To:
The Honourable François-Philippe Champagne, P.C., M.P., Minister of Innovation, Science and Industry
The Honourable Dominic LeBlanc, P.C., M.P., Minister of Public Safety
Joël Lightbound, Chair of the Standing Committee on Industry and Technology

CC:
The Honourable Harjit Singh Sajjan, Minister of Emergency Preparedness
The Honourable Pierre Poilievre, P.C., M.P., Leader of the Opposition
Yves-François Blanchet M.P., Bloc Québécois Leader
Jagmeet Singh M.P., NDP Leader
Elizabeth May M.P., Green Party Parliamentary Leader
Members of the Standing Committee on Access to Information, Privacy and Ethics
Members of the Standing Committee on Industry and Technology

Dear Ministers,

Joint letter on Bill C-27's impact on oversight of facial recognition technology

As Bill C-27 comes to study by the Standing Committee on Industry and Technology (INDU), the Right2YourFace Coalition expresses our deep concerns with what Bill C-27 means for oversight of facial recognition technology (FRT) in Canada.

FRT is a type of biometric recognition technology that uses artificial intelligence (AI) algorithms and other computational tools to ostensibly identify individuals based on their facial features. Researchers have found that these tools are about as invasive as technologies get. Biometric data, such as our faces, are inherently sensitive types of information. As mentioned in our Joint Letter of Concern regarding the government's response to the ETHI Report on Facial Recognition Technology and the Growing Power of Artificial Intelligence, the use of FRT threatens human rights, equity principles, and fundamental freedoms including the right to privacy, freedom of association, freedom of assembly, and the right to non-discrimination. AI systems are being adopted at an increasingly rapid pace and Canada needs meaningful legislation to prevent the harms that FRT poses. As it stands, Bill C-27 is *not* that legislation – it is not fit for purpose and is in dire need of significant amendments.

Bill C-27 is comprised of three parts and our concerns lie primarily with two of them: The *Consumer Privacy Protection Act* (CPPA) and the *Artificial Intelligence and Data Act* (AIDA). The CPPA creates the rules for data collection, use, and privacy that flow into implementations covered by the *Artificial Intelligence and Data Act* (AIDA). While implementations like FRT are the target of AIDA, the datasets FRT systems rely on must be collected and used under the

terms of the CPPA. Consequently, we submit that both CPPA and AIDA require amendments to fully protect vulnerable biometric information.

We have identified five core issues with the Bill, including elements of both the CPPA and AIDA, that require immediate attention in order to avoid significant harm. They are:

1. The CPPA does not flag biometric information as sensitive information, and it does not define "sensitive information" at all. This omission leaves some of our most valuable and vulnerable information—including the faces to which we must have a right—without adequate protections;
2. The CPPA's "legitimate business purposes" exemption is too broad and will not protect consumers from private entities wishing to use FRT;
3. "High impact systems" is undefined in AIDA. Leaving this crucial concept to be defined later in regulations leaves Canadians without meaningful basis from which to assess the impact of the Act, and FRT must be included;
4. AIDA does not apply to government institutions, including national security agencies who use AI for surveillance, and exempts private sector AI technology developed for use by those national security agencies - creating an unprecedented power imbalance; and
5. AIDA focuses on the concept of individual harm, which excludes the impacts of FRT on communities at large.

Biometric information is sensitive information and must be defined as such

Not all data are built the same, and they should not be treated the same. Biometric information is a particularly sensitive form of information that goes to the core of an individual's identity. It includes, but is not limited to, face data, fingerprints, and vocal patterns, and carries with it particular risk for racial and gender bias. Biometric information must be considered as sensitive information and afforded relevant protections. While the CPPA mentions sensitive information in reference to the personal information of minors, the text of the Act neither defines nor protects it. This leaves some of our most valuable and vulnerable identifiable information without adequate protection. The CPPA should include special provisions for sensitive information, and its definition should explicitly provide for enhanced protection of biometric data - understanding that the safest biometric data is biometric data that does not exist.

"Legitimate business purposes" requires a better definition to protect against abuse

The CPPA states in provision 12(2) that purposes which "represent legitimate business needs of the organization" are appropriate purposes to collect user information without the user's knowledge or consent. It is not difficult to see businesses framing their use of FRT as in service of legitimate business purposes like loss prevention, which is already happening in the private sector despite being established as violating Canadian privacy law. Disturbingly, the CPPA's

legitimate business purpose loophole tilts the scales in favour of business over personal privacy, suggesting that individuals' privacy rights are less important than profit.

It should be demonstrably clear that a person's rights and freedoms must be adequately balanced. Provision 5 of the CPPA states that the purpose of the Act is to establish "rules to govern the protection of personal information." Businesses, thus, should not be given free rein to decide that their use of FRT—and the risks to privacy that come with the use and collection of that highly sensitive data—qualifies as legitimate and that biometric data could be collected without an individual knowing or consenting.

What is a high-impact system?

AIDA imposes additional measures on "high-impact systems", requiring those who administer them to "assess and mitigate risks of harm or biased output." Given that FRT and its associated AI systems have the ability to identify individuals using the above-mentioned biometric information, FRT must be considered high-impact. Yet, the Act offers no definition of what qualifies as high-impact, instead leaving this crucial step to the regulations.

The risk-based analysis associated with high-impact systems suggested by the wording in AIDA takes us down the wrong path. Would a grocery store's coupon-distribution system be considered high-impact and thus require assessment and mitigation of risks of harm or biased output? What if that system were using FRT? What may seem to be a low-impact system of coupon distribution may in fact be incorporating and collecting biometric data. Given the risks and harms that FRT poses for human rights and fundamental freedoms, FRT's impacts are both high *and* dangerous.

A rights-based analysis must accompany risks-based calculations. A definition of high-impact systems that includes FRT and other biometric identification technologies must be included in the bill itself.

National Security is absent from the Bill but must be addressed within it

Section 3(2) of AIDA states that the Act does not apply to a "product, service, or activity under the direction or control of" government institutions including the Department of National Defence (DND), the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE), or "any other person who is responsible for a federal or provincial department or agency and who is prescribed by regulation." In plain language, private sector technology developed to be used by any of these institutions is exempt from AIDA's reach. Given FRT's connection to broader surveillance and AI-driven systems, excluding the DND, CSIS, and CSE—three pillars of Canada's surveillance infrastructure—from AIDA leaves room for gross violations of privacy in the name of state security.

Further, provision 3(2)(d) gives regulators the ability to exclude whichever department or agency they please any time *after* AIDA has passed. This runs counter to the notion of accountable government and creates the risk that other organizations and departments using or wanting to use FRT may escape meaningful regulation and public consultation.

Collective - not just individual - harm must be considered

While protection of individuals' data is central to AIDA, Parliament must remember that AI in general and FRT in particular is built on collective data that may pose collective harms to society. FRT systems are consistently less accurate for racialized individuals, children, elders, members of the LGBTQ+ community, and disabled people – which is in direct conflict with C-27's intent to restrict biased outputs. This makes the inclusion of collective harm in C-27 all the more necessary.

Final Remarks

The above-outlined issues are by no means exhaustive but are crucial problems that leave Bill C-27 unequipped to protect individuals and communities from the risks of FRT. While we agree that Canada's privacy protections need to meet the needs of an ever-evolving digital landscape, legislative and policy changes cannot be made at the cost of fundamental human rights or meaningful privacy protections. Parliament must meaningfully address these glaring issues. Together, we can work toward a digital landscape that prioritizes privacy, dignity, and human rights over profit.

Sincerely,

Canadian Civil Liberties Association

Privacy and Access Council of Canada

Ligue des droits et libertés

International Civil Liberties Monitoring Group

Criminalization and Punishment Education Project

The Dais at Toronto Metropolitan University

Digital Public

Tech Reset Canada

BC Freedom of Information and Privacy Association

1. Aaron Tucker, Postdoctoral Scholar, University of Toronto
2. Adam Molnar, Assistant Professor, Sociology and Legal Studies, University of Waterloo
3. Alison Harvey, York University
4. Alessandra Puopolo, Technology and legal rights advocate
5. Ana Brandusescu, McGill University
6. Bianca Wylie, writer and public technology advocate
7. Brenda McPhail, Acting Executive Director, Master of Public Policy in Digital Society, McMaster University
8. Charles Luke Stark, Assistant Professor, Faculty of Information and Media Studies, Western University
9. Christelle Tessono, Tech Policy Researcher
10. Daniel Konikoff, Canadian Civil Liberties Association
11. Danielle Thompson, PhD Candidate, Sociology and Legal Studies, University of Waterloo
12. Evan Light, York University
13. Fenwick McKelvey, Concordia University; Director of the Algorithmic Media Observatory
14. Florian Martin-Bariteau, Associate Professor of Law and University Research Chair in Technology and Society, University of Ottawa.
15. Jane Bailey, Professor, University of Ottawa Faculty of Law
16. Joanna Redden, Associate Professor, Faculty of Information and Media Studies, Western University
17. Joe Masoodi, The Dais, Toronto Metropolitan University
18. Justin Piché, PhD, Associate Professor, Criminology, University of Ottawa
19. Kanika Samuels-Wortley, Associate Professor and Canada Research Chair in in Systemic Racism, Technology, and Criminal Justice
20. Kate Winiarz, Canadian Civil Liberties Association
21. Kristen Thomasen, Assistant Professor, Peter A Allard School of Law, UBC
22. Laurence Guénette, Coordinator of the Ligue Des Droits et Libertés
23. Matthew Malone, Assistant Professor, Faculty of Law, Thompson Rivers University
24. Mike Larsen, BC Freedom of Information and Privacy Association
25. Prem Sylvester, Researcher, Digital Democracies Institute
26. Petra Molnar, York University and Harvard University
27. Sébastien Gambs, Professor and Canada Research in Privacy-preserving and Ethical Analysis of Big Data, Université du Québec à Montréal
28. Seher Shafiq, Writer
29. Sharon Polsky, Privacy and Access Council of Canada

30. Tim McSorley, International Civil Liberties Monitoring Group

—

Destinataires :
L'honorable Dominic LeBlanc, C.P., député, ministre de la Sécurité publique
L'honorable François-Philippe Champagne, C.P., député, ministre de l'Innovation, des Sciences et de l'Industrie
Joël Lightbound, président du Comité permanent de l'industrie et de la technologie

c. c.:
L'honorable Harjit Singh Sajjan, ministre de la Protection civile
L'honorable Pierre Poilievre, C.P., député, chef de l'opposition
Yves-François Blanchet, député, chef du Bloc Québécois
Jagmeet Singh, député, chef du NPD
Elizabeth May, députée, leader parlementaire du Parti vert
Membres du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI)
Membres du Comité permanent de l'industrie et de la technologie (INDU)
Mesdames et messieurs les ministres,

Lettre transpartisane sur l'incidence du projet de loi C-27 sur la surveillance des technologies de reconnaissance faciale

À la veille de l'étude du projet de loi C-27 par le Comité permanent de l'industrie et de la technologie (INDU), la coalition Right2YourFace exprime ses profondes préoccupations quant aux implications du projet de loi C-27 pour la surveillance de la technologie de reconnaissance faciale (TRF) au Canada.

La TRF est un type de technologie de reconnaissance biométrique qui fait appel aux algorithmes d'intelligence artificielle (IA) et à d'autres outils informatiques ostensiblement pour identifier des personnes d'après les traits de leur visage. Les chercheurs ont constaté que ces outils technologiques sont parmi les plus envahissants qui soient. Les données biométriques, comme nos visages, sont des types de renseignements sensibles en soi. Comme nous l'avons mentionné dans notre lettre de préoccupation transpartisane concernant la réponse du gouvernement au Rapport sur la technologie de reconnaissance faciale et le pouvoir grandissant de l'intelligence artificielle de l'ETHI, le recours à la TRF menace les droits de la personne, les principes d'équité et les libertés fondamentales, notamment le droit à la vie privée, la liberté d'association, la

liberté de réunion et le droit à la non-discrimination. Les systèmes d'IA sont adoptés à un rythme de plus en plus rapide et le Canada a besoin d'une mesure législative significative pour prévenir les préjudices causés par la TRF. Dans sa formule actuelle, le projet de loi C-27 n'est *pas* cette mesure. Il n'est pas adapté à l'objectif visé et nécessite des modifications importantes.

Le projet de loi C-27 comprend trois parties et nos préoccupations portent principalement sur deux d'entre elles : la *Loi sur la protection de la vie privée des consommateurs* (LPVPC) et la *Loi sur l'intelligence artificielle et les données* (LIAD). La LPVPC énonce les règles relatives à la collecte, à l'utilisation et à la confidentialité des données qui s'appliquent aux mises en œuvre régies par la *Loi sur l'intelligence artificielle et les données* (LIAD). Si la LIAD régit des applications comme la TRF, la LPVPC régit la collecte et l'utilisation des ensembles de données sur lesquels les systèmes de TRF s'appuient. Par conséquent, nous estimons que la LPVPC et la LIAD doivent être modifiées afin de protéger pleinement les renseignements biométriques vulnérables.

Nous avons recensé cinq problèmes fondamentaux liés au projet de loi, y compris des éléments de la LPVPC et de la LIAD, qui requièrent une attention immédiate afin d'éviter des préjudices importants. Ce sont les suivants :

1. La LPVPC ne considère pas les renseignements biométriques comme des renseignements sensibles et ne définit pas du tout ce qu'est un « renseignement sensible ». Cette omission laisse certains de nos renseignements les plus précieux et les plus vulnérables – y compris notre visage qui doit être protégé par le droit – sans protection adéquate.
2. L'exemption prévue par la LPVPC pour les « besoins commerciaux légitimes » est trop large et ne protégera pas les consommateurs contre les entités privées qui souhaitent utiliser la TRF.
3. L'expression « système à incidence élevée » n'est pas définie dans la LIAD. En reportant la définition de ce concept essentiel dans les règlements, on prive les Canadiens d'une base significative pour évaluer l'incidence de la loi, et la TRF doit en faire partie.
4. La LIAD ne s'applique pas aux institutions gouvernementales, y compris les agences de sécurité nationale qui utilisent l'IA à des fins de surveillance, et exempte les technologies d'IA du secteur privé mises au point pour être utilisées par ces agences de sécurité nationale, ce qui crée un déséquilibre de pouvoir sans précédent.
5. La LIAD se concentre sur le concept de préjudice individuel, ce qui exclut l'incidence de la TRF sur les collectivités dans leur ensemble.

Les renseignements biométriques sont des renseignements sensibles et doivent être définis comme tels

Toutes les données ne sont pas construites de la même manière et il n'existe pas de traitement universel de celles-ci. Les renseignements biométriques sont une forme particulièrement sensible de renseignements qui touchent au cœur de l'identité d'un individu. Ils comprennent, entre autres, les données faciales, les empreintes digitales et les modèles vocaux, et comportent un risque particulier de préjugés raciaux et sexistes. Les renseignements biométriques doivent être considérés comme des renseignements sensibles et bénéficier des protections appropriées. Bien que la LPVPC mentionne les renseignements sensibles en référence aux renseignements personnels des mineurs, le texte de la loi ne les définit pas et ne les protège pas. Certains de nos renseignements identifiables les plus précieux et les plus vulnérables ne bénéficient donc pas d'une protection adéquate. La LPVPC devrait prévoir des dispositions particulières pour les renseignements sensibles, et sa définition devrait explicitement prévoir une protection renforcée des données biométriques – étant entendu que les données biométriques les plus sûres sont les données biométriques qui n'existent pas.

La notion de « besoins commerciaux légitimes » doit être mieux définie pour éviter les abus

L'article 12, paragraphe 2, de la LPVPC stipule que les fins qui « correspondent à des besoins commerciaux légitimes de l'organisation » sont des fins acceptables pour collecter des renseignements sur l'utilisateur à son insu ou sans son consentement. Il n'est pas difficile de voir des entreprises présenter leur utilisation de la TRF comme étant au service d'objectifs commerciaux légitimes tels que la prévention des pertes, ce qui est déjà le cas dans le secteur privé bien qu'il soit établi qu'il s'agit d'une violation de la *Loi sur la protection des renseignements personnels du Canada*. Il est inquiétant de constater que l'échappatoire de la LCVPC concernant les besoins commerciaux légitimes fait pencher la balance en faveur des entreprises plutôt que de la vie privée, suggérant que le droit à la vie privée des individus est moins important que le profit.

Il devrait être clairement établi que les droits et les libertés d'une personne doivent être adéquatement pris en considération. La disposition 5 de la LPVPC stipule que l'objectif de la loi est d'établir « des règles régissant la protection des renseignements personnels ». Les entreprises, par conséquent, ne devraient pas avoir carte blanche pour décider que leur utilisation de la TRF – et les risques pour la protection des renseignements personnels qui accompagnent l'utilisation et la collecte de ces données très sensibles – est légitime et que les données biométriques peuvent être collectées à l'insu de l'intéressé ou sans son consentement.

Qu'est-ce qu'un système à incidence élevée?

La LIAD impose des mesures supplémentaires aux « systèmes à incidence élevée », exigeant de leurs administrateurs qu'ils « évaluent et atténuent les risques de préjudices ou de résultats biaisés ». Étant donné que la TRF et les systèmes d'IA qui lui sont associés ont la capacité d'identifier des personnes à partir des renseignements biométriques susmentionnés, la TRF doit

être considérée comme ayant une incidence élevée. Cependant, la loi ne donne aucune définition de ce qui constitue une incidence élevée, laissant cette étape cruciale à la réglementation.

L'analyse fondée sur le risque associé aux systèmes à incidence élevée suggérée par la formulation de la LIAD nous mène sur la mauvaise voie. Le système de distribution de bons de réduction d'un magasin d'alimentation serait-il considéré comme ayant une incidence élevée et nécessiterait-il donc une évaluation et une atténuation des risques de dommages ou de résultats biaisés? Et si ce système utilisait la TRF? Ce qui peut sembler être un système de distribution de bons à faible incidence peut en fait incorporer et collecter des données biométriques. Compte tenu des risques et des préjudices que la TRF fait peser sur les droits de la personne et les libertés fondamentales, les incidences de la TRF sont à la fois élevées *et* dangereuses.

Une analyse fondée sur les droits doit accompagner les calculs fondés sur les risques. Une définition des systèmes à incidence élevée englobant la TFR et d'autres technologies d'identification biométrique doit être incluse dans le projet de loi lui-même.

La Sécurité nationale est absente du projet de loi, mais elle doit être abordée dans le cadre de celui-ci

L'article 3, paragraphe 2, de la LPVPC stipule que la loi ne s'applique pas aux « à l'égard des produits, services ou activités qui relèvent de la compétence ou de l'autorité » d'institutions gouvernementales, notamment le ministère de la Défense nationale (MDN), le Service canadien du renseignement de sécurité (SCRS), le Centre de la sécurité des télécommunications (CST), ou de « toute autre personne qui est responsable d'un ministère ou d'un organisme fédéral ou provincial et qui est désignée par règlement ». En clair, les technologies du secteur privé mises au point pour être utilisées par l'une ou l'autre de ces institutions sont exclues du champ d'application de la LIAD. Étant donné le lien entre la TRF et les systèmes de surveillance et d'IA plus larges, l'exclusion du MDN, du SCRS et du CST – trois piliers de l'infrastructure de surveillance du Canada – de la LIAD laisse place à des violations flagrantes de la vie privée au nom de la sécurité de l'État.

De plus, l'alinéa 3(2)d) donne au législateur la possibilité d'exclure le ministère ou l'agence de son choix à tout moment *après* l'adoption de la LIAD. Cela va à l'encontre de la notion de gouvernement responsable et entraîne le risque que d'autres organisations et ministères utilisant ou souhaitant utiliser la TRF échappent à une réglementation significative et à une consultation publique.

Le préjudice collectif – et pas seulement individuel – doit être pris en considération

Si la protection des données individuelles est au cœur de la LIAD, le Parlement ne doit pas oublier que l'IA en général et la TRF en particulier reposent sur des données collectives

susceptibles de causer des préjudices collectifs à la société. Les systèmes de TRF sont systématiquement moins précis pour les personnes racialisées, les enfants, les personnes âgées, les membres de la communauté LGBTQ+ et les personnes handicapées, ce qui est en contradiction directe avec l'intention du projet de loi C-27 de limiter les résultats biaisés. Cela rend d'autant plus nécessaire l'inclusion du préjudice collectif dans le projet de loi C-27.

Observations finales

Les questions susmentionnées ne sont en aucun cas exhaustives, mais constituent des problèmes cruciaux associés à l'échec du projet de loi C-27 de protéger les individus et les collectivités contre les risques de la TRF. Si nous convenons que les protections de la vie privée au Canada doivent répondre aux besoins d'un paysage numérique en constante évolution, les changements législatifs et politiques ne peuvent se faire au détriment des droits de la personne fondamentaux ou de protections significatives des renseignements personnels. Le Parlement doit s'attaquer sérieusement à ces problèmes flagrants. Ensemble, nous pouvons œuvrer en faveur d'un paysage numérique qui privilégie la protection des renseignements personnels, la dignité et les droits de la personne plutôt que le profit.

Nous vous prions d'agréer, Mesdames et messieurs les ministres, l'expression de notre considération respectueuse.

Association canadienne des libertés civiles

Conseil du Canada de l'accès à la vie privée

Ligue des droits et libertés

Coalition pour la surveillance internationale des libertés civiles

Projet d'éducation sur la criminalisation et la punition

The Dais à Toronto Metropolitan University

Digital Public

Tech Reset Canada

BC Freedom of Information and Privacy Association

–

Aaron Tucker, Postdoctoral Scholar, University of Toronto

Adam Molnar, Assistant Professor, Sociology and Legal Studies, University of Waterloo

Alison Harvey, Université York

Alessandra Puopolo, avocate de la technologie et des droits juridiques

Ana Brandusescu, Université McGill

Bianca Wylie, écrivaine et défenseur public de la technologie

Brenda McPhail, Directrice exécutif par intérim, maîtrise en politiques publiques dans la société numérique, Université McMaster

Charles Luke Stark, Professeur adjoint, Faculté des études de l'information et des médias, Université Western

Christelle Tessono, Chercheuse en politique technologique

Daniel Konikoff, Association canadienne des libertés civiles

Danielle Thompson, Candidate au doctorat, sociologie et études juridiques, Université de Waterloo

Evan Light, Université York

Fenwick McKelvey, Université Concordia; Directeur de l'Observatoire Algorithmique des Médias

Florian Martin-Bariteau, Professeur agrégé de droit et Chaire de recherche universitaire en technologie et société, Université d'Ottawa

Jane Bailey, Professeure, Faculté de droit de l'Université d'Ottawa

Joanna Redden, Professeur agrégé, Faculté des études de l'information et des médias, Université Western

Joe Masoodi, The Dais, Université métropolitaine de Toronto

Justin Piché, PhD, Professeur agrégé, criminologie, Université d'Ottawa

Kanika Samuels-Wortley, Professeur agrégé et Chaire de recherche du Canada sur le racisme systémique, la technologie et la justice pénale

Kate Winiarz, Association canadienne des libertés civiles

Kristen Thomasen, Professeur adjoint, Faculté de droit Peter A Allard, UBC

Laurence Guénette, Coordonnatrice Ligue Des Droits et Libertés

Matthew Malone, Professeur adjoint, Faculté de droit, Université Thompson Rivers

Mike Larsen, Association pour l'accès à l'information et la protection de la vie privée de la Colombie-Britannique

Prem Sylvester, Chercheur, Institut des démocraties numériques

Petra Molnar, Université et Université Harvard

Sébastien Gambs, Professeur et Chaire de recherche du Canada en analyse respectueuse de la vie privée et éthique des données massives, Université du Québec à Montréal

Seher Shafiq, écrivaine

Sharon Polsky, Conseil canadien de la protection de la vie privée et de l'accès

Tim McSorely, Coalition pour la surveillance internationale des libertés civiles

ETHI LETTER OF CONCERN RECORDKEEPING

To:
The Honourable Marco E. L. Mendicino, P.C., M.P., Minister of Public Safety
The Honourable François-Philippe Champagne, P.C., M.P., Minister of Innovation, Science and Industry
Joël Lightbound, Chair of the Standing Committee on Industry and Technology

CC:
The Honourable Bill Blair, Minister of Emergency Preparedness
The Honourable Pierre Poilievre, P.C., M.P., Leader of the Opposition
Yves-François Blanchet M.P., Bloc Québécois Leader
Jagmeet Singh M.P., NDP Leader
Elizabeth May M.P., Green Party Parliamentary Leader
The Honourable Michelle Rempel Garner, P.C., M.P., Parliamentary Caucus on Emerging Technology
The Honourable Colin Deacon, Senator, Parliamentary Caucus on Emerging Technology
Members of the Standing Committee on Access to Information, Privacy and Ethics
Members of the Standing Committee on Industry and Technology

Joint Letter of Concern regarding the government's response to the ETHI Report on Facial Recognition Technology and the Growing Power of Artificial Intelligence

Dear Ministers,

We are writing to express our concerns with the **government's response** to the recent publication of the Committee on Access to Information, Privacy and Ethics (ETHI) report, "**Facial Recognition Technology and the Growing Power of Artificial Intelligence.**" After careful review, we find that it fails to address the severity of the challenges caused by facial recognition technology (FRT) and artificial intelligence (AI). Canada needs to take action now.

The ETHI Committee's study confirmed that Canada's current legislation does not adequately regulate facial recognition technology and artificial intelligence. While discussions concerning FRT often focus on security and surveillance, the report demonstrates how FRT and AI systems are increasingly being adopted across many Canadian sectors, including retail, e-commerce, and healthcare - quickly becoming ubiquitous in daily life.

Critically, these technologies threaten many human rights, equity principles, and fundamental freedoms, including the right to privacy, freedom of association, freedom of assembly, freedom of expression and right to non-discrimination. These harms are not only caused by the real-time

use of FRT, but by FRT's connection to broader surveillance and AI driven systems, such as its use in populating biometric databases and training of AI algorithms. Without adopting a robust legislative framework to govern this invasive technology, there is a pervasive and increasing risk of individual, collective, and social harm.

The ETHI Committee's recommendations are generally strong and represent a meaningful step towards the responsible governance of FRT and AI in Canada. Through a participatory approach, the Committee listened to feedback and advice from a range of witnesses, whose recommendations were reflected in the report.

Significantly, the ETHI Committee acknowledges the disproportionate implications FRT has for historically racialized and marginalized communities, particularly because of biased and inaccurate algorithms. Consequently, the Committee calls on the government to invest in studying and disclosing such impacts. This is an important recommendation. However, even if increased accuracy is achieved within FRT applications, and technical bias is resolved, we note that the technology still raises serious concerns. If left unregulated, the use of more accurate facial recognition technologies will become even more detrimental to groups that already experience systemic discrimination. The use of FRT would further exacerbate inequalities through more perfect targeting of those who are already disproportionately surveilled such as unhoused communities, sex workers, individuals who receive income assistance, among others.

The ETHI Committee's report also considers some of the ways in which FRT could benefit society. This Coalition is of the view that even if there are positive uses for this technology, proper regulatory safeguards are necessary to ensure that any potentially socially beneficial purposes are fulfilled, and harmful uses are prohibited.

This Coalition would like to highlight what we believe are the key recommendations for government action purposed by the ETHI Committee:

- Imposing a federal moratorium on the use of facial recognition technology by federal policing services and Canadian industries until a robust regulatory framework is developed and implemented.
- Developing a regulatory framework that defines acceptable and unacceptable uses of facial recognition technology with a view to protect individuals and communities against mass surveillance, with clear penalties for violations by police.
- Increasing transparency mechanisms for the disclosure of racial, age, or other biases that exist in FRT and policy measures with participation frameworks for these marginalized groups to address such issues.
- Restricting private sector entities from requiring biometric information as a condition of service.

- Amending the *Privacy Act* and PIPEDA to prohibit entities from capturing images of Canadians from the internet or public spaces for the purpose of populating FRT databases or AI algorithms.
- Strengthening the ability of the Privacy Commissioner to impose meaningful penalties on entities that break the law and to be engaged in regulatory reform concerning FRT.
- Increasing transparency and oversight mechanisms for the use of FRT in the context of national security and procurement.

In its reply, the government failed to address many of the key recommendations made by the ETHI Committee. The government instead relied upon nascent or outdated pieces of privacy legislation that, in their current form, are unable to address the serious risks and challenges caused by the adoption and deployment of facial recognition technologies. This Coalition would like to highlight some of the crucial areas where the government reply was inadequate.

Lack of Engagement with the Calls for a Federal Moratorium on the Use of FRT

The government has not adequately addressed the Committee's Recommendation 18, that calls for a federal moratorium on the use of facial recognition technology by federal police services. In June 2022, in response to the Standing Committee's Report on Systemic Racism in Policing in Canada, the Minister of Public Safety announced the government's commitment to addressing racial bias within Canadian policing. As previously discussed, the ETHI Report acknowledges that FRT can exacerbate racial inequalities and can contribute to the over-policing of equity deserving communities. Given the highly invasive nature of FRT and the fundamental rights at stake, Canada cannot continue to wait for legislative amendments to the Privacy Act and should enact a moratorium until adequate regulations are in place to protect against discrimination and prescribe appropriate standards for law enforcement.

Instructive lessons can be learned from other jurisdictions. In 2021, the European Union instituted a ban on FRT by law enforcement in public spaces. In 2022, the Italian government prohibited the use of FRT until adequate legislation could be passed to regulate the technology. Similarly, numerous American municipalities, including San Francisco, have banned the use of FRT by police and other public agencies. In Canada, a moratorium is possible and should be adopted.

The Federal Government Should Assume a Leadership Role in Responsible Tech Policy

In its reply, the government noted that jurisdictional issues preclude it from regulating the use of FRT by provincial police forces. However, the RCMP maintains over 700 detachments in 150 communities across Canada and provides policing services in over 600 Indigenous communities. The scope of the RCMP's jurisdiction is significant.

Given Canada's current patchwork of privacy legislation, the federal government should work with provincial and territorial leaders to promote the development of a comprehensive regulatory framework for FRT. The federal government can and should play a leadership role in developing and guiding responsible tech policy. Looking forward, concerted effort from the federal government is required.

The Treasury Board Directive is Limited in Scope and Lacks Transparency Mechanisms

In its response, the government relies heavily on the Treasury Board Directive on Automated Decision Making to protect against the irresponsible use of FRT by federal departments. However, in its current form this instrument will not solve many of the issues related to the government's use of FRT and AI. The scope of the Directive is limited. It covers only external and not internal services, such as automated decisions that impact federal employees. Moreover, national security systems are exempt, as well as systems developed or procured before April 1, 2020.

The Directive does not promote transparency because it does not define nor expand upon key reporting processes. For example, under the Directive individuals are entitled to receive a "meaningful explanation" for decisions made by an automated process employed by a federal department, but the Directive does not define or set a standard for what constitutes a meaningful explanation. Additionally, the instrument does not contain any mechanisms to provide the public with a justification for the government's decision to adopt an AI system in the first place.

Bill C-27 Will Not Protect Individuals' Privacy Rights and Leaves Stakeholders Behind

The ETHI Committee's report demonstrates that prompt and meaningful legislative action is required to protect the rights of individuals in Canada. Other jurisdictions have begun taking the necessary steps to ensure responsible governance of FRT as evidenced by the European Union's recent proposed Artificial Intelligence Act, or even biometric-specific legislation, such as Illinois's Biometric Information Privacy Act. In comparison, despite unified calls from Federal, Provincial, and Territorial Privacy Commissioners to establish a legal framework for FRT, Canada's regulatory framework has remained largely stagnant.

While Bill C-27 is a necessary first step in regulating the use of artificial intelligence and updating Canada's privacy legislation, it ultimately falls short of addressing the risks and recommendations identified in the ETHI Committee's report. The legislation was largely developed without necessary input from key stakeholders including civil society groups, researchers, and historically marginalized communities as stated by the ETHI Committee in Recommendation 10. Bill C-27 fails to comprehensively consider the human rights implications

of AI, particularly its potential for collective and diffuse harms, in addition to individual and targeted harms.

Bill C-27's *Consumer Privacy Protection Act*, the new legislation to regulate industry, irresponsibly prioritizes the rights of businesses over individuals in Canada. Critically, it will permit businesses to collect and use individuals' information without their consent for certain activities. Additionally, it is notably silent on special protections for sensitive personal information such as biometric data including faces, fingerprints, and vocal patterns. Instead, almost all types of data are treated the same.

Similarly, Bill C-27's *Artificial Intelligence and Data Act* (AIDA) is wrought with issues. It is limited in scope and leaves many important aspects of the proposed framework to future regulations, thereby undermining transparency. Key provisions such as the definition of high-impact AI systems have been omitted, leaving their formulation to a later date. While the AIDA Companion document lists biometric information of "interest" to the government, biometric information, which goes to the core of individuals' identity, has not been explicitly identified as sensitive information within the legislation itself. These details should be included in the core of the legislation, and follow the government's pattern of leaving key elements to future regulations. AI systems developed by the private sector for use by national security agencies are also exempt from AIDA, creating a troubling exclusion for some of the highest risk uses of these tools. Additionally, businesses have been granted far-reaching discretion to make decisions about what might be in their own legitimate business interest, without a full recognition enshrined in the Act that what they are making decisions about is not an individual's privacy "interest", but an individual's fundamental human rights.

Facial recognition technology and artificial intelligence pose a serious risk to a range of fundamental human rights, including equity, privacy, non-discrimination, and freedom of expression. Despite the high-risks associated with these technologies, absent clear legislative standards, they are increasingly being used in ways that are invasive, arbitrary, and irresponsible by law enforcement, private entities, and governments in Canada. The Canadian Government has a responsibility to ensure that individuals' rights are not subverted with the emergence of AI driven technologies.

We hope that the government will reconsider the recommendations made by the ETHI Committee as it seeks to amend and develop new legislation. As regulations to address the issues posed by FRT move through the legislative process, we look forward to working with you to craft a robust regulatory framework.

Sincerely,

Brenda McPhail, Acting Executive Director, Master of Public Policy in Digital Society, McMaster University

Kanika Samuels-Wortley, Researcher & Professor, Toronto Metropolitan University

Christelle Tessono, Tech Policy Researcher

Alessandra Puopolo, Project Coordinator & Researcher, Canadian Civil Liberties Association

Prem Sylvester, Researcher, Digital Democracies Institute

Tim McSorley, National Coordinator, International Civil Liberties Monitoring Group

Aaron Tucker, Academic, University of Toronto

Adam Molnar, Assistant Professor, Sociology and Legal Studies, University of Waterloo

Alana Saulnier, Criminologist, Assistant Professor, Queen's University

Dr. Kristen Thomasen, Legal Academic

Evan Light, Associate Professor, York University

Fenwick McKelvey, Concordia University

Joanna Redden, Associate Professor Western University

Joe Masoodi, The Dais, Toronto Metropolitan University

Jon Penney, Academic, Osgoode Hall Law School & Citizen Lab

Karim Benyekhlef, Ad.E., Professeur et directeur du Laboratoire de cyberjustice, Faculté de droit, Université de Montréal

Luke Stark, Assistant Professor, Faculty of Information and Media Studies, Western University

Matt Hatfield, Campaigns Director, OpenMedia

Mike Larsen, President, BC Freedom of Information and Privacy Association (FIPA)

Pam Hrick, Executive Director & General Counsel, Women's Legal Education and Action Fund (LEAF)

Petra Molnar, Associate Director, Refugee Law Lab; Fellow at Harvard's Berkman Klein Center for Internet and Society

Rosel Kim, Senior Staff Lawyer, Women's Legal Education and Action Fund (LEAF)

Sam Andrey, The Dais, Toronto Metropolitan University

Sébastien Gambs, Professor at the Université du Québec à Montréal, Canada Research Chair in Privacy-preserving and Ethical Analysis of Big Data

Sharon Polsky, MAPP, President, Privacy & Access Council of Canada

Sonja Solomun, McGill University

Stéphane Leman-Langlois, Laval University

Thomas Linder, PhD, Researcher at Open North

Yuan Stevens, Human Rights Lawyer & Activist

Sent on June 21st, 2023 by the Canadian Civil Liberties Association (CCLA) on behalf of the above organizations and individuals.