three points: First, according to Canada's Office of the Privacy Commissioner,<sup>9</sup> biometrics like facial recognition are intimately associated with the human body and cannot be easily changed. If breached, they can expose someone to serious and ongoing harm, such as fraud. Second, and contrary to the previous point, for trans and gender non-conforming individuals, facial recognition technologies often fail to correctly identify and classify their faces (i.e., false positives, false negatives), as individuals' faces change.<sup>10</sup> Third, as we know from predictive policing, there are consequences to false positives and negatives with systems built on facial

---

<sup>8</sup> "In 2014, the Organisation for Economic Co-operation and Development (OECD) published a guide, *The Governance of Regulators*, which stresses the importance of independent regulatory decision making, conducted at arm's length from the political process in instances where perception of impartiality drives public confidence and where the decisions of the regulator could have a significant impact on particular interests": Witzel, M. (2022, August 11). A Few Questions about Canada's Artificial Intelligence and Data Act. *Centre for International Governance Innovation*.

<https://www.cigionline.org/articles/a-few-questions-about-canadas-artificial-intelligence-and-data-act/>

<sup>9</sup> Office of the Privacy Commissioner of Canada. (2021). The Use and Impact of Facial Recognition Technology Issue Sheets.

[https://priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/ethi\\_frt\\_20210510/is\\_frt\\_20210510/](https://priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/ethi_frt_20210510/is_frt_20210510/)

<sup>10</sup> Hicks, M. (2019) Hacking the Cis-tem. *Transgender Citizens and the Early Digital*. *IEEE Annals of the History of Computing* (Jan/March), 20-33. <https://ieeexplore.ieee.org/document/8634814>

recognition technologies: namely the wrong people are arrested because the technology is racially biased in the accuracy of its detection.<sup>11</sup>

**On autonomous weapons:** See our answer to Question 7. A treaty should be cautious in limiting discussion of autonomous weapons to their lethality because non-lethal weapons contribute to surveillance; they can be easily repurposed or work in concert with lethal systems; and human oversight can too easily be omitted, especially when speed of response is demanded by governments. Moreover, the risks of misidentification of non-lethal weapons is still an issue of life or death.<sup>12</sup>

**On the treatment of AI workers:** The role of human labour is essential to AI development and often outsourced to AI workers around the world,<sup>13</sup> who are predominantly based in low and middle income countries,<sup>14</sup> and whose work can remain hidden from what we think of as AI development.<sup>15</sup> The job of data/content moderators is essential to improving the quality AI training models. The workers manually tag photos<sup>16</sup> for Facebook (Meta) and TikTok, and more recently text, for the GPT firm OpenAI, through intermediary companies like Sama and Scale AI. This data labelling work includes the moderation of harmful and abusive content, which has led to the traumatization and dehumanization of workers.<sup>17 18 19</sup>

Workers rights include the rights of AI workers to unionize and receive whistleblower protection. In Kenya, Daniel Motaung, an ex-Facebook content moderator and whistleblower, filed a lawsuit against companies Meta and Sama's country operations.<sup>20 21</sup> In the US, The Silenced No More Act in California was passed to ensure that workers who experienced

---

<sup>11</sup> Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine Bias. *ProPublica*.

<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

<sup>12</sup> International Committee of the Red Cross. (2022, July 26). What you need to know about autonomous weapons.

<https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons>

<sup>13</sup> Posada, J. (2020). From development to deployment: For a comprehensive approach to ethics of AI and labour. In *The 21st Annual Conference AoIR Selected Papers of Internet Research*.

<sup>14</sup> Miceli, M., Posada, J., & Yang, T. (2022). Studying up machine learning data: Why talk about bias when we mean power?. In *Proceedings of the ACM on Human-Computer Interaction* 6, 1-14.

<sup>15</sup> Gray, M. L., & Suri, S. (2019). *Ghost work: How to stop Silicon Valley from building a new global underclass*. Eamon Dolan Books.

<sup>16</sup> Roberts, S. T. (2019). *Behind the screen*. Yale University Press.

<sup>17</sup> Perrigo, B. (2022, February 17). Inside Facebook's African Sweatshop. *TIME*.

<https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/>

<sup>18</sup> Perrigo, B. (2023, January 18). Exclusive: OpenAI Used Kenyan Workers on Less Than \$2 Per Hour to Make ChatGPT Less Toxic. *TIME*.

<https://time.com/6247678/openai-chatgpt-kenya-workers/>

<sup>19</sup> Tan, R., & Cabato, R. (2023, August 28). Behind the AI boom, an army of overseas workers in 'digital sweatshops'. *The Washington Post*.

<https://www.washingtonpost.com/world/2023/08/28/scale-ai-remotasks-philippines-artificial-intelligence/>

<sup>20</sup> Perrigo, B. (2022, January 10). Under fire, Facebook's 'ethical' outsourcing partner quits content moderation work. *TIME*.

<https://time.com/6246018/facebook-sama-quits-content-moderation/>

<sup>21</sup> Sambuli, N. (2022, August 12). Facebook lawsuit in Kenya could affect Big Tech accountability across Africa.

*OpenDemocracy*. <https://www.opendemocracy.net/en/5050/facebook-meta-sama-daniel-motaung-court-kenya/>

workplace discrimination or harassment get heard and supported.<sup>22</sup> Unionization and government support for unionization represents an important remedy to harms from AI.<sup>23 24</sup> The support should extend to strong whistleblower protection for public sector workers. The 2017 House of Commons Report: Review of Public Servants Disclosure Protection Act includes substantial recommendations on how to improve Canada’s whistleblower protection legislation<sup>25</sup> to address civil society concerns on Canada’s current legal framework for whistleblowing, which is “outdated and out of step with internationally recognized best practices.”<sup>26</sup> Treaty protections also could extend to protection for private sector whistleblowers, who reveal societal harms as a result of AI.<sup>27</sup>

### **3. Do you see the Council of Europe’s draft treaty on AI, human rights, democracy and rule of law as compatible with Canadian interests and values?**

The treaty appears compatible with the Canadian Charter of Rights and Freedoms. However, Canadian values and case law reveal strong support for Indigenous rights,<sup>28 29</sup> which are not explicit in the treaty and therefore should be strengthened. The same can be said for environmental protection. AI can cause considerable harm to the physical environment, which will only increase with the increased use of GPTs.<sup>30</sup> Additionally, decommissioning as a concept is in line with the military peacekeeping values of Canadians.<sup>31</sup>

### **4. Are there other values, principles, or perspectives that you would like to see Canada advocate for during these negotiations that are not addressed in the draft treaty?**

---

<sup>22</sup> Paul, K. (2021, May 10). She broke her NDA to speak out against Pinterest. Now she’s helping others come forward. *The Guardian*.

<https://www.theguardian.com/technology/2021/may/10/pinterest-discrimination-ifeoma-ozoma-nda>

<sup>23</sup> Perrigo, B. (2023, May 1). 150 African Workers for ChatGPT, TikTok and Facebook Vote to Unionize at Landmark Nairobi Meeting. *TIME*. <https://time.com/6275995/chatgpt-facebook-african-workers-union/>

<sup>24</sup> Siele, M. K. N. (2023, May 22). “It’s been tough for us”: Meta’s Kenyan content moderators say they’ll keep fighting. *Rest of World*. <https://restofworld.org/2023/meta-content-moderators-kenya-fired-unionize/>

<sup>25</sup> House of Commons Canada. (2017, June). Strengthening the Protection of the Public Interest Within the Public Servants Disclosure Protection Act. Report of the Standing Committee on Government Operations and Estimates. *42nd Parliament, 1st Session*.

<https://www.ourcommons.ca/Committees/en/OGGO/StudyActivity?studyActivityId=9339754>

<sup>26</sup> Transparency International Canada. Enhancing Whistleblower Protection. Canada’s Open Government Portal.


<https://open.canada.ca/en/idea/enhancing-whistleblower-protection>

<sup>27</sup> Brown, S. (2021, October 6). Ex-Google researcher: AI workers need whistleblower protection. *MIT Management Sloan School*.

<https://mitsloan.mit.edu/ideas-made-to-matter/ex-google-researcher-ai-workers-need-whistleblower-protection>

<sup>28</sup> OECD. (2020). Linking Indigenous Communities with Regional Development in Canada. *OECD Rural Policy Reviews*. OECD Publishing, Paris. <https://doi.org/10.1787/fa0f60c6-en>

<sup>29</sup> Crown-Indigenous Relations and Northern Affairs Canada. (2011). A History of Treaty-Making in Canada. <https://www.rcaanc-cirnac.gc.ca/eng/1314977704533/1544620451420>

<sup>30</sup> Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021, March). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? . In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610-623). <https://dl.acm.org/doi/10.1145/3442188.3445922>

<sup>31</sup> Prime Minister of Canada, Justin Trudeau. (2022, August 9). Statement by the Prime Minister on National Peacekeepers’ Day.

<https://www.pm.gc.ca/en/news/statements/2022/08/09/statement-prime-minister-national-peacekeepers-day>

There are several positions we would like to see Canada advocate for during these negotiations that are not addressed in the treaty: (1) the use of autonomous weaponry; (2) an increased emphasis on actual, current harms of existing technologies (e.g., harms to AI workers); and (3) the assertion of collective rights and not simply personal data protection.

See our answers to other questions for explication of these points.

**5. Are there any key rights, principles, or obligations that should be included that are not currently reflected in the draft treaty? Conversely, are there any elements that raise potential concerns?**

**Movement from individual privacy to collective privacy:** Numerous reasons prompt a movement from individual to collective or community privacy. Harms are often incurred in groups and not in individuals.<sup>32</sup> AI outcomes can disproportionately affect marginalized communities and amplify race and gender inequalities.<sup>33</sup> For example, privacy violations that occur in group settings or involve data about a group's activities cannot be addressed only through personal data protection. One is not assuaged if their personal data was protected while they were falsely arrested.

Cultural, social, and ethnic groups may have unique privacy concerns that stem from their specific backgrounds and practices. For instance, an Indigenous community may exert data sovereignty to determine that the tribe determines whether the data is shared, not the individual.<sup>34</sup> This responds to the lack of consideration of Indigenous rights, which “are rarely discussed as part of this global dialogue apart from a recent report prepared by the Australian Council of Learned Academies, that discussed wellbeing, equity, self-determination and Indigenous data sovereignty.”<sup>35</sup>

Often the solution to individual privacy is aggregation of individual to collective. This presents yet another way individual privacy in AI is problematic is that the technology “allows for a new type of algorithmically assembled group to be formed that does not necessarily align with classes or attributes already protected by privacy and anti-discrimination law.”<sup>36</sup>

**Elements that raise potential concerns in the draft treaty:** The treaty excludes trans and gender non-conforming individuals in Preamble 3. AI has induced differential harms to various marginalized groups that cannot be captured in ambiguous language like “members of other

---

<sup>32</sup> Smuha, N. A. (2021). Beyond the individual: governing AI's societal harm. *Internet Policy Review*, 10(3).

<sup>33</sup> Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim Code*. New York, NY: Polity.

<sup>34</sup> Lewis, J. E., Abdilla, A., Arista, N., Baker, K., Benesiinaabandan, S., Brown, M., ... & Whaanga, H. (2020). Indigenous protocol and artificial intelligence position paper. *Indigenous AI*.  
<https://www.indigenous-ai.net/position-paper>

<sup>35</sup> Ibid.

<sup>36</sup> Mittelstadt, B. (2017). From individual to group privacy in big data analytics. *Philosophy & Technology*, 30(4), 475-494.

groups” found in Preamble 6. We propose these changes to avoid excluding and ‘othering’ these groups, especially since they are more vulnerable to AI systems, in particular facial recognition technology.

*Preamble 3. Conscious of the accelerating developments in science and technology and the profound changes brought about through [by the design, development, use and decommissioning of] artificial intelligence systems which have the potential to promote human prosperity as well as individual and societal well-being, sustainable development, gender equality and the empowerment of all women and [children/girls], and other important goals and interests, by enhancing progress and innovation;*

**Changes to Preamble 3:** Instead of "gender equality and the empowerment of all women and [children/girls]", please change to "gender equality and the empowerment of all women, trans, and gender non-conforming adults and children..."

*Preamble 6. [Expressing deep concern that discrimination in digital contexts, particularly those involving artificial intelligence systems, prevent women, [girls/children], and members of other groups from fully enjoying their human rights and fundamental freedoms, which hinders their full, equal and effective participation in economic, social, cultural and political affairs;]*

**Changes to Preamble 6:** Instead of "...prevent women, [girls/children]... and members of other groups” change to "...prevent women, trans and gender non-conforming adults and children..."

## **6. From your perspective, what impact could the obligations, rights or principles in the draft treaty have on industry and innovation in Canada?**

Broadening the obligations, rights and principles in the treaty will improve industry and innovation. For example, obligations, rights and principles and augmentations can reflect Canada's more thoughtful approach to innovation. This includes Canada’s consideration of collective rights (see First Nations Principles of OCAP® - ownership, control, access, and possession<sup>37</sup>); the respect for trans and gender non-conforming individuals; Canada’s emphasis on privacy protection; and the protection and elevation of Canadian content (which also means protection of Canadian intellectual property). Rather than impeding innovation, regulation--hard law--has been found to create greater certainty for the private sector.<sup>38</sup> Labour protections, whether here or abroad, form a necessary component of sustainable innovation. Lastly, public engagement improves user satisfaction and thus the AI system.<sup>39</sup>

## **7. In your view, are there any uses of AI that merit special treatment in the treaty?**

---

<sup>37</sup> First Nations Information Governance Centre. (2023). The First Nations Principles of OCAP®. <https://fnigc.ca/ocap-training/>

<sup>38</sup> Smuha, N. A. (2021). Beyond the individual: governing AI’s societal harm. *Internet Policy Review*, 10(3).

<sup>39</sup> Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389-399.



The use of facial recognition technology and autonomous weapons systems as AI systems merit special treatment in the treaty.

**The use of facial recognition technology:** Facial recognition technology already has proven to be harmful due to race and gender discrimination found in numerous research and reports. Facial recognition technology and human rights concerns remain prevalent, including systemic racism evidenced by the misidentification of groups, especially black women. Research by scholars like Buolamwini and Gebru found that “darker skinned females are the most misclassified group (with error rates of up to 34.7%). The maximum error rate for lighter-skinned males is 0.8%.”<sup>40</sup> Another study revealed that facial recognition technology from IBM, Amazon, Microsoft and Clarifai used images of trans men who were misidentified as women 38%. Conversely, women and men who identify as their birth gender were only misidentified 1.7% and 2.4% of the time. Facial recognition technology also misidentifies non binary people 100% of the time.<sup>41</sup> In addition, Uber’s facial recognition technology, the algorithms chosen to model faces can produce harm and “undermine [their] stated commitment to more inclusive and equitable practices.”<sup>42</sup> Facial recognition technology also can exacerbate systemic discrimination in government departments and agencies as well as other organizations.<sup>43</sup>

Despite the harm that facial recognition technology causes, its implementation by government continues with little or no transparency in democracies without any public feedback, deliberation or consultation.<sup>44</sup>

**The use of autonomous weapons systems:** Regardless of their lethality, the rise of autonomous weapons systems is deeply concerning. Loitering munitions can strike on their own or from the command of a human. Azerbaijan ended and won the 2020 six week war with Armenia using drones made by companies from Israel and Turkey. Most discussions of autonomous weapons systems focus on hardware or the presence/absence of human in the loop.<sup>45</sup> Without human intervention, autonomous weapons systems could make decisions that clash with human ethics and the laws of war. These systems are not currently capable of distinguishing civilian and military targets, which is a basic requirement of international humanitarian law. As a result, it

---

<sup>40</sup> Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research* 81, 1–15.

<https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

<sup>41</sup> Millar, M. (2019, October 30). Facial recognition technology struggles to see past gender binary. *Reuters*.

<https://www.reuters.com/article/us-usa-lgbt-facial-recognition-idUSKBN1X92OD>

<sup>42</sup> Ibid.

<sup>43</sup> House of Commons Canada. (2022, October). Facial Recognition and the Growing Power of Artificial Intelligence: *Report of the Standing Committee on Access to Information, Privacy and Ethics. 44th Parliament, 1st Session*.

<https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf>

<sup>44</sup> Garvie, C. (2019). Garbage in, garbage out: Face recognition on flawed data. *Georgetown Law, Center on Privacy & Technology*. <https://www.flawedfacedata.com/>

<sup>45</sup> Marijan, B. (2023). Regulating military use of AI. *The Ploughshares Monitor* 44, 2 Summer 2023.

[https://uploads-ssl.webflow.com/63e066081ef50cb16a3f4157/648b20bb22cf9e52e05bd085\\_SummerMonitor2023WEB.pdf](https://uploads-ssl.webflow.com/63e066081ef50cb16a3f4157/648b20bb22cf9e52e05bd085_SummerMonitor2023WEB.pdf)

becomes much easier to commit atrocities or war crimes where no individual or institution would be held accountable. Governments would not be held accountable for machines they deploy. Additionally, the use of psychological operations (PSYOPS) using deep fakes, both foreign and domestic, warrants special consideration, although we note the allusion to PSYOPS in Article 6 of the treaty. PSYOPS can create and customize very intimate and highly customized forms of propaganda. PSYOPS therefore constitute a clear threat to democratic processes and demand clarification in the treaty.

The challenge in this treaty aligns with an international human rights-based treaty that prioritizes meaningful human control. Thus far only 30 states support the Campaign to Stop Killer Robots campaign.<sup>46</sup> We note that the great powers, US, China and Russia, did not ban the development, production and use of autonomous weapons systems.<sup>47</sup> Through the rule of consensus, treaties provide the opportunity to compel certain countries to ensure humans are in the decision making loop.

National security or law enforcement are the agencies responsible for procuring and using autonomous weapons and surveillance systems. We suggest that there be no exemptions for national security or law enforcement.<sup>48 49</sup>

## **8. Are there any to regulate AI that Canada should take into consideration in its participation in the negotiations of this treaty?**

Canada is recognized as an international leader in responsible AI<sup>50</sup> with best practice policy instruments like the Directive on Automated Decision-Making and the Algorithmic Impact Assessment.<sup>51</sup> These tools were created with participation from academia, private sector, and civil society. According to the international Open Government Partnership, “While the current version of the AIA does not refer to specific human rights instruments, the intent is to account for potential impacts on rights enshrined in domestic and international human rights law.”<sup>52</sup>

---

<sup>46</sup> Stop Killer Robots Campaign. (n.d.). <https://www.stopkillerrobots.org/>

<sup>47</sup> As far as the authors are aware, the only exception is China, who agreed to not use autonomous weapons systems.

<sup>48</sup> Ifill, E. (2022, July 4). The problems with the federal data-privacy bill will disproportionately hurt marginalized Canadians. *Globe and Mail*.

<https://www.theglobeandmail.com/opinion/article-the-problems-with-the-federal-data-privacy-bill-will/>

<sup>49</sup> Centre for Media, Technology and Democracy. (2022, July 7). Roundtable on the Artificial Intelligence and Data Act. <https://www.mediatechdemocracy.com/events/roundtable-on-the-artificial-intelligence-and-data-act>

<sup>50</sup> Darbyshire, T. (2022, May 5). In Praise of the Canadian Algorithmic Impact Assessment framework. *Tech UK*.

<https://www.techuk.org/resource/in-praise-of-the-canadian-algorithmic-impact-assessment-framework.html>

<sup>51</sup> Government of Canada (2022). Responsible use of artificial intelligence (AI): Exploring the future of responsible AI in government. *Digital Government Innovation*.

<https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html>

<sup>52</sup> Perez, P., & Braithwaite, P. (2022, June 28). Algorithms and Human Rights: Understanding Their Impacts. *Open Government Partnership*.

<https://www.opengovpartnership.org/stories/algorithms-and-human-rights-understanding-their-impacts/>

Canada therefore can leverage its recognized leadership role in a measured approach to AI innovation.

There are numerous international examples of moratoria, bans, decommissionings, and hard law. We will focus on facial recognition technology, which can be used as an example for other high-risk technologies like autonomous weaponry. Regulation of AI can exist in the form of bans on certain AI systems considered to be high-risk like facial recognition technology. The use of facial recognition technology in law enforcement has come under intense scrutiny in Canada and elsewhere in the world. For example with the use of Clearview AI<sup>53</sup> which was declared unlawful by Canada's Office of the Privacy Commissioner (OPC). The OPC concluded that the use of facial recognition technology by law enforcement represented mass surveillance and a clear violation of the Personal Information Protection and Electronic Documents Act.<sup>54</sup> The UK Court of Appeal ruled that the use of facial recognition technology by police breaches data protection, equality, and privacy laws.<sup>55</sup>

The harms associated with the use of facial recognition technology by law enforcement are so significant that governments across jurisdictional levels have banned its use. US cities such as Portland, Maine, Portland, Oregon, and San Francisco and Oakland, California have banned their police forces from using the technology. At the federal level, the US Internal Revenue Service (IRS) announced that it would roll out facial recognition technology as a feature and a means for residents to file taxes.<sup>56</sup> A sufficiently large backlash occurred from civil society organizations like Algorithmic Justice League. As a result, IRS removed the facial recognition technology feature.<sup>57</sup>

In Brazil, civil society wrote and signed an open letter calling for a ban on facial recognition technology, asserting that "Despite claims of a supposed improvement in public safety [facial

---

<sup>53</sup> Stevens, Y., & Brandusescu, A. (2021, April). Weak privacy, weak procurement: The state of facial recognition in Canada. *Weak Procurement: The State of Facial Recognition in Canada*. *Centre for Media, Technology & Democracy*. <https://www.mediatechdemocracy.com/all-work/weak-privacy-weak-procurement-the-state-of-facial-recognition-in-canada>

<sup>54</sup> Government of Canada. (2021, June 10). Police use of Facial Recognition Technology in Canada and the way forward. *Office of the Privacy Commissioner of Canada*. [https://www.priv.gc.ca/en/opc-actions-and-decisions/ar\\_index/202021/sr RCMP/](https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr RCMP/)

<sup>55</sup> Winder, D. (2020, August 12). Police Facial Recognition Use Unlawful—U.K. Court Of Appeal Makes Landmark Ruling. *Forbes*. <https://www.forbes.com/sites/daveywinder/2020/08/12/police-facial-recognition-use-unlawful-uk-court-of-appeal-makes-landmark-ruling/>

<sup>56</sup> United States Government. (2022, February 7). IRS announces transition away from use of third-party verification involving facial recognition. *IRS Newsroom*. <https://www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition>

<sup>57</sup> Metz, R. (2022, March 7). Activists pushed the IRS to drop facial recognition. They won, but they're not done yet. *CNN*. <https://www.cnn.com/2022/03/07/tech/facial-recognition-activists-irs/index.html>

recognition technology] reproduces the culture of punitivism and incarceration, instead of focusing on prevention and restoration measures.”<sup>58</sup>

The use of facial recognition technology by law enforcement represented mass surveillance and a clear violation of privacy from the Canadian Civil Liberties Association.<sup>59</sup> In Canada, Open Media, a Canadian digital rights non-profit, launched the “Stop Clearview AI’s Facial Recognition” campaign to provide support for individuals to retrieve data about them from Clearview AI, a facial recognition technology company.<sup>60</sup> Amnesty International Canada published a letter calling for the immediate ban on facial recognition technology for Canada’s law enforcement and intelligence agencies.<sup>61</sup> The American Civil Liberties Union has petitioned the US to halt facial recognition technologies.<sup>62 63</sup>

The European Parliament adopted a ban on facial recognition technology. However, the rights of migrants, refugees and asylum seekers are not protected.<sup>64</sup> Therefore, the treaty should extend the right to non-citizens and individuals with provisional status.

---

<sup>58</sup> #TireMeuRostoDaSuaMira. (2022). Open Letter to Ban the Use of Digital Facial Recognition Technologies in Public Security. <https://tiremeurostodasuamira.org.br/open-letter-en/>

<sup>59</sup> McPhail, B. (2021, February 3). Clearview AI Engaged In “Mass Surveillance”. Canadian Civil Liberties Association. <https://ccla.org/privacy/surveillance-technology/clearview-ai-engaged-in-mass-surveillance/>

<sup>60</sup> Open Media. (n.d.). Police technology is out of control! <https://action.openmedia.org/page/119050/petition/1>

<sup>61</sup> Amnesty International Canada. (2020). Open Letter: Canadian Government Must Ban Use of Facial Recognition Surveillance by Federal Law Enforcement, Intelligence Agencies. *Amnesty International Canada News*. <https://amnesty.ca/human-rights-news/open-letter-canadian-government-must-ban-use-of-facial-recognition-surveillance-by-federal-law-enforcement-intelligence-agencies/>

<sup>62</sup> American Civil Liberties Union. (n.d.). Petition to Halt Dangerous Face Recognition Technologies. <https://action.aclu.org/petition/halt-dangerous-face-recognition-technologies>

<sup>63</sup> Edinger, J. (2021, July 16). Facial Recognition Creates Risks for Trans Individuals, Others. *GovTech*. <https://www.govtech.com/products/facial-recognition-creates-risks-for-trans-individuals-others>

<sup>64</sup> Amnesty International. (2023, June 14). EU: European Parliament adopts ban on facial recognition but leaves migrants, refugees and asylum seekers at risk. <https://www.amnesty.org/en/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/>