BOTS AT THE GATE

A HUMAN RIGHTS ANALYSIS OF AUTOMATED DECISION-MAKING IN CANADA'S IMMIGRATION AND REFUGEE SYSTEM

THECITIZENLAB

UNIVERSITY OF TORONTO
FACULTY OF LAW

INTERNATIONAL
HUMAN RIGHTS
PROGRAM

This publication is the result of an investigation by the University of Toronto's International Human Rights Program (IHRP) at the Faculty of Law and the Citizen Lab at the Munk School of Global Affairs and Public Policy, with support from the IT3 Lab at the University of Toronto.

Authors: Petra Molnar and Lex Gill

Design and Illustrations: Jenny Kim

Copyright

Electronic version first published by the International Human Rights Program and the Citizen Lab in September, 2018. This work can be accessed through https://ihrp.law.utoronto.ca/ and https://citizenlab.ca.

Acknowledgements

The International Human Rights Program and the Citizen Lab wish to express their sincere gratitude for the support from many people who made this work possible.

This report was researched and written by **Petra Molnar**, Technology and Human Rights Researcher, and **Lex Gill**[1], Citizen Lab Research Fellow. The report was reviewed by **Ronald J. Deibert**, Professor of Political Science and Director of the Citizen Lab; **Samer Muscati**, Director of the IHRP; **Lisa Austin**, University of Toronto Faculty of Law, Professor and Chair in Law and Technology; **Audrey Macklin**, University of Toronto Faculty of Law, Professor and Chair in Human Rights Law; **David Lie**, Department of Electrical and Computer Engineering, University of Toronto; **Cynthia Khoo**, Google Policy Fellow at the Citizen Lab; **Tamir Israel**, Staff Lawyer at Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) at the University of Ottawa, Faculty of Law; and **Omar Khan**, computer scientist and refugee advocate.

This report was copy-edited by **Miles Kenyon**, Communications Specialist at the Citizen Lab, and **Cynthia Khoo** (who also provided extensive substantive written additions and revisions to the document). University of Toronto law students **Jenny Mao** and **Ritika Rai** provided valuable research assistance.

We would also like to thank **Eric Sears**, Senior Program Officer, Technology in the Public Interest at the MacArthur Foundation and **Jason Schultz**, Professor of Clinical Law, Director of NYU's Technology Law & Policy Clinic, and Area Lead in Law & Policy for the AI Now Institute for their insight and feedback in the development of this report. We are also grateful to the participants in our workshop at the **Citizen Lab Summer Institute 2018** for their valuable insights and lively critiques.

This report would not be possible without the generous support of the **John D. and Catherine T. MacArthur Foundation**, the **Honourable William C. Graham**, and the **Ford Foundation**. The **IT3 Lab at the University of Toronto** provided significant intellectual leadership, funding, and advisory support for the report.

1 The final text of this report was completed during Lex Gill's term as a Citizen Lab Research Fellow (ending 16 August, 2018). Nothing in this publication reflects the position or views of her present or future employers.

TABLE OF CONTENTS

TABLE OF CONTENTS

About the International Human Rights Program

The International Human Rights Program (IHRP) at the University of Toronto Faculty of Law addresses the most pressing human rights issues through two avenues: The Program shines a light on egregious human rights abuses through reports, publications, and public outreach activities; and the Program offers students unparalleled opportunities to refine their legal research and advocacy skills through legal clinic projects and global fellowships.

The IHRP's fundamental priority is impact: The Program strives to equip students and recent graduates with the skills, the knowledge, and the professional network to become effective human rights advocates. The Program also seeks to address human rights violations in Canada and abroad by engaging in comprehensive research and advocacy that aims to reform law, policy, and practice.

About the Citizen Lab

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

The Citizen Lab uses a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Our research includes: investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security, and information controls of popular applications; and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

About the IT3 Lab

The Information Technology, Transparency, and Transformation (IT3) Lab is an interdisciplinary research lab at the University of Toronto that combines the insights of law, computer engineering, and computer science to address questions of digital transparency. Individuals are becoming more transparent to corporations and governments, while the technology facilitating this is becoming more opaque. The IT3 Lab engages in innovative research to close this transparency gap. Its projects include work on the development of "dynamic" privacy policies, new privacy-protective methods of lawful access, accountable and privacy-protective practices for open data, and transparent AI.

LIST OF ACRONYMS

AI	Artificial Intelligence
ACLU	American Civil Liberties Union
AIA	Algorithmic Impact Assessment
ATI / ATIP	Access to Information (and Privacy)
CBSA	Canada Border Services Agency
CEPEJ	Council of Europe European Commission for the Efficiency of Justice
CIFAR	Canadian Institute for Advanced Research
CJEU	Court of Justice of the European Union
CPIC	Canadian Police Information Centre
CRA	Canada Revenue Agency
CSC	Correctional Service of Canada
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DOJ	Department of Justice
ESDC	Employment and Social Development Canada
ETA	Electronic Travel Authorization
GAC	Global Affairs Canada
GDPR	General Data Protection Regulation
H&C	Humanitarian and Compassionate (Application)
IAD	Immigration Appeal Division
IMP	International Mobility Program
IRB	Immigration and Refugee Board
IRCC	Immigration, Refugees and Citizenship Canada
IRPA	*Immigration and Refugee Protection Act*
ISED	Innovation, Science and Economic Development
PNR	(EU-Canada) Passenger Name Records
PRRA	Pre-Removal Risk Assessment
PSEP	Public Safety and Emergency Preparedness
RCMP	Royal Canadian Mounted Police
RFI	Request for Information (Procurement)
SBT	Scenario Based Targeting
TBCS	Treasury Board of Canada Secretariat
TFW	Temporary Foreign Worker (Program)
TRP	Temporary Resident Permit

Summary

This report focuses on the impacts of automated decision-making in Canada's immigration and refugee system from a human rights perspective. It highlights how the use of algorithmic and automated technologies to replace or augment administrative decision-making in this context threatens to create a laboratory for high-risk experiments within an already highly discretionary system. Vulnerable and under-resourced communities such as non-citizens often have access to less robust human rights protections and fewer resources with which to defend those rights. Adopting these technologies in an irresponsible manner may only serve to exacerbate these disparities.

The use of these technologies is not merely speculative: the Canadian government has already been experimenting with their adoption in the immigration context since at least 2014. For example, the federal government has been in the process of developing a system of "predictive analytics" to automate certain activities currently conducted by immigration officials and to support the evaluation of some immigrant and visitor applications. The government has also quietly sought input from the private sector related to a 2018 pilot project for an "Artificial Intelligence Solution" in immigration decision-making and assessments, including in Humanitarian and Compassionate applications and Pre-Removal Risk Assessments. These two applications are often used as a last resort by vulnerable people fleeing violence and war to remain in Canada.

The ramifications of using automated decision-making in the immigration and refugee space are far-reaching. Hundreds of thousands of people enter Canada every year through a variety of applications for temporary and permanent status. Many come from war-torn countries seeking protection from violence and persecution. The nuanced and complex nature of many refugee and immigration claims may be lost on these technologies, leading to serious breaches of internationally and domestically protected human rights, in the form of bias, discrimination, privacy breaches, due process and procedural fairness issues, among others. These systems will have life-and-death ramifications for ordinary people, many of whom are fleeing for their lives.

This report first outlines the methodology and scope of analysis and provides a few conceptual building blocks to situate the discussion surrounding automated decision systems. It then surveys some of the current and proposed uses of automated decision-making in Canada's immigration and refugee system. Next, it provides an overview of the various levels of decision-making across the full lifecycle of the immigration and refugee process to illustrate how these decisions may be affected by new technologies. The report then develops a human rights analysis of the use of automated decision systems from a domestic and international perspective. Without a critical human rights analysis, the use of automated decision-making may result in infringements on a variety of rights, including the rights to equality and non-discrimination; freedom of movement, expression, religion, and association; privacy rights and the rights to life, liberty, and security of the person. These technologies in the immigration and refugee system also raise crucial constitutional and administrative law issues, including matters of procedural fairness and standard of review. Finally, the report documents a number of other systemic policy challenges related to the adoption of these technologies—including those concerning access to justice, public confidence in the legal system, private sector accountability, technical capacity within government, and other global impacts.

The report concludes with a series of specific recommendations for the federal government, the complete and detailed list of which are available at the end of this publication. In summary, they include recommendations that the federal government:

1. **Publish** a complete and detailed report, to be maintained on an ongoing basis, of all automated decision systems currently in use within Canada's immigration and refugee system, including detailed and specific information about each system.
2. **Freeze** all efforts to procure, develop, or adopt any new automated decision system technology until existing systems fully comply with a government-wide Standard or Directive governing the responsible use of these technologies.
3. **Adopt** a binding, government-wide Standard or Directive for the use of automated decision systems, which should apply to all new automated decision systems as well as those currently in use by the federal government.
4. **Establish** an independent, arms-length body with the power to engage in all aspects of oversight and review of all use of automated decision systems by the federal government.
5. **Create** a rational, transparent, and public methodology for determining the types of administrative processes and systems which are appropriate for the experimental use of automated decision system technologies, and which are not.
6. **Commit** to making complete source code for all federal government automated decision systems—regardless of whether they are developed internally or by the private sector—public and open source by default, subject only to limited exceptions for reasons of privacy and national security.
7. **Launch** a federal Task Force that brings key government stakeholders alongside academia and civil society to better understand the current and prospective impacts of automated decision system technologies on human rights and the public interest more broadly.

Immigration and refugee law is a useful lens through which to examine state practices, particularly in times of greater border control security and screening measures, complex systems of global migration management, the increasingly widespread criminalization of migration, and rising xenophobia. Immigration law operates at the nexus of domestic and international law and draws upon global norms of international human rights and the rule of law. Canada has clear domestic and international legal obligations to respect and protect human rights when it comes to the use of these technologies and it is incumbent upon policy makers, government officials, technologists, engineers, lawyers, civil society, and academia to take a broad and critical look at the very real impacts of these technologies on human lives.

Introduction

Scope of Report

In this report, the term **automated decision systems** is used to refer to a particular class of technologies that either assist or replace the judgment of human decision-makers. These systems draw from fields like statistics, linguistics, and computer science, and use techniques such as regression, rules-based systems, predictive analytics, machine learning, deep learning, and neural networks, often in combination with one another. Automated decision systems may be used for any number of diverse applications—by both government and the private sector—depending on the ultimate "decision" at issue. For example, technical systems in this class have been used by governments to predict the risk of recidivism in pre-trial detention and sentencing decisions,[2] to automate the identification of unemployment fraud,[3] and to predict "hot spots" for future crime[4]—supplementing or replacing the human judgment of judges, civil servants, and police officers in the process.

The introduction of automated systems can impact both the **processes** and **outcomes** associated with decisions that would otherwise be made by administrative tribunals, immigration officers, border agents, legal analysts, and other officials responsible for the administration of Canada's immigration and refugee system. Automated decision systems are likely to have important human rights implications regardless of whether they operate autonomously and in lieu of a human decision-maker, or whether their outputs are simply one factor considered by a human in rendering a final decision. As a result, this report is concerned with the use of these technologies both in **assisting** and in **replacing** the judgment of human decision-makers within Canada's immigration and refugee system. This analysis therefore includes systems that:

- Classify cases, applications, or individuals for triage (e.g., in terms of risk, priority, or complexity);
- Generate scores, probability assessments, and other indicators for consideration as factors to support a human decision-maker's reasoning;[5]
- Identify or "flag" certain cases for human review or investigation;
- Provide overall recommendations about whether an application should be approved; or
- Render the complete administrative decision.[6]

---

2 Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, "Machine Bias," *ProPublica* (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

3 Robert N. Charette, "Michigan's MiDAS Unemployment System: Algorithm Alchemy Created Lead, Not Gold," *IEEE* Spectrum (24 January 2018) <https://spectrum.ieee.org/riskfactor/computing/software/michigans-midas-unemployment-system-algorithm-alchemy-that-created-lead-not-gold>.

4 See generally Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: NYU Press, 2017).

5 This includes automated systems which which generate "risk scores," such as those used in bail, parole, and sentencing decisions in the criminal law context. See Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, "Machine Bias," *ProPublica* (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; Electronic Privacy Information Center, "Algorithms in the Criminal Justice System" (last updated 2017) <https://epic.org/algorithmic-transparency/crim-justice/>.

6 Many of these bullet points are similar to the boundary conditions outlined in Treasury Board Canada Secretariat, "Treasury Board Directive on Automated Decision Making," Draft 1.0 (uploaded 9 August 2018) <https://wiki.gccollab.ca/Treasury_Board_Directive_on_Automated_Decision_Making>.

While the focus of this report is specific to the immigration and refugee law context, the analysis may also serve as a useful contribution to the broader conversation about automated decision systems of this nature.

Immigration and Refugee Law as a High-Risk Laboratory

This report focuses specifically on the deployment of automated decision systems in the context of **Canadian immigration and refugee law**. This context is particularly important because vulnerable and under-resourced communities such as non-citizens often have access to less robust human rights protections and fewer resources with which to defend those rights. This section reviews a number of factors which make Canadian immigration and refugee law a high-risk laboratory for experiments in automated decision-making.

First, there is a pressing need to develop research and analysis that responds to the Canadian government's express intention to pursue greater adoption of these technologies. As documented in this report, administrative decision-makers within the Canadian immigration and refugee system are already relying on automated decision systems to some degree and the federal government is beginning to explore their use in new contexts that pose ever-higher risks to human rights and civil liberties. As these systems become increasingly normalized and integrated, it is crucial that choices related to their adoption are made in a transparent, accountable, fair, and rights-respecting manner. There is an urgent need for Canadian academic and civil society engagement on this issue.

The sheer scale of potential impact is another reason for the focus on the immigration and refugee context. In 2017, Immigration, Refugees and Citizenship Canada (IRCC) and the Canada Border Services Agency (CBSA) processed over 50,000 refugee claims.[7] Canada is projecting the admission of 310,000 new permanent residents in 2018 and up to 340,000 new permanent residents annually by 2020.[8] In 2016, there were over 266,000 students holding an international study permit in Canada; the government issued over 10,000 Temporary Resident Permits (TRPs) and extensions; it approved over 1.3 million applications for individuals wanting to visit Canada and over 2.5 million electronic travel authorization (ETA) applications; and it issued over 78,500 work permits under the Temporary Foreign Worker (TFW) Program and over 208,500 work permits under the International Mobility Program (IMP).[9] Cumulatively, these programs involve millions of determinations and decisions every year. They change the course of millions of lives.

Indeed, the potential impact of these systems on individuals' physical safety, human rights, and livelihoods is far reaching. Bias, error, or system failure can result in irreparable harm to individuals and their families. For individuals navigating Canada's immigration system, extensive delay, substantial financial cost, interrupted work or studies, detention (often for months or years at a time),[10] prolonged family separation, and

---

7 Government of Canada, "2017 Asylum Claims" (last modified 12 July 2018) <https://www.canada.ca/en/immigration-refugees-citizenship/services/refugees/asylum-claims-2017.html>.

8 Government of Canada (Immigration, Refugees and Citizenship), "2017 Annual Report to Parliament on Immigration" (last modified 1 November 2017) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/annual-report-parliament-immigration-2017.html>.

9 Ibid.

10 See for example, The International Human Rights Program at the University of Toronto Faculty of Law, "UN Review Should Urge Canada To Reform Immigration Detention System" (5 October 2017) <https://ihrp.law.utoronto.ca/un-review-should-urge-canada-reform-immigration-detention-system>

deportation are all possibilities. For refugee claimants, the consequence of a rejected claim on an erroneous basis can result in persecution on the basis of an individual's "race, religion, nationality, membership in a particular social group, or political opinion."[11] For persons in need of protection under section 97(1) of the *Immigration and Refugee Protection Act*, error or bias in determining their application may expose them to the threat of torture, cruel and inhumane treatment or punishment, or a risk to their life.[12]

Despite these risks, immigration and refugee law is an area where safeguards and oversight can be limited.[13] At the level of procedural fairness, an individual's "right to be heard" and their "right to know the case to meet" may be restricted depending on the nature of the legal issue at stake. For example, they may not be entitled to an in-person interview or a full hearing,[14] and may not receive full disclosure of the information being considered in their case.[15] Even when there is a legal requirement to provide written reasons for a decision, those reasons will rarely be as extensive or detailed as those in a civil or criminal proceeding.[16] Administrative decision-makers are also afforded considerable deference upon judicial review by a court: immigration and refugee cases are generally reviewed on a "reasonableness" rather than a "correctness" standard.[17] As a result, immigration and refugee law sits at an uncomfortable legal nexus: the impact on the rights and interests of individuals is often very significant, even where the degree of deference is high and the procedural safeguards are weak. There is also a serious lack of clarity surrounding how courts will interpret administrative law principles like natural justice, procedural fairness, and standard of review where an automated decision system is concerned.

There are also a number of areas where immigration and refugee law intersects with national security law, such as in the case of pre-removal risk assessments or security certificates. In these cases, the processes and decision-making infrastructure become even more opaque and complex. For instance, despite the Supreme Court of Canada's rulings in *Charkaoui I*[18] and *Harkat*,[19] sections 83(1) and 85.4(1) of the *Immigration and Refugee Protection Act (IRPA)* continue to allow the government to withhold information (including relevant information) from special advocates in security certificate proceedings.[20] Although this problem was introduced in the controversial 2015 national security bill, C-51 (*the Anti-terrorism Act 2015*), the federal government did not correct it in its 2017 reform bill, C-59.[21] The use of datasets collected by intelligence

---

11 s. 96, *Immigration and Refugee Protection Act*, S.C. 2001, c. 27.

12 s. 97(1), *Immigration and Refugee Protection Act*, S.C. 2001, c. 27.

13 The Canadian Press, "Federal audit highly critical of Canada's treatment of immigration detainees, fuelling calls for reform," *The Globe and Mail* (24 July 2018) <https://www.theglobeandmail.com/canada/article-federal-audit-highly-critical-of-canadas-treatment-of-immigration/>

14 Government of Canada (Immigration and Citizenship Canada), "Procedural fairness," (last modified 31 March 2017) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/service-delivery/procedural-fairness.html>.

15 *Krishnamoorthy v. Canada* (Citizenship and Immigration), 2011 FC 1342 at paragraph 32 et seq.

16 *Baker v. Canada* (Minister of Citizenship and Immigration), [1999] 2 SCR 817.

17 *Dunsmuir v New Brunswick*, 2008 SCC 9.

18 *Charkaoui v Canada* (Minister of Citizenship and Immigration), 2007 SCC 9.

19 *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37

20 ss. 83(1) and 85.4(1), *Immigration and Refugee Protection Act*, S.C. 2001, c. 27.

21 See Canadian Civil Liberties Association, "Submission to the Standing Committee on Public Safety and National Security regarding Bill C-59, An Act respecting national security matters," (January 2018) at 27-29

agencies like the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) could also become even more problematic once fed into automated decision systems in the immigration and refugee law context, highlighting the intimate relationship between these emerging technologies and "big data" surveillance. International case studies suggest that predictive analytics and artificial intelligence technologies are also increasingly making their way into international affairs, diplomacy, and intelligence.[22]

There is an international race for strategic leadership in this arena. In 2017, China adopted a development plan that aims to build a domestic industry for artificial intelligence projected to be worth almost $150-billion (U.S.) by the year 2030.[23] In April of 2018, the European Commission called for a €20 billion cash injection of research and development funds toward artificial intelligence.[24] As of July 2018, a researcher had documented the publication of 23 separate national or supranational AI strategies over a 15-month period alone, including ones from "Canada, China, Denmark, the EU Commission, Finland, France, India, Italy, Japan, Mexico, the Nordic-Baltic region, Singapore, South Korea, Sweden, Taiwan, the UAE, and the UK."[25] The Canadian government was the first among them, setting out a $125-million (CAD) "Pan-Canadian Artificial Intelligence Strategy" with leadership from the Canadian Institute for Advanced Research (CIFAR) that aimed to develop research excellence and enhance Canada's profile in the field internationally.[26] Ahead of the 2018 G7 meeting, Canada and France announced that they were entering into a new partnership to create an international study group "charged with understanding emerging AI technologies and how to ensure they are beneficial."[27] This influx of interest and investment has made artificial intelligence and machine learning attractive and well-funded research areas for the public and private sectors alike.[28]

<https://ccla.org/cclanewsite/wp-content/uploads/2018/01/2018-01-17-Written-submissions-to-SECU-re-C-59.pdf>.

22 See for example, Stephen Chen, "Artificial intelligence, immune to fear or favour, is helping to make China's foreign policy," *South China Morning Post* (30 July 2018) <https://www.scmp.com/news/china/society/article/2157223/artificial-intelligence-immune-fear-or-favour-helping-make-chinas>.

23 Paul Mozur, "Beijing Wants A.I. to Be Made in China by 2030," *The New York Times* (20 July 2017) <https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html>.

24 Jennifer Rankin, "Artificial intelligence: €20bn investment call from EU commission," *The Guardian* (25 April 2018) <https://www.theguardian.com/technology/2018/apr/25/european-commission-ai-artificial-intelligence>.

25 Tim Dutton, "An Overview of National AI Strategies," *Medium* (28 June 2018) <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd>

26 Canadian Institute for Advanced Research, "Pan-Canadian Artificial Intelligence Strategy <https://www.cifar.ca/ai/pan-canadian-artificial-intelligence-strategy>.

27 Canadian Institute for Advanced Research, "Canada and France make historic commitment to include inclusive and ethical AI" (6 June 2018) <https://www.cifar.ca/news/news/2018/06/06/canada-and-france-make-historic-commitment-to-inclusive-and-ethical-ai>. See also Government of Canada, "Canada-France Statement on Artificial Intelligence" (7 June 2018) <http://international.gc.ca/world-monde/international_relations-relations_internationales/europe/2018-06-07-france_ai-ia_france.aspx?lang=eng>.

28 For example, in response to the demand for interdisciplinary research in this field, New York University has launched the AI Now Institute, a research center dedicated to examining the social implications of artificial intelligence. The Ethics and Governance of Artificial Intelligence Initiative, a hybrid research effort and philanthropic fund led jointly by the Berkman Klein Center at Harvard University and the MIT Media Lab, is another example of academic development in the field. See: "AI Now," *AI Now Institute* <https://ainowinstitute.org/>; "The Ethics and Governance of Artificial Intelligence Initiative" <https://aiethicsinitiative.org/>; and Christopher Bavitz, "Algorithms and Justice," *Medium* (9 July 2018) <https://medium.com/berkman-klein-center/algorithms-and-justice-the-berkman-klein-center-for-internet-society-examines-the-role-of-the-84a3a7d90a6>.

The challenge, then, is not how to use new technology to entrench old problems, but instead to better understand how we may use this opportunity to imagine and design systems that are more transparent, equitable, and just.

Simultaneously, the global experiences of migrants and refugees represents a grave humanitarian crisis. In response to issues like migration, even well-intentioned policymakers are sometimes too eager to see new technologies as a quick solution to what are otherwise tremendously complex and intractable policy issues. Interest in artificial intelligence, machine learning, predictive analytics, and automated decision-making is not immune to this tendency. In this light, critical, empirical, and rights-oriented research should serve not only as an important counterbalance to stopgap responses or technological solutionism, but serve as the central starting point from which to assess whether such technological approaches are appropriate to begin with. At the same time, Canada's immigration and refugee system is the source of long-standing human rights concerns—including protracted family separation, long wait times, and indefinite immigration detention—and any skepticism of new initiatives should not be perceived as an endorsement of the status quo. Indeed, as the author Tarleton Gillespie writes, "[W]e sometimes wish for more 'algorithmic' interventions when the ones we face are discriminatory, nepotistic, and fraught with error; sometimes procedure is truly democratic."[29] The challenge, then, is not how to use new technology to entrench old problems, but instead to better understand how we may use this opportunity to imagine and design systems that are more transparent, equitable, and just.

A Note on Terminology

While this report uses the term a**utomated decision-making** (or **automated decision systems**), in practice there is a constellation of overlapping and interrelated terms that refer to various technologies in this field—as well as to their specific applications and use cases.

For example, the terms **artificial intelligence** (AI), **machine learning**, and **predictive analytics** have been used by various Canadian federal departments and agencies in this context. Most recently, they appeared in a 2018 Request for Information (RFI) submitted by Immigration, Refugees and Citizenship Canada (IRCC), Employment and Social Development Canada (ESDC), and the Department of Justice (DOJ) with regard to a proposed "Artificial Intelligence Solution,"[30] as explored in this report. However, this usage is not uniform

29 Tarleton Gillespie, "Algorithm," In *Digital Keywords: A Vocabulary of Information Society and Culture,* edited by Ben Peters (Princeton: Princeton University Press, 2016) at 27 <http://culturedigitally.org/wp-content/uploads/2016/07/Gillespie-2016-Algorithm-Digital-Keywords-Peters-ed.pdf>.

30 Public Works and Government Services Canada, "Artificial Intelligence Solution (B8607-180311/A)," Tender Notice (13 April 2018, amended 23 May 2018) <https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EE-017-33462>.

across the federal government. In 2018 the Treasury Board of Canada Secretariat (TBCS) began a consultation in order to develop a new draft Standard on the use and adoption of these technologies by federal government institutions. As of August 2018, the preferred term in that draft (now elevated to a draft Directive) was **automated decision systems**—though earlier versions have also made reference to **automated systems**, **decision support systems**, **machine learning**, and **machine intelligence.**[31]

The 2018 Toronto Declaration—a recent civil society coalition statement on the topic—applies to **machine learning systems** and references "**artificial intelligence** more broadly."[32] A set of ethical principles from 2017 called the Montréal Declaration uses the term **artificial intelligence** almost exclusively, but also refers to non-human, **autonomous and intelligent agents**, **intelligent machines**, and **artificial agents**.[33] Like Canada's TBCS, the European Union's General Data Protection Regulation (GDPR) uses the term **automated decision-making** specifically.[34] Relatedly, a significant portion of the academic literature uses the language of **algorithmic decision-making**.[35] Where these technologies are used for the specific purpose of conducting legal research or legal analysis, they are also sometimes referred to as **legal automation**.[36] Terms referring to techniques such as predictive analytics,[37] **algorithmic prediction**,[38] and **automated prediction**[39] are also closely related. It is important to understand that while technical and disciplinary differences exist between all of these terms, they are often used interchangeably by both government and the popular press. Indeed, these definitional boundaries are regularly contested even by experts.

---

31 Treasury Board Canada Secretariat, "Treasury Board Directive on Automated Decision Making," Draft 1.0 (uploaded 9 August 2018) <https://wiki.gccollab.ca/Treasury_Board_Directive_on_Automated_Decision_Making> [earlier drafts accessed by Lex Gill].

32 Access Now, "The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems," *Access Now* (May 2018) <https://www.accessnow.org/cms/assets/uploads/2018/05/Toronto-Declaration-D0V2.pdf>.

33 Université de Montréal, "Montreal Declaration for a Responsible Development of AI," *Université de Montréal* (November 2017) <https://www.montrealdeclaration-responsibleai.com/the-declaration>.

34 Article 22, General Data Protection Regulation (GDPR) (EU) 2016/679 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>.

35 See for example, Tal Zarsky (2016), ''The Trouble with Algorithmic Decisions: An Analytic Roadmap to Examine Efficiency and Fairness in Automated and Opaque Decision Making,'' *Science, Technology, & Human Values* 41:1 <http://sth.sagepub.com/content/early/2015/10/13/0162243915605575.abstract>; Bryce Goodman and Seth Flaxman (2017), "EU regulations on algorithmic decision-making and a 'right to explanation'" *AI Magazine* 38:3 <https://doi.org/10.1609/aimag.v38i3.2741>.

36 See for example, Frank Pasquale and Glyn Cashwell (2015), "Four Futures of Legal Automation," *UCLA Law Review Discourse* 63 <https://www.uclalawreview.org/four-futures-legal-automation/>.

37 See for example, Bernstein Institute for Human Rights, "Tyranny of the Algorithm? Predictive Analytics & Human Rights," Conference Proceedings, Annual Symposium (2016) <http://www.law.nyu.edu/bernstein-institute/conference-2016>.

38 See for example, Lyria Bennett Moses and Janet Chan (2016), "Algorithmic prediction in policing: assumptions, evaluation, and accountability," *Policing and Society* 28:7 <https://doi.org/10.1080/10439463.2016.1253695>.

39 See for example, Danielle Keats Citron and Frank Pasquale (2014), "The Scored Society: Due Process for Automated Predictions," *Washington Law Review* 89:1 <https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1318/89WLR0001.pdf?sequence=1>.

A Few Conceptual Building Blocks

Automated decision systems process information in the form of input data using an **algorithm** (or algorithms) to generate an output of some kind. At its most basic level, an algorithm is a set of instructions, "a recipe composed in programmable steps," designed for the purpose of "organizing and acting on a body of data to quickly achieve a desired outcome."[40] Certain algorithms, including those that use techniques like **machine learning**, are "trained" using a large, existing corpus of data, which allows the algorithm to classify and "generalize beyond the examples in the training set."[41] These systems are generally designed to map an input to an output based on a set of labeled training examples. For example, **training data** could include a body of case law, a collection of photographs, or a database of statistics—some or all of which have been pre-categorized or labeled based on the designer's criteria. A system designed to recognize images of cars captured by traffic camera footage can therefore be trained on a body of images labelled as "contains car" (and potentially as "does not contain a car"). As the system is exposed to more data, it may improve its ability to identify cars and reduce its error rate—noting that the potential for error cuts both ways: a system may identify non-cars as cars, just as it may fail to recognize a car when one appears in a given image.

The quality of the training data impacts the quality of the output data. As a recent report from the Canadian company Integrate.ai points out, "[I]n standard practice, machine learning assumes the future will look like the past. When the past is unfair or biased, machine learning will propagate these biases and enhance them through feedback loops."[42] One classic illustration of this principle is the finding that facial recognition software trained predominantly on the faces of white and lighter-skinned people may be less capable of accurately identifying individuals with darker skin tones.[43] In other words, the values, assumptions, biases, shortcomings, and blind spots involved in the selection or substantive content of training data—as well as the types of input data deemed "relevant" to an automated system's decision-making process—will impact both outputs and outcomes.

This issue is exacerbated where the training data is already coloured by human agency (directly or indirectly) and pre-existing bias, or where variables that do not appear discriminatory at face value serve as "proxies" for protected categories.[44] In a 2018 Council of Europe study, the authors make this point by highlighting the legal distinction between direct and indirect discrimination. In the first instance, discrimination arises where

---

40 Tarleton Gillespie, "Algorithm," in *Digital Keywords: A Vocabulary of Information Society and Culture*, edited by Ben Peters (Princeton: Princeton University Press, 2016) <http://culturedigitally.org/wp-content/uploads/2016/07/Gillespie-2016-Algorithm-Digital-Keywords-Peters-ed.pdf> at page 19.

41 Pedro Domingos (2012), "A Few Useful Things to Know about Machine Learning," *Communications of the ACM* 55:10 <https://homes.cs.washington.edu/~pedrod/papers/cacm12.pdf> at page 79.

42 Integrate AI (2018), "Responsible AI in Consumer Enterprise" <https://d1x0mwiac2rqwt.cloudfront.net/HyzJkRoYc5DUHtHbg_AMyo4gk1MGM3QUIssSk-I3TpwLPecIgrWocjUeVJ9wtp4x/by/903235/as/IntegrateAI_Responsible_AI_White_Paper_1_.pdf> at page 6.

43 Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Lineup: Unregulated Police Face Recognition in America, Racial Bias," *Georgetown Law Center on Privacy & Technology* (18 October 2016) <https://www.perpetuallineup.org/findings/racial-bias>; Brendan F. Klare et al. (20120, "Face Recognition Performance: Role of Demographic Information," *IEEE Transactions on Information Forensics and Security* 7 <http://openbiometrics.org/publications/klare2012demographics.pdf>.

44 Council of Europe (2018), "Algorithms and Human Rights: Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications" <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> at page 26.

the factors that are considered (whether consciously or not) to make a decision are directly unlawful.[45] For example, an algorithm trained on a company's historical hiring decisions in order to recommend future job candidates may reproduce patterns of racial or gender bias exhibited by past hiring committees. Indirect discrimination, by contrast, can arise "Where a certain characteristic or factor occurs more frequently in the population groups against whom it is unlawful to discriminate (such as a person with a certain racial or ethnic background living in a certain geographical area; women having fewer pensionable years because of career breaks)."[46]

Automated decision systems, which "may be based on correlation between data sets and efficiency considerations," can rely on these variables to generate outputs that perpetuate or exacerbate patterns of bias and discrimination.[47] This kind of **proxy discrimination** can be difficult to correct—or even to detect in the first place.[48] And yet as Gillespie has written, "To call a service or process an algorithm is to lend it a set of associations: mathematical, logical, impartial, consistent."[49] The very fact that an outcome is the result of an automated process may afford it greater legitimacy, increase the perceived "neutrality" of an outcome, or weaken the accountability of human actors and institutions responsible for adopting the tool in the first place.[50] This report's analysis challenges this default presumption of greater "objectivity," noting that all technological choices—about what to count, who counts, and why—have an inherently political dimension.

Indeed, as Bavitz and Hessekiel note, "One of the first questions that computer scientists ask lawyers when considering use of algorithms generally (and, particularly, to facilitate functions of government) is—**for what are we optimizing?**"[51] And yet in policy circles, this question is sometimes overlooked or taken for granted. In some cases, the answer may be found to some degree in statutory objectives; in other cases, it may be less clear. When evaluating a given automated decision system, it is crucial to understand how "success" is defined in its implementation, and what specific metrics will be used to evaluate that success or failure. The Center for Democracy and Technology provides a useful explanation on this point, with regard to the need to clarify the goals of predictive technologies in particular:

> Some algorithms are designed to predict a future outcome. Designing a predictive algorithm involves coming up with a definition of success and choosing **target variables** that will bring it about. For example, when designing an algorithm that sifts through job applications to recommend hires, success could mean saving money, hiring a diverse group of employees, or any number

45 Council of Europe (2018), "Algorithms and Human Rights: Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications" <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> at page 27-28.

46 Ibid.

47 Ibid.

48 Anupam Datta et al. (2017), "Proxy Discrimination in Data-Driven Systems: Theory and Experiments with Machine Learnt Programs" <https://arxiv.org/pdf/1707.08120.pdf>.

49 Tarleton Gillespie, "Algorithm," in *Digital Keywords: A Vocabulary of Information Society and Culture,* edited by Ben Peters (Princeton: Princeton University Press, 2016) <http://culturedigitally.org/wp-content/uploads/2016/07/Gillespie-2016-Algorithm-Digital-Keywords-Peters-ed.pdf> at page 23.

50 Ibid.

51 Christopher Bavitz and Kira Hessekiel, "Algorithms and Justice," *Medium* (9 July 2018) <https://medium.com/berkman-klein-center/algorithms-and-justice-the-berkman-klein-center-for-internet-society-examines-the-role-of-the-84a3a7d90a6>

of other metrics. The definition of success determines the **target variables**—the thing the algorithm will actually try to predict. If success means saving money, and employee turnover costs money, then a good hire may be defined as one who is likely to stay at the company for a long time (so the target variable would be longevity).

Target variables get further broken down in a process called **feature selection**. This is where programmers decide what specific criteria they will prioritize to sort, score, or rank cases. For example, the qualities that determine whether an employee will stay at a company long-term may include the amount of time a person stayed in his or her previous job.[52]

Regardless of whether a system is designed to more quickly and efficiently reproduce the status quo or whether its purpose is to dramatically transform policy outcomes, design choices are reflective of normative values.

Finally, the criteria, methodology, or "reasoning" employed by a machine learning system may be very different than that of a human mind engaged in the same exercise (even when they arrive at the same result). When attempting to unpack *how* and *why* a given automated decision system yields a certain output, three different barriers to transparency tend to arise. First, automated decision systems used by government are not always developed "in house;" instead, they may be sold to departments and agencies of government by private sector vendors, whether as a product or as a service. As a result, an algorithm's source code, its training data, or other inputs may be proprietary, and—to the extent that they exists as confidential business asset or intellectual property—can sometimes be shielded from public scrutiny on that basis. Where there is a nexus between immigration or refugee law and matters of national security, both input data and source code are also more likely to be classified. Second, scholars have raised concerns that in some cases, full source code disclosure may not always be desirable, to the extent that revealing how an automated decision system functions can facilitate attempts to "game" or circumvent it.[53] Third, as these systems become more sophisticated (and as they begin to learn, iterate, and improve upon themselves in unpredictable or otherwise unintelligible ways), their logic often becomes less intuitive to human onlookers. In these cases, even when all aspects of a system are reviewable and superficially "transparent," the precise rationale for a given output may remain uninterpretable and unexplainable. As technologist David Weinberger writes, "We are increasingly relying on machines that derive conclusions from models that they themselves have created … models that 'think' about the world differently than we do."[54] This means that in some cases there may be no simple way to render an automated decision system or process meaningfully "explainable" to a human observer. Whether the lack of transparency arises as a result of financial interest, circumvention concerns, technical design, or a combination thereof, the result is that some automated systems are essentially black boxes.[55]

---

52 Centre for Democracy, "Digital Decisions" <https://cdt.org/issue/privacy-data/digital-decisions/>.

53 Joshua A. Kroll et al. (2017), "Accountable Algorithms," *University of Pennsylvania Law Review* 165:3 <https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/> at page 639.

54 David Weinberger, "Our Machines Now Have Knowledge We'll Never Understand," *Wired*, 18 April 2017 <https://www.wired.com/story/our-machines-now-have-knowledge-well-never-understand/>.

55 See generally Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge: Harvard University

Methodology

This report uses a human rights based approach to examine automated decision systems in the Canadian immigration and refugee context. It outlines some of the ways that these systems must account for existing and emerging human rights, including equality and freedom from discrimination; freedom of association, religion, and expression; mobility rights; the right to privacy; and the rights to life, liberty, and security of the person. It also examines critical constitutional and administrative law issues (including principles of fairness, accountability, transparency) and other systemic policy issues related to the adoption of these technologies. This report provides an analysis of public statements, records, policies, and drafts provided by the Government of Canada and its various departments, agencies, and ministries. The IHRP and the Citizen Lab have also submitted 27 separate Access to Information (ATI) requests (see **Appendix A**) to the Government of Canada, including to the CBSA, IRCC, CSIS, Shared Services Canada (SSC), Public Safety and Emergency Preparedness (PSEP), Global Affairs Canada (GAC), Innovation, Science and Economic Development (ISED), and the Royal Canadian Mounted Police (RCMP). The authors continue to await data in response to these requests and intend to publish results in full as they become available.

This report takes an interdisciplinary approach, drawing from literature in law, computer science, and science and technology studies (STS). The analysis also integrates examples from a scan of other jurisdictions, including both promising practices and familiar challenges to Canada's immigration system and the use of automated decision technologies. Comparison is a fundamental tool of analysis and the comparative case study method is particularly valuable in human rights research, because it allows for broader linkages to be made using carefully obtained data.[56]

The report's analysis relies on principles enshrined in international legal instruments that Canada has ratified, such as the *International Covenant on Civil and Political Rights*,[57] the *International Convention on the Elimination of All Forms of Racial Discrimination*,[58] and the *Convention relating to the Status of Refugees*,[59] among others. Where the responsibilities of private sector actors are concerned, the report is informed by the United Nations Guiding Principles on Businesses and Human Rights (the "Protect, Respect and Remedy" Framework).[60]

Press, 2015); Andrew Burt, Brenda Leong, Stuart Shirrell, and Xiangnong (George) Wang, "Beyond Explainability: A Practical Guide to Managing Risk in Machine Learning Models," Future of Privacy Forum (June 2018) <https://fpf.org/wp-content/uploads/2018/06/Beyond-Explainability.pdf>.

56 The case study approach is widely used by many established human rights organizations such as Human Rights Watch, Amnesty International, as well as various UN Bodies, such as UNICEF. See for example Delwyn Goodrick (2014), "Comparative Case Studies," *UNICEF Office of Research Methodological Briefs, Impact Evaluation* No. 9 <https://pdfs.semanticscholar.org/95fd/65e368d32fda49f22b94f24f3aed3fedafdc.pdf>. See also Fons Coomans, Fred Grünfeld, and Menno T. Kamminga (2010), "Methods of Human Rights Research: A Primer" *Human Rights Quarterly* 32:1 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1395689>.

57 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

58 UN General Assembly, *International Convention on the Elimination of All Forms of Racial Discrimination*, 21 December 1965 <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CERD.aspx>.

59 UN General Assembly, Convention relating to the Status of Refugees, 14 December 1950 <https://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfRefugees.aspx>.

60 United Nations Human Rights Office of the High Commissioner (2011), "Guiding Principles on Businesses and Human Rights: 135 Implementing the United Nations "Protect, Respect and Remedy" Framework" <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

Beyond the legal and international human rights community, a number of academic and civil society coalitions have produced guiding principles and declarations on the human rights dimension of these technologies. For example, in 2017 the Forum on the Socially Responsible Development of Artificial Intelligence at the Université de Montréal launched a document entitled "The Montreal Declaration on the Responsible Development of Artificial Intelligence."[61] Similarly, in May of 2018 researchers and advocates launched "The Toronto Declaration," which focuses on the rights to equality and non-discrimination in machine learning systems.[62] The Fairness, Accountability, Transparency [and Ethics] (F.A.T. or F.A.T.E.) framework, which emerged as part of multidisciplinary academic efforts,[63] is also increasingly used as a research lens by industry.[64] The research community is also continuously iterating on design and evaluation principles in this field, encouraging the use of frameworks like Social Impact Statements[65] and Algorithmic Impact Assessments in the public sector's adoption of algorithm-driven technologies.[66] The European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe has also recently convened a multidisciplinary expert body to "lead the drafting of guidelines for the ethical use of algorithms within justice systems, including predictive justice."[67]

This analysis is also supplemented by input from over thirty experts from various fields at a workshop held at the Citizen Lab's 2018 Summer Institute on June 15th 2018 under the Chatham House Rule.[68] The session was convened to discuss the preliminary findings and scope of this report, and to probe future directions and human rights considerations related to the use of automated decision systems in Canada's immigration and refugee context. Participants included an interdisciplinary cohort of computer scientists, technologists, public servants, immigration and refugee lawyers, technology and human rights advocates, academics, and artists representing regions from Canada and the United States to Hong Kong, South Korea, Australia, and Brazil. Analysis, critique, and commentary from participants has been integrated into our findings throughout this report.

---

61 Université de Montréal, "Montreal Declaration for a Responsible Development of AI," *Université de Montréal* (November 2017) <https://www.montrealdeclaration-responsibleai.com/the-declaration>.

62 Access Now, "The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems," *Access Now* (May 2018) <https://www.accessnow.org/cms/assets/uploads/2018/05/Toronto-Declaration-D0V2.pdf>.

63 See for example, FAT/ML, Fairness, Accountability, and Transparency in Machine Learning (annual academic conference) <https://www.fatml.org/>.

64 See for example, Microsoft Research, "FATE: Fairness, Accountability, Transparency, and Ethics in AI," <https://www.microsoft.com/en-us/research/group/fate/>.

65 FAT/ML, "Principles for Accountable Algorithms and a Social Impact Statement for Algorithms," <https://www.fatml.org/resources/principles-for-accountable-algorithms>.

66 Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker (2018), "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability," *AI Now Institute* <https://ainowinstitute.org/aiareport2018.pdf>; Eddie Copeland, "10 principles for public sector use of algorithmic decision making," *Nesta* (Blog) (20 February 2018) <https://www.nesta.org.uk/blog/10-principles-for-public-sector-use-of-algorithmic-decision-making/>.

67 Council of Europe, "Council of Europe European Commission for the efficiency of justice (CEPEJ)" (8 February 2018) <https://www.coe.int/en/web/cepej/-/launch-of-cepej-s-work-on-the-use-of-artificial-intelligence-ai-in-judicial-systems>.

68 Citizen Lab, 2018 Citizen Lab Summer Institute (University of Toronto, June 13-15, 2018) <https://citizenlab.ca/summerinstitute/2018.html>. The Chatham House Rule reads that "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." See Chatham House: The Royal Institute of International Affairs, "Chatham House Rule," Accessed 10 August 2018, <https://www.chathamhouse.org/chatham-house-rule>

The Canadian Context: What We Know

Public records demonstrate that the Canadian government already makes use of automated decision systems in the immigration and refugee law context, as well as in related areas, such as border and national security screening. However, a number of data points suggest that government interest in, and adoption of, these technologies may be accelerating. Some of these developments are quite encouraging from a human rights perspective; others may contribute to increased risk and concern of human rights violations. This section provides a general overview of what is known about the Canadian government's current and intended use of automated decision systems, with a particular focus on the immigration and refugee context.

Experimenting with "Predictive Analytics"

Since 2014, IRCC has been in the process of developing a "predictive analytics" system to automate activities currently conducted by immigration officials and to support the evaluation of immigrant and visitor applications.[69] The system, as reported, will or can be used "to identify the merits of an immigration application, spot potential red flags for fraud and weigh all these factors to recommend whether an applicant should be accepted or refused."[70] Public statements from the federal government indicate that the proposed development and adoption of this technology emerged in response to an immigration system encumbered by backlogs and delays. The project was initiated in early 2013, but as reported in the *Toronto Star* in 2017, it is unclear how much progress has been made. In that article, a spokesperson for IRCC highlighted the need for "extensive testing" and "quality assurance" prior to adoption, explaining that IRCC envisions a multi-phased, program-by-program approach.[71] A call with a senior IRCC data analyst in June 2018 confirmed that IRCC is already using some form of automated system to "triage" certain applications into two streams, with "simple" cases being processed and "complex" cases being flagged for review.[72] The data analyst also confirmed that IRCC had experimented with a pilot program to use automated systems in the Express Entry application stream, which has since been discontinued.[73] The IHRP and Citizen Lab have a number of outstanding access to information requests, the results of which are likely to clarify these facts and the rationale for program discontinuance.

It should be noted that "predictive analytics" technology is already used extensively throughout the federal government in other fields and to achieve a range of objectives. For example, documents from 2014 obtained under the *Access to Information Act* note that the Canada Revenue Agency (CRA) uses predictive analytics to address non-compliance and that it has planned to use the results of these predictive systems to

---

69 Nicholas Keung, "Canadian immigration applications could soon be assessed by computers," *Toronto Star* (5 January 2017) <https://www.thestar.com/news/immigration/2017/01/05/immigration-applications-could-soon-be-assessed-by-computers.html>.

70 Ibid.

71 Ibid.

72 IHRP call with data analyst (name withheld) at Immigration, Refugees, and Citizenship Canada, 5 June 2018, with regard to Access to Information requests #A-2018-00848, A-2018-00877; A-2018-00866; A-2018-00857, A-2018-00852; A-2018-00849; A-2018-00848; A-2018-00836; and A-2018-00831.

73 Ibid.

experiment with interventions to modify the behaviour of taxpaying enterprises.[74] The same report notes that Employment and Social Development Canada (ESDC), the body responsible for administering employment insurance and benefits, had apparently "greatly improved the effectiveness of its overpayment investigations by using a risk-scoring algorithm."[75] It also mentioned that the Department of Justice (DOJ) planned to "use predictive models to manage legal risks and allocate resources for legal service delivery."[76]

A Search for New "Artificial Intelligence Solutions"

In April 2018, an RFI was submitted by IRCC, ESDC, and the DOJ with regard to a proposed "Artificial Intelligence Solution."[77] An RFI is a preliminary form of procurement document, and allows government to seek input and guidance from industry vendors prior to pursuing a more formal process for the acquisition of private sector technology or services. In this case, the RFI pertained to two separate pilot projects, one of which is between the IRCC and the DOJ. The document specifies that "AI/ML powered solutions leveraging data-driven insights are sought to assist and inform three activities: legal research and development of legal advice/legal risk assessments; prediction of outcomes in litigation; and trend analysis in litigation."[78] The requesting departments also sought to "explore the possibility of whether or not the AI/ML powered solution(s) could also be used by front-end IRCC administrative decision-makers across the domestic and international networks to aid in their assessment of the merits of an application before decisions are finalized."[79]

In other words, the proposed technology would be involved in screening cases for strategic legal purposes, as well as potentially for assisting administrative decision-makers in reaching conclusions in the longer-term. The proposed users of the technology include "IRCC Litigation Analysts, DOJ Departmental Legal Services Unit counsel and regional DOJ litigators and paralegals," who currently conduct legal research and analysis "manually."[80] The specific functionalities sought include the abilities to:

- "Allow users to conduct detailed research of case law relevant to a particular legal question and factor(s);
- Use historical data to predict the likelihood of a case being successfully litigated;
- Provide an analysis or narrative explaining which factors about a specific case are most relevant for predicting the likelihood of successful litigation; and
- Identify/summarize the relevance of similar cases within the existing case law history."[81]

---

74 Shared Services Canada, Steering Committee on Big Data, "Diagnostic Report" (8 December 2014), released under the *Access to Information Act* to Lex Gill (Citizen Lab) at page 8 <https://drive.google.com/file/d/1HpVgzMdF7SPH319iNA2wkkQkDwDax7F7/view?usp=sharing>.

75 Ibid.

76 Ibid.

77 Public Works and Government Services Canada, "Artificial Intelligence Solution (B8607-180311/A)," Tender Notice, (13 April 2018, amended 23 May 2018) <https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EE-017-33462>.

78 Ibid.

79 Ibid.

80 Ibid.

81 Ibid.

It is notable that the two specific use cases identified in the RFI are Humanitarian and Compassionate (H&C) applications and Pre-Removal Risk Assessments (PRRAs).[82] H&C applications and PRRAs are considered applications "of last resort." Both are considered highly discretionary and involve very vulnerable individuals.

Policy Engagement and Standard Setting

In April 2018, the Treasury Board of Canada Secretariat (TBCS) released a White Paper on "Responsible Artificial Intelligence in the Government of Canada."[83] The White Paper envisions a broad range of use cases for artificial intelligence technologies in government, from streamlined service delivery to policy design, risk response, and internal government service provision.[84] The document notes that these applications exist on a spectrum—from the routine and formalistic (such as processing payments) to those which are "critical to the fundamental well-being of people, the economy, and the state."[85] The White Paper commits TBCS to the development of "a tool by which institutions can assess the degree of automation that is appropriate for their program" based on the degree of potential risk to those interests.[86] It also addresses issues of privacy, bias, explainability, and transparency to some degree, setting out a list of seven principles for "responsible" government adoption of artificial intelligence technology.[87] These include an emphasis on democratic governance, auditability, transparency (as balanced against privacy and national security), the need for contingencies and alternatives in case of system failure, diversity in those who design and evaluate AI systems, and the desire to minimize negative consequences to existing workers.[88] They also specifically note that systems deployed on behalf of government "should be trained to reflect .... Canadian and international human rights obligations" and "used to reinforce these values where possible" as well as be "developed in a diverse team that includes individuals capable of assessing the ethical and socioeconomic implications of the system."[89]

While these principles are reassuring, they remain non-binding and aspirational at present. However, TBSC has also been in the process of a semi-public stakeholder consultation in order to develop a new draft Directive (initially proposed as a Standard) on the use of automated decision systems.[90] The Directive—if adopted—would mandatorily apply to technologies like those sought in the RFI described above, as well as retroactively, to all preexisting automated decision systems used by federal government institutions.[91] It is interesting to

82 Ibid.

83 Treasury Board of Canada Secretariat, "Responsible Artificial Intelligence in the Government of Canada," *Digital Disruption White Paper Series* (10 April 2018) <https://docs.google.com/document/d/1Sn-qBZUXEUG4dVk909eSg5qvfbpNlRhzIefWPtBwbxY/edit>.

84 Ibid.

85 Ibid at page 19.

86 Ibid.

87 Ibid at page 4.

88 Ibid.

89 Ibid.

90 Treasury Board Canada Secretariat, "Treasury Board Directive on Automated Decision Making," Draft 1.0 (uploaded 9 August 2018) <https://wiki.gccollab.ca/Treasury_Board_Directive_on_Automated_Decision_Making>.

91 Ibid at 1.2.

note that the proposed requirements are extensive—and compared to current practice, they would appear to represent a dramatic change of course.

For example, the Directive would require advance notice to individuals that an automated decision system will be used to render a decision, as well as certain transparency requirements that explain how the decision will be made.[92] It also includes proposed requirements for public-by-default source code (alongside a framework for justified non-disclosure);[93] high-level principles with regard to testing and monitoring training data for bias;[94] clear process for recourse and/or appeal of decisions;[95] and annual reporting obligations.[96] Importantly, once a decision is rendered, the proposed Directive would require "a meaningful explanation to affected individuals of how and why the decision was made," commensurate with the degree of impact on the rights or interests of the affected party.[97] This requirement would be in some ways similar to provisions concerning automated decision-making under the European Union's General Data Protection Regulation (GDPR), which require notice and may provide some limited form of a "right to explanation" for decisions rendered by automated systems.[98]

The proposed Directive would also require the completion of an Algorithmic Impact Assessment (AIA) prior to adoption (and retroactive assessments for technologies currently in use).[99] The inclusion of AIAs into this framework is motivated by calls in 2018 from Nesta and the AI Now Institute, two major civil society agencies based in the United Kingdom and the United States respectively.[100] Both have suggested that some form of AIA become a requirement for public sector adoption of automated decision system technology, though the particular requirements of such a process remain in development.[101] In general, the draft Directive envisions a model where greater safeguards, oversight, and procedural rights are engaged as the potential impact on "the rights or interests of an individual, community, organization, society, or the environment" increases.[102] From a human rights perspective, these proposed requirements are promising. However, it should be

92 Ibid at 6.2.1

93 Ibid at 6.2.3, 6.2.4, 6.2.5.

94 Ibid at 6.3.1, 6.3.2.

95 Ibid at 6.4.1.

96 Ibid at 6.5.1, 6.5.2.

97 Ibid at 6.2.2, Appendix C.

98 See Recital 71, Art. 14(2)(g), and Art. 15(1)(h) , General Data Protection Regulation (GDPR) (EU) 2016/679 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>. The GDPR moreover requires human intervention in automated decisions with legal or "similarly significant" effects on an individual, in Art. 22 ("Automated individual decision-making, including profiling").

99 Treasury Board Canada Secretariat, "Treasury Board Directive on Automated Decision Making," Draft 1.0 (uploaded 9 August 2018) <https://wiki.gccollab.ca/Treasury_Board_Directive_on_Automated_Decision_Making> at 1.2, 6.1, Appendix B.

100 Michael Karlin (Supergovernance), "A Canadian Algorithmic Impact Assessment," *Medium* (18 March 2018) <https://medium.com/@supergovernance/a-canadian-algorithmic-impact-assessment-128a2b2e7f85>.

101 Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker (2018), "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability," *AI Now Institute* <https://ainowinstitute.org/aiareport2018.pdf>; Eddie Copeland, "10 principles for public sector use of algorithmic decision making," *Nesta (Blog)* (20 February 2018) <https://www.nesta.org.uk/blog/10-principles-for-public-sector-use-of-algorithmic-decision-making/>.

102 Treasury Board Canada Secretariat, "Treasury Board Directive on Automated Decision Making," Draft 1.0 (uploaded 9 August 2018) <https://wiki.gccollab.ca/Treasury_Board_Directive_on_Automated_Decision_Making> at Appendix B.

reiterated that as of August 2018, this document remains non-binding and subject to change.

The Intersection of Immigration Law, Public Safety, and National Security

The immigration and refugee law context is closely interconnected with Canada's national security apparatus. Under the authority of the *Canadian Security Intelligence Service Act (CSIS Act)*, Canada's intelligence service has expansive powers to enter into arrangements with foreign states and other entities for the purpose of conducting security assessments, to provide advice and information to any minister with regard to security matters or criminal activities, and to conduct investigations in support of government objectives under the *Citizenship Act* or the *Immigration and Refugee Protection Act*.[103] For example, CSIS may provide information related to findings of inadmissibility into Canada on the basis of national security, or evidence in security certificate screenings. As a result, the nature of the data collected and analyzed by CSIS—as well as by Canada's signals intelligence agency, the Communications Security Establishment (CSE)—is likely to eventually play some role in certain immigration-related automated decision systems.

As of this report's publication, both CSIS and the CSE are currently facing substantial reform in light of Bill C-59 (*An Act respecting national security matters*), which proposes major changes to the *CSIS Act* and which would create the *Communications Security Establishment Act*.[104] In particular, the bill involves complex and problematic amendments related to the collection, use, and disclosure of information about individuals.[105] While C-59 introduces certain much-needed reforms and a new review framework, it also further entrenches the controversial surveillance practices of both CSIS and CSE, including the mass and untargeted "bulk collection" of electronic data.[106] Despite serious concerns from the international human rights law community with regard to this practice,[107] where the subjects of surveillance are non-Canadian persons outside of Canada, no meaningful safeguards to protect their right to privacy exist.[108] This practice of mass data collection is crucial to understanding the risks of algorithmic decision-making in public policy, as it illustrates that the potential sources of "input data" for automated decision systems may be vast, open-ended, and deeply problematic from a human rights perspective. In Canada, immigrants and refugees are both at particular risk of disproportionate surveillance of their electronic communications, and also face more serious potential consequences as a result.

It should be noted that even for Canadians and persons in Canada, the proposed *CSE Act* would allow near-unlimited collection of "publicly available information" about individuals, which is broadly defined as

---

103 Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23), ss. 13-15.

104 Bill C-59, *An Act respecting national security matters*, 1st Sess, 42nd Parl, 2015 (first reading in Senate 20 June 2018) <https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=9057418>.

105 Bill C-59, An Act respecting national security matters, 1st Sess, 42nd Parl, 2015 (first reading in Senate 20 June 2018) <https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=9057418>. See also Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert (2017), "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59" <https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf>.

106 Ibid.

107 Office of the United High Commissioner for Human Rights, "The right to privacy in the digital age," (2014) A/HRC/27/37 <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>.

108 Ibid.

information "that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase."[109] In practice, this may include anything from social media posts, information sold by data brokers, and data obtained through hacks, leaks, and breaches.[110] The sheer scale of information potentially captured by such programs necessitates the use of automated and algorithmic systems for analysis in a manner which will almost inevitably have an impact on the immigration and refugee context.

CSIS and CSE are also not the only government bodies engaged in gathering intelligence or evidence in this manner. In June 2018, the National Energy Board (NEB) posted an RFI for "Security Threat Monitoring Services," seeking technology which would allow it to monitor publicly available sources related to pipeline projects and energy development.[111] The proposed intelligence gathering tool would offer "real-time capability to algorithmically process vast amounts of traditional media, open source and public social media," as well as the ability to generate briefing reports and detect risks.[112] Despite these technologies raising important human rights concerns,[113] they are likely to remain of interest to a wide range of government departments and agencies.

There are also open questions about data collection and information sharing between law enforcement and the immigration and refugee system. For example, in 2017, the RCMP faced heavy criticism for engaging in religious and ethnic profiling of migrants near the unofficial border crossing between the United States and Quebec at Roxham Road.[114] Without any clear rationale, and apparently on its own initiative, the RCMP collected questionnaires from over 5,000 asylum seekers, featuring questions clearly coloured by Islamophobic stereotypes.[115] The questionnaire sought information about social values, political beliefs, and religion—including questions related to the individual's perception of women who do not wear a hijab, their opinions on ISIS and the Taliban, as well as the number of times a day the individual prayed.[116] The questions were directly targeted toward Muslim individuals crossing the border, as no questions were included about

---

109 ss. 2 and 24(1) of the proposed Communications Security Establishment Act in An Act respecting national security matters (Bill C-59), 1st Sess 42nd Parl. First Reading, June 20, 2017 <https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/first-reading>.

110 Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert (2017), "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59" at page 49 et. seq. <https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf>.

111 Robson Fletcher, "NEB seeks contractor to monitor 'vast amounts' of online chatter for potential security threats," *CBC News* (21 June 2018) <https://www.cbc.ca/news/canada/calgary/neb-security-monitoring-services-contractor-request-1.4715921>.

112 National Energy Board, "Security Threat Monitoring Services (#84084-18-0093)" RFI Process (19 June 2018) <https://buyandsell.gc.ca/cds/public/2018/06/19/0fca7d98764973b16caf4ccdc156d6af/rfi_84084-18-0093_eng.pdf> at pages 2-3.

113 See for example, Citizen Lab (Ronald J. Deibert), "Letter to Canada's National Energy Board Regarding 'Security Threat Monitoring Services' Request for Information," (25 June 2018) <https://citizenlab.ca/wp-content/uploads/2018/06/citizen-lab-letter-national-energy-board-canada.pdf>.

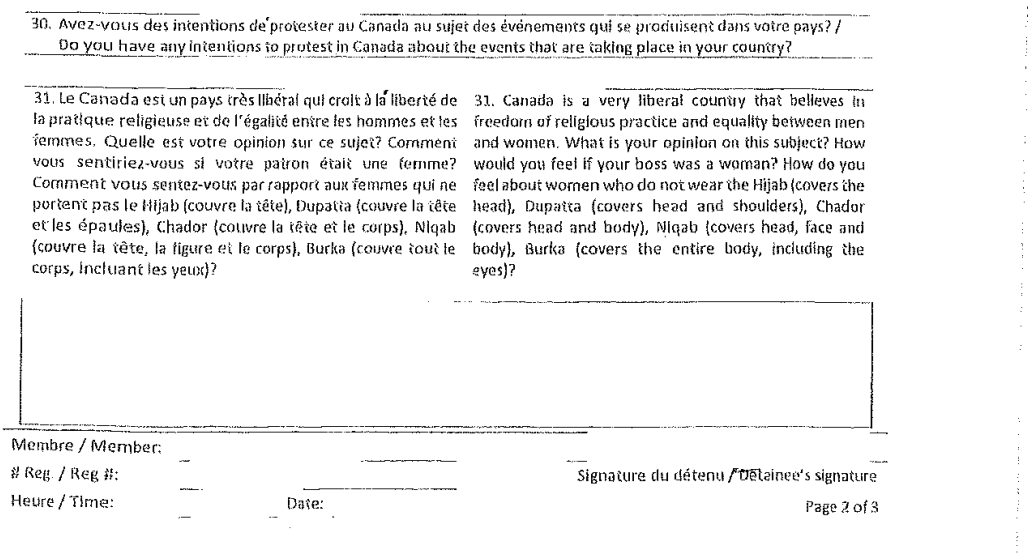
114 Ingrid Peritz and Daniel Leblanc, "RCMP accused of racial profiling over 'interview guide' targeting Muslim border crossers," *The Globe and Mail* (12 October 2017) <https://www.theglobeandmail.com/news/national/rcmp-halts-use-of-screening-questionnaire-aimed-at-muslim-asylum-seekers/article36560918/>.

115 Michelle Shepherd, "RCMP will redact more than 5,000 records collected using questionnaire targeting Muslim asylum seekers" *Toronto Star* (27 November 2017) <https://www.thestar.com/news/canada/2017/11/27/rcmp-will-redact-more-than-5000-records-collected-using-questionnaire-targeting-muslim-asylum-seekers.html>.

116 Ibid.

other religious practices or terrorist groups.[117] According to RCMP spokesperson, the collected answers were then entered into an RCMP database, which could be shared with CBSA and "other security partners."[118] The RCMP claims that the questionnaire ceased to be used following an investigation by the *Toronto Star* in October 2017 and that 5,438 files have been redacted.[119] However, concerns remain about the data, including its collection and storage, the extent to which it may have been shared with other agencies or foreign partners, and oversight related to its use. The RCMP questionnaire is part of a larger story about the risk that data fed into technological systems—whether used by administrative bodies, national security agencies, or law enforcement—may be coloured by both implicit and explicit bias.

"How would you feel if your boss was a woman?" RCMP QUESTIONNAIRE[120]



30. Avez-vous des intentions de protester au Canada au sujet des événements qui se produisent dans votre pays? / Do you have any intentions to protest in Canada about the events that are taking place in your country?

31. Le Canada est un pays très libéral qui croit à la liberté de la pratique religieuse et de l'égalité entre les hommes et les femmes. Quelle est votre opinion sur ce sujet? Comment vous sentiriez-vous si votre patron était une femme? Comment vous sentez-vous par rapport aux femmes qui ne portent pas le Hijab (couvre la tête), Dupatta (couvre la tête et les épaules), Chador (couvre la tête et le corps), Niqab (couvre la tête, la figure et le corps), Burka (couvre tout le corps, incluant les yeux)?

31. Canada is a very liberal country that believes in freedom of religious practice and equality between men and women. What is your opinion on this subject? How would you feel if your boss was a woman? How do you feel about women who do not wear the Hijab (covers the head), Dupatta (covers head and shoulders), Chador (covers head and body), Niqab (covers head, face and body), Burka (covers the entire body, including the eyes)?

Membre / Member:

Reg. / Reg #:

Heure / Time: Date:

Signature du détenu / Detainee's signature

Page 2 of 3

This pattern of rights-violating data collection also applies in the border security context, where large and secretive databases are used to profile and identify individuals for secondary screening, questioning, detention, refusal, and arrest at ports of entry. CBSA has direct access to some law enforcement databases,[121]

117 Ibid.

118 Michelle Shephard, "RCMP officers screened Quebec border crossers on religion and values, questionnaire shows," The *Toronto Star* (11 October 2017) <https://www.thestar.com/news/canada/2017/10/11/rcmp-officers-screened-quebec-border-crossers-on-religion-and-values-questionnaire-shows.html>.

119 Michelle Shepherd, "RCMP will redact more than 5,000 records collected using questionnaire targeting Muslim asylum seekers" *Toronto Star* (27 November 2017) <https://www.thestar.com/news/canada/2017/11/27/rcmp-will-redact-more-than-5000-records-collected-using-questionnaire-targeting-muslim-asylum-seekers.html>.

120 For full questionnaire, see Appendix B of this report.

121 See e.g., *Martin-Ivie v. Canada (Attorney General)*, 2013 FC 772 at paragraph 25:
"The [Border Security Officers] in secondary have access to a number of databases:

a. ICES, a CBSA database that, amongst other things, contains information about Canadians who have come into contact with CBSA or individuals who might seek to enter the country and might pose a risk;
b. Field Operations Support System [FOSS], Citizenship and Immigration Canada [CIC] and CBSA's shared database, which contains millions of records about all CBSA and CIC contacts with non-Canadian citizens;
c. Canadian Police Information Center [CPIC], the database used by Canadian law enforcement agencies; and

including access to the Canadian Police Information Centre (CPIC) database, which contains sensitive health information, including suicide attempts and apprehension warrants under the *Mental Health Act*.[122]

There have also been long-standing civil liberties concerns with the Canadian Passenger Protect program (i.e., the "no-fly list")—from issues with false positives and other errors, to the listing of children, to weak or entirely non-existent mechanisms for redress.[123] In June 2018, a Canadian journalist writing for *The Guardian*, citing documents obtained through an ATI request, revealed that Canada also adheres to a second list called Tuscan (Tipoff US/Canada), a secret database which essentially functions "as a second, unofficial no-fly list" maintained entirely by the United States and not bound by Canadian rules or safeguards.[124] The CBSA also uses a Scenario Based Targeting (SBT) system to identify potential security threats, using algorithms to process large volumes of personal information (such as age, gender, nationality, and travel routes) to profile individuals.[125] The system assesses travelers for "predictive risk factors" in areas that include "immigration fraud, organized and transnational crime, smuggling of contraband, and terrorism and terrorism-related crimes."[126] A 2017 report from the Office of the Privacy Commissioner indicated that while some safeguards had been put in place to limit the threat that SBT posed to privacy rights and civil liberties, various gaps remained.[127]

Notably, in July of 2017, the Court of Justice of the European Union (CJEU) held in an opinion that the proposed EU-Canada Passenger Name Records (PNR) data sharing agreement was incompatible with fundamental rights recognised by the EU and could not be signed.[128] The CJEU opinion highlighted that the Canadian system for risk assessments of EU travellers operated in "a systematic and automated manner, and with a "significant" margin of error exposing a large number of individuals who posed no risk to ongoing scrutiny by CBSA and other agencies.[129] The opinion emphasized that algorithmic systems and risk

---

d. National Crime Information Center [NCIC], a somewhat comparable database used by American law enforcement agencies."

122 Ann Cavoukian (2014), "Crossing the Line The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC" <https://www.ipc.on.ca/wp-content/uploads/Resources/indiscriminate_disclosure.pdf> at page 11.

123 See, for example Canadian Civil Liberties Association, "Submission to the Standing Committee on Public Safety and National Security regarding Bill C-59, An Act respecting national security matters" (January 2018) <https://www.ourcommons.ca/Content/Committee/421/SECU/Brief/BR9643692/br-external/CanadianCivilLibertiesAssociation-e.pdf>

124 Justin Ling, "Inside Tuscan: the other no-fly list Canada didn't tell you about," *The Guardian* (30 June 2018) <https://www.theguardian.com/world/2018/jun/30/canada-us-tuscan-database-no-fly-list-trudeau>.

125 Office of the Privacy Commissioner of Canada, "Canada Border Services Agency – Scenario Based Targeting of Travelers – National Security" (last modified 21 September 2017) <https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_cbsa_2017/>.

126 Ibid.

127 Ibid.

128 Access Now, "In Win for Privacy, European Court Rejects EU-Canada 'PNR' Agreement", 26 July 2017 <https://www.accessnow.org/win-privacy-european-court-rejects-eu-canada-pnr-agreement/>; Court of Justice of the European Union, "The Court declares that the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data may not be concluded in its current form," Press Release No 84/17, Luxembour (26 July 2017) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf>.

129 Joint Civil Society Response to Discussion Guide on a 2nd Additional Protocol to the Budapest Convention on Cybercrime, 28 June 2018 (Electronic Frontier Foundation, European Digital Rights, Association for Civil Rights, Derechos Digitales, Elektronisk Forpost Norge, IPANDETEC, Karisma Foundation, OpenMedia, Panoptykon Foundation, R3D: Red en Defensa de los Derechos Digitales, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, SonTusDatos (Artículo 12, A.C.) and TEDIC) <https://www.eff.org/Submission-COE-Protocol-Cross-Border-Access-Data> at pages 27-28.

assessment technology must be "applied in a non-discriminatory manner,"[130] and that final decisions "are based 'solely and decisively' on individualized human-based assessment." Negotiations between Canada and the EU related to the agreement (which is not yet in effect) remain ongoing.[131]

The Canadian government is also investing in new border security and identification efforts, many of which have been criticized by immigration lawyers and civil liberties advocates alike. They include an expansion of efforts to collect fingerprints of foreign nationals[132] and a move toward developing a "Known Traveller Digital Identity concept" to facilitate "pre-vetting risk assessment and security procedures," for example, by allowing "for risk-based immigration lanes."[133] In July 2018, it was also revealed that CBSA has employed the use of private third-party DNA ancestry services such as Familytreedna.com and Ancestry.com to establish the nationality of individuals subject to potential deportation.[134] These measures raise concerns not only because of the coercive nature of the privacy invasion, but also because one's DNA is clearly not determinative of (and indeed, often entirely unrelated to) nationality.

130 Ibid.

131 Joint Cooperation Committee to the Joint Ministerial Committee (2018), "Annual Report on the State of the EU-Canada Relationship" <https://eeas.europa.eu/sites/eeas/files/eu-canada_annual_report_2018.pdf> at paragraph 64; and European Commission Migration and Home Affairs, "Passenger Name Record (PNR) " (8 March 2018) <https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en>.

132 Kathleen Harris, "Ottawa expands program to collect fingerprints, photos from foreign nationals coming to Canada," *CBC News* (5 June 2018) <http://www.cbc.ca/news/politics/ottawa-expands-program-to-collect-fingerprints-photos-from-foreign-nationals-coming-to-canada-1.4690735>; Nicholas Keung, "Travellers from Europe, Middle East, Africa now must provide fingerprints when applying to visit Canada" The *Toronto Star* (29 July 2018) <https://www.thestar.com/news/immigration/2018/07/28/travellers-from-europe-middle-east-africa-now-must-provide-fingerprints-when-applying-to-visit-canada.html>.

133 World Economic Forum, "The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel," (January 2018) at pages 5 and 16 <http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf>.

134 Tamara Khandaker, "Canada is Using Ancestry DNA Websites to Help It Deport People" Vice News (26 July 2018) <https://news.vice.com/en_ca/article/wjkxmy/canada-is-using-ancestry-dna-websites-to-help-it-deport-people>.

Canada's Immigration System: A Taxonomy

Canada's immigration system falls under the rubric of administrative law and is federally regulated by the Ministry of Immigration, Refugees and Citizenship Canada (IRCC). It is governed by the *Immigration and Refugee Protection Act* (IRPA),[135] the *Immigration and Refugee Protection Regulations* (IRPR),[136] and internal operational manuals for its various subsidiary branches. All initial immigration decisions are made by either an administrative tribunal such as the Immigration and Refugee Board or individual immigration officers employed by Immigration, Refugees and Citizenship Canada, or by the enforcement arm of the immigration system, the Canadian Border Services Agency (CBSA). These decisions are then reviewable either by an appeals body such as the Refugee Appeal Division and/or by the Federal Court of Canada and the Federal Court of Appeal, before moving up to the Supreme Court of Canada.

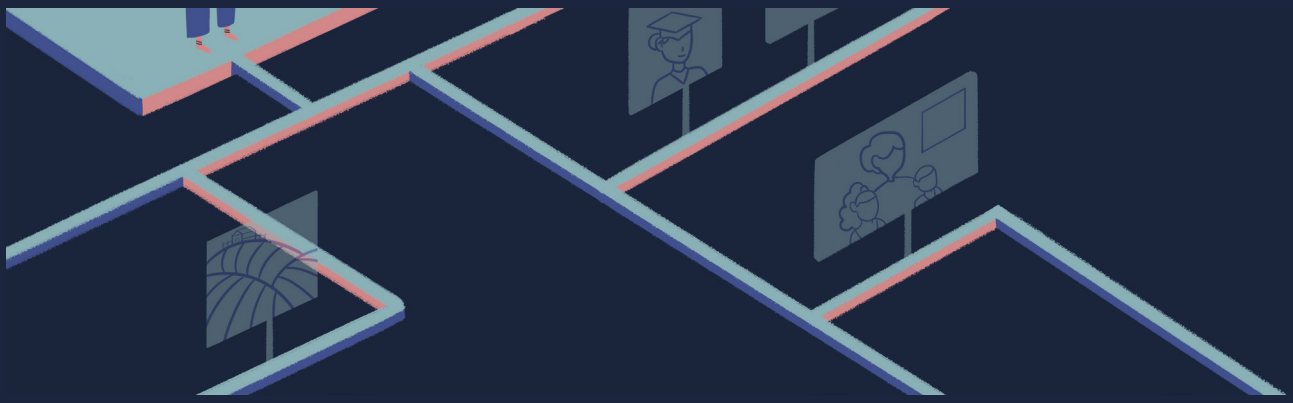
At every stage of a person's immigration proceedings, many decisions are made regarding their application. The following taxonomy situates the reader in the centre of the narrative and traces a person's journey through the Canadian immigration system to highlight the multiple instances in which automated decision-making could be introduced to augment or replace the decision-making of human officers, highlighting the potential pitfalls and human rights risks. This analysis offers a few questions about the potential use of automated decision systems in each context—but they are by no means exhaustive. This section is written with immigrants and refugees applying to enter Canada in mind, as they are most directly impacted by these systems. For those who are not immigrants or refugees, the hope is that reading from this perspective will prompt more internalized reflections on the far-reaching impacts of algorithmic decision-making in the immigration and refugee context.

HOW COULD YOU BE AFFECTED IF AN AUTOMATED SYSTEM DECIDED YOUR IMMIGRATION APPLICATION?

135 *Immigration and Refugee Protection Act* (IRPA), SC 2001, c. 27, 1 November 2001, available at: <http://www.refworld.org/docid/4f0dc8f12.html>

136 *Immigration and Refugee Protection Regulations*, 11 June 2002, SOR/2002-227, available at: http://www.refworld.org/docid/4f0efde32.html

Pre-Arrival



Before you set foot on Canadian soil, there are multiple ways that automated decision-making could impact your application. This decision-making in the numerous immigration and temporary visa streams, temporary foreign worker programs, and family sponsorship schemes all present the possibility of rights violations and prejudicial impacts.

The Government has been employing automated decision systems in the Express Entry Comprehensive Ranking System for prospective applicants.[137] However, it is not clear how exactly these automated systems

Canada Runs Many Immigration and Temporary Visa Streams

Immigration:

- Express Entry Program
- Startup Visa Program
- Self-Employed Person in Cultural or Athletic Activities or at a Farm Program
- Provincial Nominees Program
- Atlantic Immigration Pilot program
- Immigrant Investor Program
- Quebec Skilled Workers Program

Visas:

- Tourist Visas, Work Visas, International Student Visas

Temporary Foreign Worker Programs
Family Sponsorship Programs

137 Steven Meurrens, "How to Help International Students Stay in Canada," *IRPP Policy Options* (12 September 2016) <http://policyoptions.irpp.org/magazines/september-2016/how-to-help-international-students-stay-in-canada/>

are used, or what criteria they are evaluating. For example, an algorithm could be optimized to determine any of the following, or for any other unknown objective:

- Completeness of your application;
- Likelihood or risk that your application is fraudulent;
- Probability that your marriage is "genuine"; or
- Probability that your child is biologically or legally yours.

The government is also planning on using algorithms to screen for "risk" and "fraud."[138] This screening may pertain to admissibility proceedings, which is a parallel decision-making process under section 33 of the IRPA to determine whether or not you can be admitted to Canada in the first place.

You can be found to be inadmissible into Canada for:

- Section 34(1): Ground of National Security (espionage, subversion of government, terrorism, among others)
- Section 35(1): International Human Rights Violations
- Section 36(1): Serious Criminality
- Section 38: Medical Inadmissibility
- Section 39: Financial Inadmissibility
- Section 40: Misrepresentation

Potential Impacts and Risks of Automated Decision Systems:

- What criteria will be used to define and assess "fraud" or "misrepresentation"?
- What type of data or evidence will be harvested and fed into the automated system?
- Who will have access to this information, and how will it be shared with other departments?
- What does the government consider an "acceptable" margin of error for these systems?
- What will be the grounds of appeal or redress if an automated system makes or supports an inadmissibility finding against you?

138 Nicholas Keung, "Canadian immigration applications could soon be assessed by computers," *Toronto Star* (5 January 2017) <https://www.thestar.com/news/immigration/2017/01/05/immigration-applications-could-soon-be-assessed-by-computers.html>. See also Justin Ling, "Federal government looks to AI in addressing issues with immigration system," *The Globe and Mail* (31 May 2018) <https://www.theglobeandmail.com/politics/article-federal-government-looks-to-ai-in-addressing-issues-with-immigration>

At the Border

Once you arrive at the Canadian border, you have access to certain applications for temporary or permanent status. For example, you can declare that you intend to file for refugee or protected persons status, under sections 96 and 97 of the *IRPA*. However, at the border, you are generally under the jurisdiction of the Canadian Border Services Agency (CBSA), which operates as the enforcement branch of IRCC. CBSA can assess whether you pose a threat to national security, and has the power to deny you entry into the country or hold you in detention. CBSA can also find you inadmissible and deport you from Canada.

Potential Impacts and Risks of Automated Decision Systems:

- Will an automated system screen you as a high risk traveler? A risk to national security?
- Will an automated system have the power to preselect or recommend you for secondary screening, detention and questioning?
- On what grounds can an automated system make these determinations?
- Will this data be shared with law enforcement or intelligence agencies?
- Will this data be shared with your country of origin or another country?
- What can you do to challenge the decision of an automated system, or a decision made with the support of an automated system, to detain you or deny you entry into Canada?
- Will this decision by an automated system bar you from being able to enter Canada in the future?

In Country

You are now in Canada. You can apply for refugee protection in-land under section 96 and 97 of the *IRPA*. You can extend your temporary work permit or visa and eventually file for permanent residence and citizenship. You can file a Humanitarian and Compassionate application (H&C) for permanent residence under section 25 of the *IRPA*, a discretionary application for status often used as a last resort to stay in Canada. You can also apply for a Pre-Removal Risk Assessment (PRRA) to assess the risk you will face if you are removed from Canada.

In-Country Applications:

- Refugee claims under section 96 and 97 of IRPA
- Visa Extensions under section 181 of IRPR
- Applications for Permanent Residence under section 10.1 of IRPA
- Applications for Citizenship under the *Citizenship Act*
- Humanitarian and Compassionate Applications under section 25 of IRPA
- Pre-Removal Risk Assessments under section 112.1 of IRPA

The government is seeking to introduce algorithms to help determine "risk" and "fraud" in refugee status applications. However, it is not clear what these terms mean and what exactly an algorithm is supposed to be looking for during the application process for protection and permanent residence.

Potential Impacts and Risks of Automated Decision Systems:

- Will an automated system decide that your refugee claim is likely to fail?
- Will an automated decision system flag your file as potentially fraudulent?
- How could this predetermination prejudice your claim for protection?
- In H&C and PRRA applications, will an automated system weigh the evidence for and against you? What evidence would that be?
- How will an automated decision system contribute to making determinations on what are meant to be "compassionate" grounds?

- Will an automated system provide a recommendation or predetermination with the officer deciding your case? Could this be prejudicial for you?
- How will this data be shared?

Leaving Canada

If your temporary status has come to an end, if you were not successful in your application for refugee status or protection, or if you were found to have engaged in serious criminal conduct, the government can start proceedings to remove you from Canada.

During deportation proceedings, CBSA may collect data which could be shared with other departments and may prevent you from being able to enter Canada in the future. This data could also be shared with your country of origin, putting you in danger with your government if you are escaping persecution.

The Ministry of Public Safety and Emergency Preparedness can also invoke a rare provision in the IRPA and issue a security certificate against you (sections 33 and 77 to 85 of IRPA), to remove you from Canada on grounds of national security.[139] Some of the information pertaining to these proceedings may not be disclosed to you, an issue that remains constitutionally ambiguous (and which has been subject of significant concern from the Supreme Court).[140]

139 Public Safety Canada, "Safety certificates," amended 1 December 2015 <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/scrt-crtfcts-en.aspx>

140 See, for example *Suresh v Canada (Minister of Citizenship and Immigration)*, [2002] 1 S.C.R. 3; *Charkaoui v Canada (Minister of Citizenship and Immigration)*, 2007 SCC 9; *Jaballah v. Canada (Minister of Public Safety and Emergency Preparedness)* (2006 FC).

International Human Rights and *Charter* Impacts

International law is a body of rules and norms recognized as binding by nations who have signed onto treaties and conventions. The foundational document of modern international human rights law is the Universal Declaration of Human Rights (UDHR), adopted by the United Nations in 1948. The UDHR is not a treaty and therefore is not binding on states. However, it spurred the creation of a number of international instruments which are binding on nations who have ratified them. These treaties are supplemented by regional instruments which also enshrine human rights.

CANADA HAS RATIFIED:[141]

International Covenant on Economic, Social and Cultural Rights
International Covenant on Civil and Political Rights
International Convention on the Elimination of All Forms of Racial Discrimination
Convention on the Elimination of All Forms of Discrimination Against Women
Convention on the Rights of Persons with Disabilities
Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
Convention on the Rights of the Child
Convention Relating to the Status of Refugees and
Protocol Relating to the Status of Refugees

OTHER RELEVANT INTERNATIONAL INSTRUMENTS:

American Declaration of the Rights and Duties of Man
Universal Declaration of Human Rights
UNHCR Guidelines on International Protection of Refugees
UN Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief.

\+ The Canadian Charter of Rights and Freedoms

DOMESTIC INSTRUMENTS:

Canadian Charter of Rights and Freedoms
Immigration and Refugee Protection Act
Provincial Human Rights Acts

141 For all ratification dates, please see United Nations Human Rights Office of The High Commissioner, "Status of Ratification Interactive Dashboard," Accessed 9 August 2018 <http://indicators.ohchr.org>

Equality Rights and Freedom from Discrimination

Equality rights and freedom from discrimination are widely protected under various international legal instruments that Canada has ratified: the *International Covenant on Economic, Social and Cultural Rights* (ICESCR),[142] the *International Covenant on Civil and Political Rights* (ICCPR),[143] the *International Convention on the Elimination of All Forms of Racial Discrimination* (ICERD),[144] the *Convention on the Elimination of All Forms of Discrimination Against Women* (CEDAW),[145] the *Convention on the Rights of Persons with Disabilities* (CRPD),[146] the *Convention on the Rights of the Child* (CRC),[147] and the *Convention Relating to the Status of Refugees*,[148] with its accompanying *Protocol*.[149] Canada has also adopted the Inter-American Commission on Human Rights' *American Declaration of the Rights and Duties of Man* (the 'Bogota Declaration')[150] and the *Universal Declaration of Human Rights*.[151] The United High Commissioner for Refugees (UNHCR) has also issued guidelines specific to countering discrimination against refugees.[152] Regional initiatives such as the May 2018 "Toronto Declaration" focus on the rights to equality and non-discrimination in machine learning systems specifically.[153] In Canada, section 15 of the *Charter* enshrines equality rights and freedom from discrimination. All provinces and territories also have their own anti-discrimination legislation.

---

142 *International Covenant on Economic, Social and Cultural Rights* (ICESCR), 19 December 1966, ratified by Canada 1976, 993 U.N.T.S. 3, Can. T.S. 1976 No. 46, 6 I.L.M. 360, entered into force 3 January 1976, ratified by Canada 1976, <https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx>

143 *International Covenant on Civil and Political Rights* (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>, ratified by Canada on May 19, 1970.

144 *International Convention on the Elimination of All Forms of Racial Discrimination*, December 21, 1965, 660 U.N.T.S. 195 ratified by Canada in 1970, <https://www.ohchr.org/en/professionalinterest/pages/cerd.asx>

145 *Convention on the Elimination of All Forms of Discrimination against Women* (CEDAW), adopted December 18, 1979, G.A. res. 34/180, 34 U.N. GAOR Supp. (No. 46) at 193, U.N. Doc. A/34/46, entered into force September 3, 1981, ratified by Canada 1981, <https://www.ohchr.org/en/professionalinterest/pages/cedaw.aspx>

146 *Convention on the Rights of Persons with Disabilities* (CRPD), adopted December 13, 2006, G.A. Res. 61/106, Annex I, U.N. GAOR, 61st Sess., Supp. (No. 49) at 65, U.N. Doc. A/61/49 (2006), entered into force May 3, 2008, <https://www.ohchr.org/en/hrbodies/crpd/pages/crpdindex.aspx>

147 Convention on the Rights of the Child (CRC), adopted November 20, 1989, G.A. Res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989), entered into force September 2, 1990, ratified by Canada 1991, <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>

148 *Convention relating to the Status of Refugees*, 189 U.N.T.S. 150, entered into force April 22, 1954, ratified by Canada on 4 June 1969

149 UN General Assembly, *Protocol Relating to the Status of Refugees*, 31 January 1967, United Nations, Treaty Series, vol. 606, p. 267, <http://www.unhcr.org/protection/basic/3b66c2aa10/convention-protocol-relating-status-refugees.html>

150 Inter-American Commission on Human Rights (IACHR), *American Declaration of the Rights and Duties of Man*, 2 May 1948, adopted by Canada in 1948.

151 Universal Declaration of Human Rights (UDHR), adopted December 10, 1948, G.A. Res. 217A(III), U.N. Doc. A/810 at 71 (1948), art. 25.

152 United Nations High Commissioner for Refugees, "Guidelines on International Protection No. 9: Claims to Refugee Status based on Sexual Orientation and/or Gender Identity within the context of Article 1A(2) of the 1951 Convention and/or its 1967 Protocol relating to the Status of Refugees" (12 October 23) <http://www.unhcr.org/509136ca9.pdf>

153 Access Now, "The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems," *Access Now & Amnesty International* (May 2018) <https://www.accessnow.org/cms/assets/uploads/2018/05/Toronto-Declaration-D0V2.pdf>.

"Algorithms of Oppression"[154] and Automated Decision Systems

An ever-increasing amount of responsibility and processes are being delegated by governments to automated systems, often under the guise of neutrality and scientific accuracy.[155] However, these systems are by no means neutral.[156] Algorithms are vulnerable to the same decision-making concerns that plague human decision-makers: transparency, accountability, discrimination, bias, and error.[157] Biases of the individual(s) designing an automated system or selecting the data that trains it, or shortcomings of the input data itself, can be compounded to create discriminatory outcomes that not only reproduce, but even sometimes magnify patterns of discrimination. This can reflect the designer's individual prejudices or pre-existing societal biases,[158] but may also embody values[159] that system designers did not intend. Depending on how an algorithm is designed to differentiate and sort data, it may result in indirect discrimination or negative feedback loops that reinforce and exacerbate existing inequalities.[160]

Current uses of AI and ML technology already have a problematic track record with regard to discrimination.[161] Something as seemingly innocuous as a simple Google search may yield discriminatory ads targeted on the basis of racially-associated personal names,[162] or systematically display lower paying job opportunities to women.[163] Machines are also learning how to perpetuate stereotypes based on appearance, such as photo recognition software that reproduces gender stereotypes (e.g., by associating "woman" with "kitchen"[164]) or software that purports to discern sexual orientation from photos.[165] Auto-complete search forms perpetuate

---

154 Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: NYU Press, 2018).

155 David Garcia-Soriano, and Francesco Bonchi (2012), "Fair-by-design algorithms: matching problems and beyond" <https://arxiv.org/pdf/1802.02562.pdf>. See also Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham: Duke University Press, 2013).

156 Kirsten E. Martin (2018), "Ethical implications and accountability of algorithms", *Journal of Business Ethics* <https://www.researchgate.net/publication/324896361>.

157 Zeynep Tufekci (2015), "Algorithmic harms beyond Facebook and Google: emergent challenges of computational agency" *Colorado Technology Law Journal* at pages 216-217 <http://ctlj.colorado.edu/wp-content/uploads/2015/08/Tufekci-final.pdf>.

158 David Garcia-Soriano and Francesco Bonchi (2012), "Fair-by-design algorithms: matching problems and beyond" <https://arxiv.org/pdf/1802.02562.pdf> at pages 1-2.

159 Helen Nissenbaum (2001), "How computer systems embody values" *Computer* 34:3 <https://www.nyu.edu/projects/nissenbaum/papers/embodyvalues.pdf>.

160 Vivian Ng, "Algorithmic decision-making and human rights," *Technology, The Human Rights, Big Data and Technology Project* (21 April 2017) <https://www.hrbdt.ac.uk/algorithmic-decision-making-and-human-rights/>; Julia Angwin, Jeff Larson, Lauren Kirchner, and Surya Mattu, "Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk," *ProPublica* (5 April 2017) <https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk>.

161 See for example, Cathy O'Neil, *Weapons Of Math Destruction: How Big Data Increases Inequality And Threatens Democracy* (New York: Crown, 2016); Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: NYU Press, 2018).

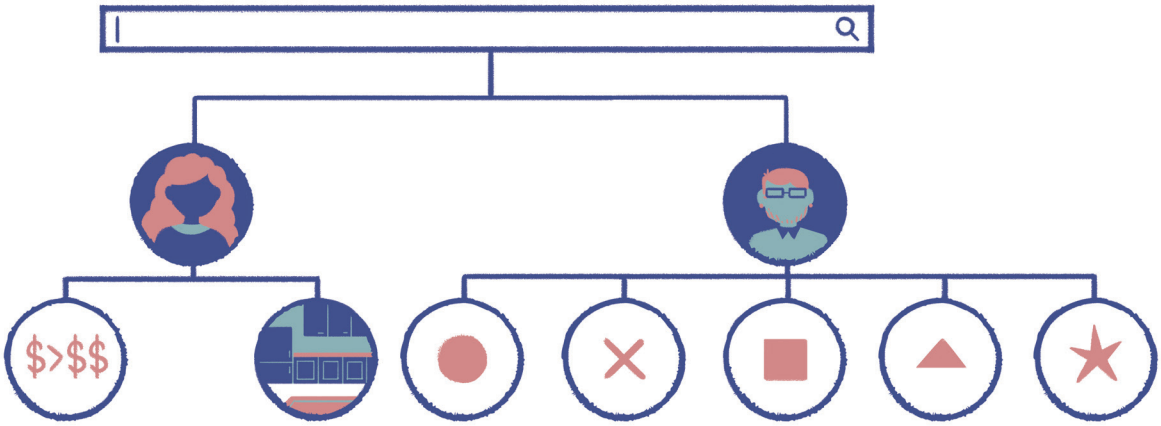
162 Latanya Sweeney (2013), "Discrimination in Online Ad Delivery" <http://dx.doi.org/10.2139/ssrn.2208240>.

163 Byron Spice, "Fewer Women Than Men Are Shown Online Ads Related to High-Paying Jobs," Carnegie Mellon University School of Computer Science (7 July 2015) <https://www.cs.cmu.edu/news/fewer-women-men-are-shown-online-ads-related-high-paying-jobs>.

164 Tom Simonite, "Machines Taught by Photos to Learn a Sexist View of Women" *Wired Magazine* (21 August 2017) archived at: <https://perma.cc/8KUQ-LPJC>.

165 Heather Murphy, "Why Stanford Researchers Tried to Create a 'Gaydar' Machine," The New York Times (9 October 2017) <https://www.nytimes.com/2017/10/09/science/stanford-sexual-orientation-study.html>

racial biases based on stereotypical appearance markers,[166] while online app stores associate popular dating apps for gay men with sex offender registry lists.[167]



There are also significant threats to individuals' other rights and liberties. Even where protected identity markers and classes of information are removed from a given dataset, discriminatory outcomes can nonetheless arise.[168] For example, the push towards the use of "predictive policing" technologies to forecast where crime is likely to occur may link racialized communities with a higher likelihood of presumed future criminality. The use of apparently "neutral" factors such as postal code may in practice serve as a proxy for race, exacerbating racial biases, affording false legitimacy to patterns of racial profiling, and undermining the presumption of innocence in the criminal justice system.[169] The Correctional Offender Management Profiling for Alternative Sanctions ("COMPAS"), an algorithm used in some United States courts to assess the risk of recidivism when making decisions relating to pre-trial detention, has come under fire for its discriminatory impact. While the algorithm was defended on the basis that it was not mathematically biased, the end result of its adoption was that individuals from racialized and vulnerable communities were falsely recommended for custodial pre-sentences at a much higher rate than white offenders.[170] The Wisconsin Supreme Court in *State v Loomis*[171] also found that while use of COMPAS does not inherently violate procedural rights, its findings must not be determinative.

---

166 Paul Baker, and Amanda Potts (2013) "'Why do white people have thin lips?' Google and the perpetuation of stereotypes via auto-complete search forms" *Critical Discourse Studies* 10:2 <https://www.tandfonline.com/doi/abs/10.1080/17405904.2012.744320>

167 Mike Ananny, "The Curious Connection Between Apps for Gay Men and Sex Offenders" *The Atlantic* (14 April 2011) <https://www.theatlantic.com/technology/archive/2011/04/the-curious-connection-between-apps-for-gay-men-and-sex-offenders/237340/>

168 Bruno Lepri et al. (2017), "Fair transparent and accountable algorithmic decision-making processes" *Philosophy & Technology* <http://www.nuriaoliver.com/papers/Philosophy_and_Technology_final.pdf> at page 5.

169 Aaron Shapiro, "Reform predictive policing," *Nature* (25 January 2017) <https://www.nature.com/news/reform-predictive-policing-1.21338>. See also David Robinson, and Logan Koepke, "Stuck in a Pattern: Early evidence on "predictive policing" and civil rights" *Upturn* (August 2016) <https://www.teamupturn.org/reports/2016/stuck-in-a-pattern/>

170 Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, "How We Analyzed the COMPAS Recidivism Algorithm" *ProPublica* (23 May 2016) <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>. See also Rachel Courtland, "Bias detectives: the researchers striving to make algorithms fair" *Nature* (20 June 2018) <https://www.nature.com/articles/d41586-018-05469-3>; Anthony W. Flores, Christopher T. Lowenkamp, and Kristin Bechtel (2017), "False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks."" <http://www.crj.org/assets/2017/07/9_Machine_bias_rejoinder.pdf>; and Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan (2016), "Inherent Trade-Offs in the Fair Determination of Risk Scores" <https://arxiv.org/abs/1609.05807>.

171 *State v Loomis*, 2016 WI 68 <https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html>.

Algorithmic Bias and Discrimination in Immigration Decisions

The opaque nature of immigration and refugee decision-making creates an environment ripe for algorithmic discrimination. Decisions in this system—from whether a refugee's life story is "truthful" to whether a prospective immigrant's marriage is "genuine"—are highly discretionary, and often hinge on an individual officer's assessment of credibility.[172] To the extent that these technologies will be used to assess "red flags," "risk," and "fraud," they also raise definitional issues, as it remains unclear what the parameters of these markers will be. In a 2017 email to the *Toronto Star*, an IRCC spokesperson wrote that "Predictive analytics models are built by analyzing thousands of past applications and their outcomes. This allows the computer to 'learn' by detecting patterns in the data, in a manner analogous to how officers learn through the experience of processing applications."[173]

Given the already limited safeguards and procedural justice protections in immigration and refugee decisions, the use of discriminatory and biased algorithms have profound ramifications on a person's safety, life, liberty, security, and mobility.

However, this does not respond to the concern that existing biases may colour the data used to teach the automated system, nor does it solve issues arising from using past decisions as a training basis for future cases.[174] For example, section 109.1 of the IRPA, which determines which countries should be placed on the Designated Countries of Origin (DCO) list, already contains a crude predictive algorithm to assess whether a country is "safe" based on past grant rates of refugee status. The overarching provision includes "countries that do not normally produce refugees and respect human rights and offer state protection."[175] The DCO list has been widely criticized as discriminatory and based on an incomplete definition of "safety" which does not take into consideration intersecting vulnerabilities and identities which may render a country unsafe for certain groups, such as women fleeing domestic violence or members of the LGBTQ+ community.[176] In 2015,

---

172 See for example, Vic Satzewich, *Points of Entry: How Canada's Immigration Officers Decide Who Gets In* (Vancouver: UBC Press, 2015); Vic Satzewich (2014), "Canadian Visa Officers and the Social Construction of "Real" Spousal Relationships," *Canadian Review of Sociology* 51:1 <https://doi.org/10.1111/cars.12031>.

173 Nicholas Keung, "Canadian immigration applications could soon be assessed by computers," *Toronto Star* (5 January 2017) <https://www.thestar.com/news/immigration/2017/01/05/immigration-applications-could-soon-be-assessed-by-computers.html>.

174 Taylor Owen, "The Violence of Algorithms: Why Big Data Is Only as Smart as Those Who Generate It," *Foreign Affairs* (25 May 2015) <https://www.foreignaffairs.com/articles/2015-05-25/violence-algorithms>

175 The Government of Canada, "Designated countries of origin policy," (last modified 3 April 2017) <https://www.canada.ca/en/immigration-refugees-citizenship/services/refugees/claim-protection-inside-canada/apply/designated-countries-policy.html>

176 See, for example Petra Molnar (2014), "The "Bogus" Refugee: Roma Asylum Claimants and Discourses of Fraud in Canada's Bill C-31" *Refugee* 30:1 <https://refuge.journals.yorku.ca/index.php/refuge/article/view/38604>; and The United Nations Human Rights Office of the High Commissioner, "Concluding observations on the sixth periodic report of Canada" CCPR/C/CAN/CO/6 (13 August 2015) <https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FCAN%2FCO%2F6&Lang=en>

the Federal Court of Canada also found that denying refugee claimants from DCOs the right of appeal was unconstitutional.[177] Given the already limited safeguards and procedural justice protections in immigration and refugee decisions, the use of discriminatory and biased algorithms have profound ramifications on a person's safety, life, liberty, security, and mobility.

The complexity of human migration is not easily reducible to an algorithm and there is no external metric for accuracy with respect to refugee and status determinations.

'Extreme Vetting' or Extreme Bias?

The United States offers a stark example of how algorithms can be used to discriminate in immigration decision-making. In 2017, Immigration and Customs Enforcement (ICE) unveiled plans to create "Extreme Vetting Initiatives" to predict the potential criminality of those who enter the country.[178] This software is meant to "[automate], [centralize], and [streamline] the manual vetting process," automatically determine the probability that an applicant would be a "positively contributing member of society" and to national interests, and predict whether they intend to commit criminal or terrorist acts after entering the country.[179] These criteria are taken directly from the Trump Administration's January 2017 Executive Order[180] (the first so-called "Muslim ban"[181]), barring travel from seven predominantly Muslim countries into the United States.[182] The Extreme Vetting Initiative will use government agency and law enforcement databases, and collect data from public information online found on social media websites. All this information will then be analyzed continuously for vetting travelers during their time in the US.[183]

The proposed Extreme Vetting Initiatives are comparable to predictive policing software already widely in use in the United States, in which algorithms determine an individual's propensity to commit a crime, or whether a crime is likely to occur in a specific area, based on past trends and data.[184] Critiques of predictive policing assert that it is unfair and inefficient because it depends on past data about previously reported crimes and not the amount of current crimes, and because it conflates reported crime rates with actual crime rates, as

---

177 Y.*Z and the Canadian Association of Refugee Lawyers* IMM-3700-13 2015 FC 892. See also Nicholas Keung, "Court rules denial of appeals for 'safe country' refugees unconstitutional," *The Toronto Star* (23 July 2015) <https://www.thestar.com/news/immigration/2015/07/23/court-strikes-down-ottawas-safe-country-list-for-refugees.html>

178 April Glaser, "ICE Wants to Use Predictive Policing Technology for Its "Extreme Vetting" Program," *Slate* (8 August 2017) <http://www.slate.com/blogs/future_tense/2017/08/08/ice_wants_to_use_predictive_policing_tech_for_extreme_vetting.html>

179 Ibid.

180 Executive Order 13769, titled Protecting the Nation from Foreign Terrorist Entry into the United States, Signed January 27, 2017, 82 FR 8977 <https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states/>

181 Brian Root, "US Immigration Officials Pull Plug on High-Tech 'Extreme Vetting'," *Human Rights Watch* (18 May 2018) <https://www.hrw.org/news/2018/05/18/us-immigration-officials-pull-plug-high-tech-extreme-vetting>.

182 Note that after multiple constitutional challenges, the Supreme Court of the United States upheld the travel ban in a 5-4 decision on June 26, 2018: http://cdn.cnn.com/cnn/2018/images/06/26/travel.ban.pdf.

183 April Glaser, "ICE Wants to Use Predictive Policing Technology for Its "Extreme Vetting" Program," *Slate* (8 August 2017) <http://www.slate.com/blogs/future_tense/2017/08/08/ice_wants_to_use_predictive_policing_tech_for_extreme_vetting.html>

184 Logan Koepke, "Predictive Policing Isn't About the Future," *Slate* (21 November 2016) <http://www.slate.com/articles/technology/future_tense/2016/11/predictive_policing_is_too_dependent_on_historical_data.html>

various factors influence which crimes are reported.[185] Automated systems that incorporate and use these statistics also may not account for inaccuracies found within them, creating a self-fulfilling feedback loop. Civil rights organizations, such as the American Civil Liberties Union and the National Association for the Advancement of Colored People (NAACP), argue that these results are often racially-biased.[186] Despite these controversies, predictive software is now used by least 20 of the 50 largest police departments in the United States.[187]

The Extreme Vetting Initiative's databases can contain biased information, including instances where the FBI opened a file on a man who was deemed suspicious because he seemed like he "practiced Islam and was looking at his computer" or a known photographer who was placed on a federal terrorist database and interrogated "because he was taking pictures of public art."[188] The heavy monitoring and use of social media sites is also contentious, as the information can often be misleading to a non-human analyst.[189] Like with predictive policing, the system risks hiding biased, politicized, and discriminatory decision-making behind the "scientific objectivity" of algorithms and machine learning.[190] Furthermore, once applicants or visa holders know they are being monitored, a chilling effect could occur on their freedom of speech, forcing them to censor themselves online to avoid attracting scrutiny,[191] as well curtail their freedom of association and religion by limiting their time in places of worship.

In May 2018, ICE stated that due to pushback, they were dropping their plan to monitor the social media activity of visa applicants within the Extreme Vetting Initiative.[192] Likewise, ICE has conceded that no software currently exists that can make these predictions, and that this software would make predictions capable of violating civil and human rights and introduce discriminatory and arbitrary criteria into the immigration vetting process.[193] Instead, ICE now emphasizes human oversight of the vetting process and are funding the training of visa screeners and the hiring of analysts to expand vetting procedures using current technological capabilities.[194] However, concerns remain that ICE continues to use discriminatory criteria from the Executive Order in manually screening applicants.[195] In June 2018, ICE was also heavily criticized for its use of a "risk

185 Ibid.

186 April Glaser, "ICE Wants to Use Predictive Policing Technology for Its "Extreme Vetting" Program," *Slate* (8 August 2017) <http://www.slate.com/blogs/future_tense/2017/08/08/ice_wants_to_use_predictive_policing_tech_for_extreme_vetting.html>

187 Ibid.

188 Ibid.

189 Jake Laperruque, "ICE Backs Down on "Extreme Vetting" Automated Social Media Scanning," *Project on Government Oversight* (23 May 2018) <http://www.pogo.org/blog/2018/05/ice-backs-down-on-extreme-vetting-automated-social-media-scanning.html>

190 Brian Root, "US Immigration Officials Pull Plug on High-Tech 'Extreme Vetting'," *Human Rights Watch* (18 May 2018) <https://www.hrw.org/news/2018/05/18/us-immigration-officials-pull-plug-high-tech-extreme-vetting>

191 Ibid.

192 Ibid.

193 Natasha Duarte, "ICE Finds Out It Can't Automate Immigration Vetting. Now What?," *CDT* (22 May 2018) <https://cdt.org/blog/ice-cant-automate-immigration-vetting/>

194 Ibid.

195 Brian Root, "US Immigration Officials Pull Plug on High-Tech 'Extreme Vetting'," *Human Rights Watch* (18 May 2018) <https://www.hrw.org/news/2018/05/18/us-immigration-officials-pull-plug-high-tech-extreme-vetting>.

classification system" that recommended the detention of migrants in every case to comply with the hardline policies of the Trump administration on the US-Mexico border.[196]

The United States is not alone in the use of these vetting initiatives. While the EU champions stronger rights protections when governments use predictive analysis, a 2017 directive also authorized the use of predictive policing mechanisms in order to combat terrorism.[197] The directive followed a voluntary code of conduct that was signed by major IT companies such as Microsoft, Youtube, and Twitter in 2015 that obliged companies to review and flag content that constitutes hate speech and incitement of violence.[198] The predictive policing data is monitored and used by the the European Union Agency for Law Enforcement Cooperation (Europol), a law enforcement agency of the EU, to conduct real-time data correlations.[199] This type of monitoring is still permitted under the new GDPR so long as it continues to fit in the clear exemption for foreign and security matters as defined in article 2.2(d), and clause 16 of the preamble.[200]

Using biometric recognition software in immigration decisions also presents an opportunity to entrench discrimination by flagging certain features as high risk or as worthy of further scrutiny. For example, Australia is also exploring the uses of biometrics and facial recognition both in airports and within passenger databases.[201] Airport passengers would be processed by biometric recognition of their faces, irises, and/or fingerprints instead of showing their passports.[202] The Australian government has also begun enacting legislation designed to implement and normalize the use of facial biometric data for surveillance purposes in law enforcement and national security.[203] In late May 2018, the Human Rights Law Center made a submission to the enquiry into Australia's proposed national facial recognition regime, specifically stating the country's legal system was not yet able to handle it responsibly, and noting that the technology itself was not reliable.[204]

---

196 Shane Ferro, "ICE's Bond Algorithm has one response: Detain," *Above The Law*, 27 June 2018, <https://abovethelaw.com/2018/06/ices-bond-algorithm-has-one-response-detain/>

197 Directive 2017/541 of the European Parliament and of the Council <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017L0541>.

198 Staffan Dahllof et. al., News Release, "EU states copy Israel's 'predictive policing,'" *Eu Observer* (6 October 2017) <https://euobserver.com/justice/139277>.

199 Ibid.

200 Article 2(2)(d) and Recital 16, General Data Protection Regulation (GDPR) (EU) 2016/679 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>.

201 Elle Hunt, "Facial Recognition to Replace Passports in Security Overhaul at Australian Airports," *The Guardian* (22 January 2017) <https://www.theguardian.com/australia-news/2017/jan/22/facial-recognition-to-replace-passports-in-security-overhaul-at-australian-airports>

202 Ibid.

203 Asha McLean, "Australian National Security COAG Says Yes to Facial Biometric Database" *ZDNet* (5 October 2017) <https://www.zdnet.com/article/australian-national-security-coag-says-yes-to-facial-biometric-database/>. Prime Minister Turnbull claimed that adding driver licenses to the federal government's database of passport photos and immigration information will allow law enforcement authorities to more quickly identify persons suspected of terrorism.

204 Human Rights Law Centre, "The Dangers of Unregulated Biometrics Use: Submission to the Inquiry into the Identity-Matching Services Bill 2018 and the Australian Passports Amendment (Identity-Matching Services) Bill 2018," (29 May 2018) <https://static1.squarespace.com/static/580025f66b8f5b2dabbe4291/t/5b0cebb66d2a73781c59100f/1527574029901/Human+Rights+Law+Centre+Submission+to+PJCIS+-+Identity-Matching+Services.pdf>.

As these examples highlight, Canada's push towards the use of new technologies must accord with basic principles of equality, otherwise it risks entrenching direct and indirect discrimination with far-reaching impacts on people's lives.

Freedom of Association, Religion, and Expression

Discriminatory practices entrenched in the use of machine learning in immigration decisions can also affect individuals' freedom of association, religion, and expression.

Freedom of association is broadly interpreted in international law and includes the right to peaceful assembly and association with others. It is enshrined in Article 22 of the *ICCPR*.[205] It is protected by section 2(c) of the Canadian *Charter*. In order for association to be considered free, it must not be impeded by government interference. However, the risk of being linked with certain groups that are more likely to be incorrectly flagged by an automated system in Canada's immigration system for further screening or as "high risk" may create a chilling effect on people's willingness to freely associate with others. This will be particularly acute in the digital space if online records of behaviour may be used to inform the systems that will decide individuals' status and ability to enter and remain in Canada.

Similar chilling effects may occur on people's ability to exercise their freedom of expression, another fundamental human right. Article 19 of ICCPR[206] protect people's right to hold opinions without interference, as well as the freedom to seek and receive information and ideas of all kinds, including oral, written, print, through art, and any other media, including digital. Freedom of expression is also one of the fundamental rights protected by section 2(b) of the Canadian *Charter*, a right integral to a free and democratic society.[207] Speaking freely on topics that may be flagged by an algorithm may result in people not exercising their freedom of expression and engage in self-censorship for fear of being associated with unwelcome groups.

Freedom of religion may also be impacted when algorithms augment or replace decisions in Canada's immigration and refugee system. Freedom of thought, conscience, and religion is widely protected in international law, particularly by Article 18 of the ICCPR[208] and the specialised UN High Commissioner for Human Rights *Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on*

---

205 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 at Article 22 <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>. This right is also protected by Article 20 of the Universal Declaration of Human Rights and Article 22 of the American Declaration of the Rights and Duties of Man. UN General Assembly, *The Universal Declaration of Human Rights*, 10 December 1948 at Article 20 <http://www.un.org/en/universal-declaration-human-rights/>; Ninth International Conference of American States, *The American Declaration of the Rights and Duties of Man*, April 1948 at Article 22 <https://www.cidh.oas.org/Basicos/English/Basic2.american%20Declaration.htm>.

206 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 at Article 19 <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>; see also UN General Assembly, *The Universal Declaration of Human Rights*, 10 December 1948 at Article 19 <http://www.un.org/en/universal-declaration-human-rights/>.

207 See also *Edmonton Journal v Alberta* (AG), [1989] 2 SCR 1326 at 1336.

208 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 at Article 18 <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>; See also UN General Assembly, *The Universal Declaration of Human Rights*, 10 December 1948 at Article 18 <http://www.un.org/en/universal-declaration-human-rights/> and Ninth International Conference of American States, *The American Declaration of the Rights and Duties of Man*, April 1948 at Article 3 <https://www.cidh.oas.org/Basicos/English/Basic2.american%20Declaration.htm>.

Religion or Belief,[209] as well as section 2(a) of the *Charter*. These rights include the ability to worship alone or in a community with others, as well as the ability to manifest religious practices through worship, observance, practice, or teaching. If state practices, such as the use of algorithms to flag certain cases, are discriminating against certain groups, such as Muslims, they are limiting the ability of individuals and communities to freely associate and practice their religion or beliefs. The exercise of these fundamental human rights cannot be impeded by technological innovation that disproportionately targets certain groups over others.

Freedom of Movement and Mobility Rights

Automated decision systems used in the immigration and refugee context can impact people's ability to exercise their freedom of movement, right to travel, and mobility rights. These rights are enshrined in Article 12 of the *ICCPR*,[210] as well as well as the *Refugee Convention* and section 6 of the *Charter*,[211] and Article 10(2) of the *CRC*, which proscribes family separation.[212] They include the ability to enter and leave a country, as well as an individual's decision where to reside and work within the country.

If automated systems generate opaque triage systems or flag certain cases for early deportation, these decisions can prevent individuals from obtaining a valid visa to remain in a country, or exercise their rights of appeal if they have received a negative decision on their previous immigration and refugee applications. For example, in 2017, Immigration New Zealand began employing a system which uses the age, gender, and ethnicity of migrants to identify "likely troublemakers."[213] This data-based racial profiling aims to identify groups that are most prone to generating high hospital costs or are most likely to commit crime, so that the agency can move faster to deport applicants rather than allow them to re-apply for visas.[214] Civil society groups have argued that the use of such identifiers in determining access to resources or opportunity is a breach of the *New Zealand Human Rights Act*, and asserted that the program is reductive and discriminatory, based on automated profiling rather than relevant and contextualized facts about the applicant's background.[215] Immigration New Zealand claimed the program was only a pilot project that had been operating for 18 months and did not involve racial profiling but instead considered a larger range of data.[216]

---

209 United Nations General Assembly, *Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief*, 25 November 1981 <https://www.ohchr.org/en/professionalinterest/pages/religionorbelief.aspx>.

210 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 at Article 12 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>. See also UN General Assembly, T*he Universal Declaration of Human Rights*, 10 December 1948 at Article 13 <http://www.un.org/en/universal-declaration-human-rights/>.

211 Mollie Dunsmuir, and Kristen Douglas, "Mobility Rights and the Charter of Rights and Freedoms" (19 August 1998) <http://publications.gc.ca/Collection-R/LoPBdP/CIR/904-e.htm>

212 UN General Assembly, *The Convention on the Rights of the Child*, 20 November 1989 <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx> at Article 10(2).

213 Lincoln Tan, "Immigration NZ's Data Profiling "Illegal" Critics Say," NZ Herald (5 April 2018) <https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12026585>

214 Ibid.

215 Ibid.

216 Ibid.

Discriminatory and decontextualized use of predictive data can exacerbate social division and future outcomes for newly arrived populations. More data is not always better, particularly in the highly complex and sensitive area of refugee resettlement.

Some countries, particularly in the Persian Gulf, also require an exit visa before an individual is allowed to leave. Countries such as Saudi Arabia and the United Arab Emirates require such visas under the *kafala* system,[217] particularly for foreign workers, to secure clearance that all obligations to an employer have been fulfilled before the worker is allowed to leave. An exit visa can be withheld, sometimes indefinitely, if there are any pending charges or penalties. The system has been widely criticized for being discriminatory and exploitative for tying foreign workers to their employers, with wide ranging protests in Beirut, Lebanon in the summer of 2018.[218] Using algorithms to determine and justify who should or should not be granted an exit visa could contravene basic freedom of movement and mobility rights.

However, machine learning and predictive analysis may also have positive effects in predicting the movement of large scale populations in ongoing conflicts which produce large numbers of refugees.[219] For example, allowing neighbouring countries to prepare services and muster resources could aid in integration and social cohesion efforts, and increase the ability of the international community to provide effective and efficient humanitarian assistance and long-term resettlement of refugees. Currently, Stanford's Immigration Policy Lab is using an algorithm to analyze historical data of refugee resettlement in the United States and Switzerland.[220] Their algorithm can predict where certain refugees are more likely to be successful based on a combination of individual characteristics such as education, background skills, and knowledge of English. The Lab found that if the algorithm had selected the resettlement locations for refugees, the average employment rate would have been about 41% and 73% higher than their current rates in the United States and Switzerland, respectively.[221] However, this use of automated systems can also reinforce and exacerbate inequalities by placing those individuals with the least prospect of success into under-resourced areas, perpetuating cycles of poverty and potentially justifying negative attitudes towards refugee integration. Discriminatory and decontextualized use of predictive data can exacerbate social division and future outcomes for newly arrived

217 "Qatar: Implementation Will Be Key for Labor Reforms" *Human Rights Watch* (27 October 2017) <https://www.hrw.org/news/2017/10/27/qatar-implementation-will-be-key-labor-reforms>

218 Aman Madan, "The Kafala System is How Capitalism Is Driving Modern Slavery," *The Wire* (23 June 2018) <https://thewire.in/labour/understand-the-kafala-system-or-how-capitalism-is-driving-modern-slavery>; "Hundreds protest Lebanon domestic worker laws," *The Daily Star Lebanon* (24 June 2018) <http://www.dailystar.com.lb/News/Lebanon-News/2018/Jun-24/454199-hundreds-protest-lebanon-domestic-worker-laws.ashx>

219 Anirudh V. S. Ruhil, "Millions of refugees could benefit from big data – but we're not using it," *The Conversation* (29 January 2018) <https://theconversation.com/millions-of-refugees-could-benefit-from-big-data-but-were-not-using-it-86286>

220 Alex Shashkevich, "Stanford scholars develop new algorithm to help resettle refugees and improve their integration," *Stanford News* (18 January 2018) <https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/>.

221 Alex Shashkevich, "Stanford scholars develop new algorithm to help resettle refugees and improve their integration," *Stanford News* (18 January 2018) <https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/>.

populations. More data is not always better, particularly in the highly complex and sensitive area of refugee resettlement.

Privacy Rights and Data Protection

Privacy is not simply a consumer or property interest: it is a human right, rooted in foundational democratic principles of dignity and autonomy.[222] The right to privacy is recognized internationally under Article 17 of the ICCPR.[223] Recently, the United Nations has also explicitly recognized the impact of digital technologies on the right to privacy.[224] In 2013 and 2014, the High Commissioner for Human Rights issued statements on the risk surveillance poses to individuals' rights, particularly privacy and freedom of expression and association.[225] The General Assembly also adopted Resolution 68/167, which expressed concerns regarding the potential negative impacts that surveillance may have on international human rights.[226] With the adoption of this Resolution, the General Assembly also requested that the High Commissioner for Human Rights prepare a report on the right to privacy in the digital age, and Canada was one of the states which shared information about its own policies.[227] In 2015, the Human Rights Council adopted Resolution 28/16, which saw the appointment of a Special Rapporteur on the right to privacy.[228] In 2016, the United Nations Committee on Social, Humanitarian and Cultural Issues adopted a new resolution on the right to privacy in the digital age, which recognizes the importance of respecting pre-existing international commitments regarding privacy rights and calls on states to develop appropriate remedies.[229] It emphasizes that states must address legitimate concerns regarding their national security in a manner that is consistent with these obligations and that personal data is increasingly susceptible to being sold without the individuals' consent or knowledge. The resolution also highlights the increased vulnerability of women, children, and marginalized communities

---

222 Lisa Austin, "We must not treat data like a natural resource," *The Globe and Mail* (9 July 2018) <https://www.theglobeandmail.com/opinion/article-we-must-not-treat-data-like-a-natural-resource/>.

223 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 at Article 17 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> See also UN General Assembly, *The Universal Declaration of Human Rights*, 10 December 1948 at Article 12 <http://www.un.org/en/universal-declaration-human-rights/>.

224 United Nations Human Rights Office of the High Commissioner, "The Right to Privacy in the Digital Age": https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx

225 United Nations Human Rights Office of the High Commissioner, "Opening Remarks by Ms. Navi Pillay, United Nations High Commissioner for Human Rights to the Side-event at the 24th session of the UN Human Rights Council How to safeguard the right to privacy in the digital age?" (20 September 2013) <https://newsarchive.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13758&LangID=E>; and United Nations Human Rights Office of the High Commissioner, "Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age" (24 February 2014) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E>.

226 United Nations General Assembly, "Resolution adopted by the General Assembly on 18 December 2013: 68/167, The right to privacy in the digital age" (21 January 2014) <http://undocs.org/A/RES/68/167>.

227 United Nations Human Rights Office of the High Commissioner, "Contributions from stakeholders: Right to privacy in the digital age" (22 April 2014) <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/Contributions.aspx#states>.

228 United Nations Human Rights Office of the High Commissioner, "Special Rapporteur on the right to privacy" <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.

229 United Nations General Assembly, "The right to privacy in the digital age" (16 November 2016) <http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1>. See also Deborah Brown, "New UN resolution on the right to privacy in the digital age: crucial and timely," Internet Policy Review (22 November 2016) <https://policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436>.

to these privacy right violations, and links the right to privacy with other human rights such as freedom of expression.[230]

Under the Canadian *Charter*, privacy is primarily safeguarded under section 8: the right to be free from unreasonable search and seizure.[231] The right to privacy is also intimately connected to freedom of expression, opinion, and belief, enshrined in section 2(b) of the *Charter*: a lack of privacy or the perception that one is being watched has a chilling effect on freedom of speech (a phenomenon which may be more acute for voices which are already marginalized or vulnerable).[232] Privacy also safeguards the "liberty" and "security of the person" interests protected under section 7. In an era of mass digital communication (and mass digital surveillance), the right to privacy has taken on a far-reaching new importance.[233] In addition to the *Charter*, certain Canadian privacy and data protection statutes (i.e., the *Privacy Act*) are now recognized as having a quasi-constitutional dimension.[234]

Automated decision systems have the potential to impact privacy rights in a number of different ways. First, these technologies almost inherently require the mass accumulation of data for the purpose of both training and analysis. This data must be collected in a manner which is lawful and should only be done where its collection is both necessary and proportionate.[235] As discussed earlier in this report, when national security databases and other infrastructures of surveillance interface with automated decision systems, serious human rights concerns may arise. In some cases, these sources of information will have been collected in a legally problematic manner, and may not be subject to the same legal frameworks as other data collected by government. Electronic surveillance practices also disproportionately target, and have disproportionate consequences for, marginalized and vulnerable groups. For example, in the EU, metadata associated with refugees' mobile phones is being used to track and deport them.[236] Individuals who choose not to participate in activities such as the use of digital devices or social media—whether due to privacy concerns or simply as a matter of preference—may also be subject to prejudicial inferences.[237]

Machine learning and artificial intelligence technologies can be used to identify patterns that human analysts would otherwise not recognize. Yet those patterns and correlations may reveal intimate information about individuals, networks, and communities—some of which may be proxies for grounds protected by law, such as race or gender. It is therefore essential to note that individuals may not only have a privacy interest in training

230 Ibid.

231 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c11, s. 8.

232 Jon Penney (2017), "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study, Internet Policy Review" <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959611>.

233 United Nations General Assembly, "Resolution adopted by the General Assembly on 18 December 2013: 68/167, The right to privacy in the digital age" (21 January 2014) <http://undocs.org/A/RES/68/167>.

234 *Lavigne v. Canada* (Office of the Commissioner of Official Languages), 2002 SCC 53; *HJ Heinz v Canada* (Attorney General), 2006 SCC 13.

235 Necessary and Proportionate Coalition (2014), "International Principles on the Application of Human Rights to Communications Surveillance" (launched July 2013, final version May 2014) <https://necessaryandproportionate.org/principles>.

236 Morgan Meaker, "Europe is using smartphone data as a weapon to deport refugees," *Wired* (2 July 2018) <http://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations>.

237 James Vertesi, "My Experiment Opting Out of Big Data Made Me Look Like a Criminal," *Time* (1 May 2014) <http://time.com/83200/privacy-internet-big-data-opt-out/>

data or inputs to an automated decision system, but also in its findings, judgments, and outputs. Automated decision systems may also impact the rights protected under section 8 of the *Charter* where outputs of those systems form the basis of "reasonable suspicion" or "reasonable belief" in order to justify a search or other privacy intrusion. As the Supreme Court wrote in *R v. Chehil*, "The elements considered as part of the reasonable suspicion analysis must respect *Charter* principles. The factors considered ... must relate to the actions of the subject of an investigation, and not his or her immutable characteristics."[238]

In most circumstances, when government decision systems use personal information, they must comply with the *Privacy Act* (and private sector vendors contracting with government will also need to comply with its private sector counterpart, *the Personal Information Protection and Electronic Documents Act*). The adoption of automated decision systems will also require substantial updates to Privacy Impact Assessments required by the federal government in virtually all circumstances where a program or service raises privacy issues.[239]

Beyond seeking to protect the confidentiality of personal information, the *Privacy Act* also includes other data protection obligations, including both the limitation that data collected needs to be linked to its objective, as well as obligations relating to accuracy.[240] The accuracy obligation may have implications both for the quality of input data (for example, the Office of the Privacy Commissioner has raised concerns about the use of social media information by CBSA in its SBT operations due to "questionable accuracy and reliability"[241]) as well as implications for the accuracy of algorithmic technologies themselves. For example, while the 2018 Supreme Court decision *Ewert v. Canada (AG)* concerns the interpretation of section 24(1) of the *Corrections and Conditional Release Act*, the provision in question closely resembles the obligation in section 6(2) of the *Privacy Act*, which prescribes that government institutions "shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible."[242] In *Ewert*, the majority found that the Correctional Service of Canada (CSC) failed to take all reasonable steps to ensure that the impugned psychological assessment tools were accurate and scientifically validated. There were furthermore particular concerns with accuracy when applied to Indigenous offenders specifically.[243] This was despite the fact that "the CSC had long been aware of concerns regarding the possibility of psychological and actuarial tools exhibiting cultural bias."[244]

---

238 R v Chehil, 2013 SCC 49 at paragraph 43.

239 Treasury Board of Canada Secretariat, "Responsible Artificial Intelligence in the Government of Canada," *Digital Disruption White Paper Series* (10 April 2018) at page 27 <https://docs.google.com/document/d/1Sn-qBZUXEUG4dVk909eSg5qvfbpNlRhzIefWPtBwbxY/edit>. See also Office of the Privacy Commissioner of Canada, "Privacy Impact Assessments" (last modified 2 March 2018) <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments>.

240 See, for example s. 6(1), *Privacy Act*, R.S.C. 1985, c. P-21.

241 Office of the Privacy Commissioner of Canada, "Canada Border Services Agency – Scenario Based Targeting of Travelers – National Security" (21 September 2017) <https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_cbsa_2017/>.

242 s. 24(1), *Corrections and Conditional Release Act*, S.C. 1992, c. 20; and s. 6(2), *Privacy Act*, R.S.C. 1985, c. P-21.

243 Ewert v Canada (AG), 2018 SCC 30 at paragraph 46.

244 Ewert v Canada (AG), 2018 SCC 30 at paragraph 49.

Vulnerable groups, including refugees, face unique privacy risks, as information about them can be weaponized by repressive governments in their countries of origin. If conducted in an irresponsible manner, information sharing can put individuals and their families at grave personal risk.

There is also an international context to Canada's use and collection of personal information. For example, the European General Data Protection Regulation (GDPR) is applicable to any company or government that may have access to the files of an EU citizen, meaning Canada may have greater obligations with respect to processing the data and applications of migrants and refugees from EU countries, as opposed to those arriving from elsewhere. Canada is also engaged in a number of arrangements involving international information sharing with foreign partners. Vulnerable groups, including refugees, face unique privacy risks, as information about them can be weaponized by repressive governments in their countries of origin. If conducted in an irresponsible manner, information sharing can put individuals and their families at grave personal risk.[245]

Private sector products designed to support individuals interfacing with the immigration and refugee system may also create new privacy risks. For example, Visabot is a Facebook Messenger-based artificial intelligence application designed to help users apply for visas and green cards, and schedule appointments with the United States Citizenship and Immigration Service (USCIS).[246] Visabot has also launched a service to specifically assist young immigrants who qualify for the Deferred Action for Childhood Arrivals program (DACA).[247] Although this program is designed to help at-risk migrants and potential immigrants, there is a significant privacy and security tradeoff inherent to using Facebook's technology as a platform. This is because Facebook, and other companies like it, operate within business models that primarily rely on the aggregation, analysis, and resale of their users' private information to third parties (such as advertisers).

245 The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, "Report of the Events Relating to Maher Arar: Factual Background, Volume I" (2006) <http://www.sirc-csars.gc.ca/pdfs/cm_arar_bgv1-eng.pdf>.

246 David Lumb, "Immigration Chat Bot Now Helps You Apply for a Green Card," *Engadget* (11 July 2017) <https://www.engadget.com/2017/07/11/immigration-chat-bot-now-helps-you-apply-for-a-green-card>

247 Khari Johnson, "Visabot Helps You Cut Green-Card Red Tape," *VentureBeat* (11 July 2017) <https://venturebeat.com/2017/07/11/visabot-helps-you-cut-green-card-red-tape/>

Life, Liberty, and Security of the Person

Article 9 of the *ICCPR*[248] recognizes the rights to life and security of the person. The *Refugee Convention*[249] enshrines the right to seek protection from persecution when life, liberty and security is threatened, including the right not to be returned to a country where persecution and risk to life is likely, under the principle of *nonrefoulement*. Numerous other specific legal instruments, such as the *Convention Against Torture and Other Cruel, Inhumane or Degrading Treatment or Punishment (CAT)*,[250] *CRPD*,[251] CEDAW,[252] CRC,[253] and CERD[254] all protect the right to liberty and security for all persons. This includes vulnerable groups who must be treated equally when exercising their rights. These provisions protect against arbitrariness in arrest and detention, and affirm principles of legality, due process, and the rule of law. Section 7 of the *Charter* protects the rights to life, liberty, and security of the person, as well as the right not to be deprived thereof except in accordance with the principles of fundamental justice.[255] These rights are engaged in various ways throughout Canada's immigration and refugee system. The "liberty" interest is engaged in detention-related cases,[256] as well as in some cases of deportation.[257] In cases where an individual faces the psychological threat of deportation to a country where they face a substantial risk of torture (and the threat of that torture itself), the "security of the person" interest is also engaged.[258]

"Principles of fundamental justice" include core legal principles of natural justice and the guarantee of procedural fairness, "having regard to the circumstances and consequences of the intrusion on life, liberty or security."[259] In particular, they include three key principles, respectively guarding against arbitrariness, overbreadth, and gross disproportionality.[260] Where a deprivation of a right bears no connection to the actual

---

248 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 at Article 9 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>. See also UN General Assembly, *The Universal Declaration of Human Rights*, 10 December 1948 at Article 3 <http://www.un.org/en/universal-declaration-human-rights/>.

249 *Convention relating to the Status of Refugees*, 189 U.N.T.S. 150, entered into force April 22, 1954, ratified by Canada on 4 June 1969

250 UN General Assembly, *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, 10 December 1984 <https://www.ohchr.org/en/professionalinterest/pages/cat.aspx>.

251 United Nations Department of Economic and Social Affairs Division for Inclusive Social Development, *Convention on the Rights of Persons with Disabilities* at Article 14 <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-14-liberty-and-security-of-person.html>.

252 United Nations Entity for Gender Equality and the Empowerment of Women, *Convention on the Elimination of All Forms of Discrimination against Women* <http://www.un.org/womenwatch/daw/cedaw/text/econvention.htm>.

253 UN General Assembly, *The Convention on the Rights of the Child*, 20 November 1989 <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>.

254 UN General Assembly, *International Convention on the Elimination of All Forms of Racial Discrimination*, 21 December 1965 at Article 5(b), for example <https://www.ohchr.org/en/professionalinterest/pages/cerd.aspx>.

255 *Canadian Charter of Rights and Freedoms*, s. 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c11, s. 7.

256 *Chaudhary v Canada (Public Safety and Emergency Preparedness)*, 2015 ONCA 700.

257 *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1.

258 Ibid.

259 *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9 at paragraph 19.

260 *Canada (Attorney General) v. Bedford*, 2013 SCC 72 at paragraph 35.

purpose of a law, it is considered "arbitrary" and in breach of section 7. Government acts or actions which are "overbroad" for the purposes of section 7 are those which are rational in part, but when applied have a collateral impact on conduct or individuals in a way that is unrelated to the legislative objective. Matters of "gross disproportionality" are those where the effects or outcome are so disproportionate that they are clearly out of sync with the legislative objective, even if they are rationally connected in some way.[261]

These three dimensions are relevant to evaluating the behaviour and outcomes of automated decision systems in a number of ways. Errors, miscalibrations, and deficiencies in training data can result in rights-infringing outcomes. For example, aspects of training data which are mere coincidences in reality may be treated as relevant patterns by a machine learning system, leading to outcomes which are considered arbitrary when examined against the purpose of the governing statute. This is one reason why the GDPR requires the ability to demonstrate that the correlations applied in algorithmic decision-making are legitimate justifications for the automated decisions.[262]

The 2018 Supreme Court decision *Ewert v. Canada (AG)*, which concerned the use of psychological and actuarial risk assessment tools by the CSC to evaluate a Métis man's risk of recidivism, is also relevant in this context. While the Court did not find that the use of the assessment tools amounted to a breach of section 7 in that particular case, it tentatively acknowledged that such practices could meet the test for arbitrariness and overbreadth in some circumstances.[263] In a U.S. case concerning algorithmic technologies used to evaluate school board teachers where a roughly analogous argument was made, the judge came to a similar conclusion as the Supreme Court majority in *Ewert*, but noted that the rational connection test is a "loose constitutional standard" which can allow governments "to use blunt tools which may produce only marginal results."[264] Notably, the Court in *Ewert* found that the burden to demonstrate the absence of a rational connection to the relevant government objective, and to prove that an impugned practice violates section 7, remains on the applicant—potentially raising some of the access to justice concerns discussed later in this report, in the case of immigrants and refugees.[265]

Principles of fundamental justice also include procedural principles which vary depending on the particular context at stake. The more serious the infringement of the right, the more extensive and rigorous the procedural requirements will be.[266] The right to a hearing before an independent and impartial tribunal,[267]

---

261 Ibid.

262 Lokke Moerel, and Marijn Storm, "Law and Autonomous Systems Series: Automated Decisions Based on Profiling - Information, Explanation or Justification? That is the Question!," *University of Oxford Faculty of Law* (27 April 2018) <https://www.law.ox.ac.uk/business-law-blog/blog/2018/04/law-and-autonomous-systems-series-automated-decisions-based-profiling>

263 *Ewert v Canada* (AG), 2018 SCC 30.

264 *Houston Fed. of Teachers v. Houston Independent*, 251 F.Supp.3d 1168 (2017) at section 3 <https://www.leagle.com/decision/infdco20170530802>.

265 *Ewert v Canada (AG)*, 2018 SCC 30 at paragraphs 70-74.

266 *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1 at paragraph 118; *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9; *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38 at paragraph 25.

267 *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9 at paragraph 29.

the disclosure of evidence[268] and the right to test that evidence, the right to "know the case to meet,"[269] and the right to written reasons[270] are among the procedural principles of fundamental justice which have been found to apply in immigration and refugee law cases, depending on the specific context. Even where national security interests are concerned—such as in security certificate proceedings—procedures must nonetheless conform to principles of fundamental justice.[271] In the case of automated decision systems that put rights to life, liberty, or security of the person at stake, the technical capabilities of the system must be evaluated against its ability to adhere to these constitutional principles. These elements of procedural justice protected under section 7 of the *Charter* are intimately linked to the administrative law principles discussed in greater detail below.

268 *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37.

269 *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1 at paragraphs 122-123; *Canada (Minister of Employment and Immigration) v. Chiarelli*, [1992] 1 SCR 711.

270 *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1 at paragraphs 126-127; *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817.

271 *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9.

Administrative Law Issues

"Administrative law" refers to the area of law concerned with the actions and operations of government agencies and administrative decision-makers. This area of law directly affects people's everyday lives, including decisions on issues ranging from social assistance to immigration, among others. In particular, it provides the framework for courts to engage in review of decisions made by a Minister, administrative boards, commissions, tribunals, or agencies. Administrative law principles apply to all manner of immigration and refugee law cases, which may be subject to judicial review by the Federal Court following an appeal to the Immigration Appeal Division (IAD) and the Refugee Appeal Division (RAD) of the Immigration and Refugee Board (IRB), or upon direct application for judicial review (depending on the nature of the case in question).

Courts and scholars generally divide administrative law into two areas: procedural fairness and substantive review. Procedural fairness is concerned with the nature and extent of the rights and protections available during the deliberation of a case, the content of which depends on the type of rights at stake and the circumstances of the case (but which may include the right to a hearing or written reasons, for example). Substantive review, by contrast, is concerned with evaluating the content and outcome of an administrative decision-maker's decision to determine whether it should be sent back for reconsideration. This section explores some of the challenges—both to procedural fairness and substantive review—raised by the use of automated decision systems to either support or replace the judgment of human decision-makers.

Procedural Fairness

> *"The values underlying the duty of procedural fairness relate to the principle that the individual or individuals affected should have the opportunity to present their case fully and fairly, and have decision affecting their rights, interests, or privileges made using a fair, impartial and open process, appropriate to the statutory, institutional and social context of the decisions."*
>
> *Baker v. Canada (Minister of Citizenship and Immigration),* [1999] 2 SCR 817, para 21

Procedural fairness is a central guiding principle of governmental and quasi-judicial decision-making in the Canadian immigration and refugee context. The highly discretionary nature of many administrative tribunals, including the Immigration and Refugee Board of Canada, makes procedural fairness in their decision-making processes even more crucial. This principle ensures that the person a decision impacts may exercise due rights of participation in their own case and, equally critically, ensures against arbitrary, unfair, or unaccountable decision-making in situations with significant consequences for people's lives.

Various sources of law dictate the specific content of procedural fairness that is owed to a person in a given decision-making process. These sources typically include the legislation governing the decision-maker, common law principles and precedents, and the principles of fundamental justice under section 7 of the *Charter*. In the Canadian immigration and refugee context, the Government of Canada has provided for

procedural fairness throughout the process associated with deciding each type of application. Immigration, Refugees and Citizenship Canada mandates its staff incorporate procedural fairness into the department's overall operations and service delivery,[272] while setting out explicit requirements of procedural fairness in relation to specific types of decisions, such as: determining eligibility when screening refugees for resettlement;[273] deciding to refuse a refugee application without interviewing them;[274] deciding whether to grant permanent residence to protected persons;[275] or deciding a person's citizenship.[276] These guidelines are rooted in and supplemented by procedural fairness principles as enshrined in leading Supreme Court of Canada cases such as *Baker v. Canada (Minister of Citizenship and Immigration)*[277] and *Charkaoui v. Canada (Citizenship and Immigration)*.[278]

Procedural fairness takes the form of a wide range of principles and practices, such as the right to make one's case, the right to know and respond to charges, and the right to a fair and impartial decision-maker. The degree of procedural fairness that the law requires for any given decision-making process increases or decreases with the significance of that decision and its impact on a person's rights and interests. For example, there is little to no procedural fairness attached to an officer's decision to give a driver a parking ticket, while someone accused of a serious crime is entitled to the high degree of procedural fairness that comes with a full trial. In the immigration context, requirements may range from a general obligation to ensure an applicant receives notice of a development impacting their application to mandating that officers fulfill specific tasks such as recording, retaining, and making available adequate notes for certain applications.

Certain core rights and responsibilities are particularly relevant when considering how automated decision systems, including the use of algorithms and machine learning, might impact procedural fairness in the context of immigration and refugee applications in Canada. For example, at least one U.S. court has recognized a limited due process right in the form of proper notice (and the opportunity to raise objection) where a government body adopts an automated system. In that case, an automated system was adopted by the Arkansas Department of Human Services to assign at-home attendant care hours for disabled Medicaid

---

272 Government of Canada, "Procedural fairness" (last modified 31 March 2017) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/service-delivery/procedural-fairness.html>

273 Government of Canada, "Procedural fairness and determining eligibility based on paper screening" (last modified 18 September 2017) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/refugee-protection/resettlement/eligibility/procedural-fairness-determining-eligibility-based-on-paper-screening.html>

274 Government of Canada, "Post-interview processing and final decisions: Refusing applications" (last modified 18 September 2017) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/refugee-protection/resettlement/processing-post-interview-processing-final-decisions/refusing-applications.html>

275 Government of Canada, "Protected persons – Processing applications for permanent residence – Stage 2: admissibility" (last modified 21 April 2017) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/permanent-residence/protected-persons/stage-2-admissibility.html>

276 Government of Canada, "Citizenship: Natural justice and procedural fairness" (last modified 3 July 2015) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/canadian-citizenship/admininistration/decisions/natural-justice-procedural-fairness.html>

277 *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817.

278 *Charkaoui v. Canada (Citizenship and Immigration)*, [2008] 2 SCR 326, 2008 SCC 38.

beneficiaries, resulting in reduced support for some individuals that threatened their health, quality of life, and personal dignity.[279]

This section surveys various elements of procedural fairness which are relevant to the adoption of automated decision systems, including the right to be heard; the right to a fair, impartial, and independent decision-maker; the right to reasons (also increasingly known as the right to an explanation); and the right to appeal an unfavourable decision. The following sections will briefly discuss each right and how it is implicated by automated decision systems.

Right to be Heard

The right to be heard dictates that a person should always have the ability to make their case and respond to concerns raised against them. In the immigration and refugee context, this translates into an applicant's right to respond to concerns that an immigration officer has with their application. The right to be heard is a core legal principle in administrative law and in the immigration law context in particular.[280] This principle encompasses not only the right to respond to concerns arising from the applicant's own materials, but further mandates that if a decision-maker relies on extrinsic evidence to make their determination, the person must be advised and given an opportunity to respond to this evidence.

The right to respond is implicated on two levels where algorithms play a key role in decision-making. First, decision-makers must consider how to provide for an applicant's "right to respond" to a decision that is made wholly or predominantly by an algorithm, and what it means to operationalize that right. For example, the decision-maker may have to be prepared to explain precisely how the algorithm works, what data it takes into account, how it weighs various factors, and the means by which it arrived at the decision about the applicant, such that the applicant has a meaningful opportunity to refute the decision. This becomes an even more challenging task in the event of machine learning, where the algorithm essentially teaches itself without human input, and reaches decisions in ways that may be difficult for humans to understand (at least at firm glance, or without more advanced testing).

Second, algorithms are trained on large sets of data used to calibrate and refine their outcomes. It is well-established that the quality of training data will have significant impact on the quality of outcomes, where "quality" here might be defined as outcomes that are consistently fair and accurate. This would appear to give rise to an applicant's right to respond to the data used to train the algorithms involved in immigration and refugee applications, on the notion that this data is the extrinsic evidence that the "decision-maker"—the algorithm—relies on to decide the applicant's fate.

---

279 *Bradley Ledgerwood, et al. v. Arkansas Department of Human Sevices* 60CV-17-442 <https://www.arktimes.com/media/pdf/ledgerwood_v_dhs--order.pdf>; Colin Lecher, "What Happens When an Algorithm Cuts Your Health Care," The Verge (21 March 2018) <https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy>.

280 See for example: s. 162(1) *Immigration and Refugee Protection Act*, S.C. 2001, c. 27; *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817; *Singh v. Minister of Employment and Immigration* [1985] 1 S.C.R. 177.

Right to a Fair, Impartial, and Independent Decision-Maker

Canadian law has long established that procedural fairness requires a decision-maker to be fair, impartial, and independent, as well as to be *seen* to be such. This principle is violated if, for example, a decision-maker displays bias or their conduct raises a reasonable apprehension of bias,[281] or if the decision-maker does not have their independence meaningfully provided for as a way of preserving impartiality.[282] A related aspect of this right in the immigration context is that the person who assesses the applicant's information must be the one who renders the final decision.[283] The use of algorithms in decision-making thus gives rise to a host of challenges in ensuring that applicants are able to meaningfully exercise these rights.

Case studies, empirical evidence, and investigative journalists have demonstrated on repeated occasions that algorithms can be, and often are, biased, in that they result in unfair outcomes or otherwise in consequences that disproportionately impact particular groups, often those already facing systemic bias in broader societal contexts (in which these algorithms are situated and cannot be separated from). In these cases, the resulting decisions likely cannot be considered to be fair or impartial. Even if a human officer ostensibly makes the final decision, they will have predominantly relied on what might be considered a proxy or subordinate decision-maker that has been shown to be biased or to be subject to a reasonable apprehension of bias (such as, for example, empirical evidence based on a data set of prior cases decided by that algorithm).

Second, while observers and researchers may be able to determine bias based on measuring the outcomes of a particular algorithm, there may be some cases in which a bias becomes sufficiently clear only if one sees the particular data used to train the algorithm, as well as specifically what the algorithm is programmed to do with that data, such as assigning different weights to different factors in determining applications. The law would have to provide a remedy for situations where the algorithm itself may be operating impartially, in the sense of the calculations it has been programmed to make, but that the originating data set is itself biased, which then skews the initially unbiased algorithm that is trained on that data. Moreover, the inner workings of many algorithms and the training data used for them are often subject to proprietary terms, and may be considered trade secrets. This opacity is a major challenge and obstacle to ensuring impartiality, and runs counter to principles of administrative law, including those of natural justice.

Third, in cases that provide algorithms as tools to assist human officers, who remain the primary decision-makers, the challenge is in assessing the degree to which the human officer has delegated their judgment to the algorithm. Courts or legislatures may have to determine, at some point, when and how an officer's decision crosses the line from being assisted by an algorithmic tool to being replaced by, unduly influenced by, or encumbered with the algorithmic assessment.

---

281 *R. v. Campbell*, [1999] 1 S.C.R. 565; *Wewaykum Indian Band v. Canada*, [2003] 2 S.C.R. 259, 2003 SCC 45; *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817

282 *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817; *Bell Canada v. Canadian Telephone Employees Association*, [2003] 1 S.C.R. 884, 2003 SCC 36.

283 Government of Canada, "Citizenship: Natural justice and procedural fairness" (last modified 3 July 2015) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/canadian-citizenship/admininistration/decisions/natural-justice-procedural-fairness.html>.

For example, in the case of COMPAS as described above, where a software tool was used to predict recidivism rates in the criminal justice context,[284] it remains unclear what rubric the decision-makers involved used to determine how much weight to place on the algorithmic prediction, as opposed to any other information available to them, including their own judgment and intuition. It also remains unclear what the appropriate weight ought to be, and this is likely to be heavily context-specific.

Despite the sliding scale approach to procedural fairness obligations in administrative law, immigration and refugee applicants are entitled to fewer protections even given the high stakes concerning life, liberty, and security of the person. Thus, carefully assessing the impacts of algorithmic tools on human decision-makers, and ensuring that the Canadian administrative and justice systems maintain the highest standards of impartiality, fairness, and independence of decision-makers after any introduction of machine learning or related tools, is imperative.

Right to Reasons ("Right to an Explanation")

The right to reasons, "right to an explanation," and right to disclosure are closely interlinked. One of the fundamental justifications for this collection of procedural rights is to ensure the applicant's ability to understand—and potentially to later contest—a decision-maker's rationale for an administrative decision.[285] The use of algorithms and automated decision tools poses particular challenge to these rights, in an algorithm's inability to explain itself or verbalize reasons for its decisions the way that a human decision-maker would be able and required to do.

This issue came to the forefront in a U.S. case which concerned "privately developed algorithms" to evaluate public school teacher performance and terminate teachers on that basis. The judge found that a teacher's inability to verify or replicate the score assigned to her, based on the limited information provided by the private service, raised due process concerns, as there was no way to verify accuracy or meaningfully contest the system's conclusions.[286]

As another example, a voice recognition algorithm has been used to deliver an oral language fluency test for individuals applying for working visas and permanent residency in Australia. Experts have criticized such tools, along with photo recognition and voice recognition software, due to their rendering decisions without making available any explanations for how they arrived at a given determination. There have been several publicized incidents of native speakers or fluent speakers whom the test failed,[287] and further indications that the test is biased,[288] yet no explanation of how the algorithm arrived at its decisions has been forthcoming, if it is even available.

---

284 Ed Yong, "A Popular Algorithm Is No Better at Predicting Crimes Than Random People," *The Atlantic* (17 January 2018) <https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/>

285 *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817.

286 *Houston Fed. of Teachers v. Houston Independent*, 251 F.Supp.3d 1168 (2017) at section 3 <https://www.leagle.com/decision/infdco20170530802>.

287 Melissa Davey, "Outsmarting the Computer: the Secret to Passing Australia's English-Proficiency Test," *The Guardian* (9 August 2017) <https://www.theguardian.com/australia-news/2017/aug/10/outsmarting-the-computer-the-secret-to-passing-australias-english-proficiency-test>

288 Ibid.

In contrast, the European Union's General Data Protection Regulation (GDPR), which addresses the use of automated decision-making in the context of data protection law, requires human intervention in decisions with legal or similarly significant consequences for a person.[289] The GDPR also explicitly refers to a right "to obtain an explanation of the decision reached" after assessment based on automated processing, in Recital 71, with similar rights provided for in Articles 14 and 15. [290]

While the scope of this right in the GDPR context sees ongoing debate,[291] there should be little question concerning its place in Canadian law, particularly given pre-existing legal requirements to provide written reasons for immigration decisions, which themselves are already rarely as extensive as those provided in criminal proceedings.[292] Given levels of potential jeopardy for those impacted, making new provision for or strengthening the right to an explanation in immigration and refugee applications, where they are subject to automated decision systems, is paramount.

Right of Appeal

The right to appeal a decision, either to an appellate tribunal or a court of law, is enshrined in the IRPA for the majority of immigration and refugee decisions.[293] To appeal a decision, however, the applicant must set out the grounds on which they are appealing. Where an algorithm has been involved in the impugned decision, it is unclear what grounds an applicant might appeal on, such as inaccuracy, bias, fairness, transparency, or other demonstrated deficiencies—though, of course, one may appeal on all of these grounds at once. Based on the other rights discussed above, perhaps an applicant should also be able to appeal a decision on the basis that an algorithm was involved at all, depending on the circumstances and details of its use, operations, and data.

Timing is a key issue when it comes to meaningfully providing applicants with the right to appeal, particularly given the significant ramifications that may result from delegating decisions to an algorithm, such as wrongful deportation. For example, in May 2018, the UK Government wrongfully deported over 7,000 foreign students after falsely accusing them of cheating in their English language equivalency tests. The government had believed the students cheated based on having used voice recognition software to determine if the student themselves were actually taking the exam, or had sent a proxy on their behalf. When the automated voice

289 Article 22, General Data Protection Regulation (GDPR) (EU) 2016/679 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>.

290 Recital 71, Article 14(2)(g), and Article 15(1)(h), General Data Protection Regulation (GDPR) (EU) 2016/679 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>.

291 J.M. Porup, "What does the GDPR and the "right to explanation" mean for AI?," CSO (9 February 2018) <https://www.csoonline.com/article/3254130/compliance/what-does-the-gdpr-and-the-right-to-explanation-mean-for-ai.html>; Andrew D. Selbst, and Julia Powles (2017), "Meaningful information and the right to explanation," *International Data Privacy Law* 7:4 <https://academic.oup.com/idpl/article/7/4/233/4762325>.

292 *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817. See also Bill C-17, 41st Parl, 2nd Sess: https://www.parl.ca/Content/Bills/412/Government/C-17/C-17_3/C-17_3.PDF which includes a provision providing leeway for transparency over commercial records, by permitting the government to disclose clinical trials and related supporting documentation provided to it by pharmaceutical companies seeking approval of various therapeutic products without consent from the company even if it implicates commercial secrecy obligations.

293 *For purposes of this report, we use the term 'right of appeal' in a non-technical sense to include both a statutory appeal to the Immigration Appeal Division and judicial review before the Federal Court. Access to the Federal Court is limited to the minority of applicants who obtain leave to seek judicial review. See IRPA, ss. 62-74.*

analysis was checked against human analysis, it was found to be wrong in over 20% of cases, yet this was the tool used to justify the wrongful deportations.[294] In cases such as these, procedural fairness would suggest that applicants be entitled to a right to appeal decisions before significant action is taken as a result of an algorithmic determination.

One further difficulty associated with ensuring applicants' right to appeal, where algorithmic decision-makers are concerned, is that some avenues of recourse permit applicants to appeal only on certain specified grounds, such as appealing on a question of law, as opposed to on a question of fact. This highlights a potential gap in the right that applicants are entitled to, if a would-be appellant demonstrates that the deficiency in the algorithm was due to factual error in a way that precludes any of the available grounds of appeal (such as if they are restricted to questions of law). However, as the discussion throughout this section should make clear, one of the central complexities of algorithm-based decision-makers is that they inherently engage questions of law just as much as they engage questions of fact, if not more so. Canada's legal system must grapple with what redress mechanisms to make available to a person who wishes to challenge an algorithm-based decision.

Substantive Review

Immigration and refugee decisions are highly discretionary: two immigration officers looking at the same application, the same set of facts, and the same evidence may routinely arrive at entirely different outcomes.

Administrative decision-makers—including those within the immigration and refugee system—are generally afforded significant deference by courts, in large part due to their subject-matter expertise. As a result, when tasked with judicial review, the question posed to the court is generally not whether the decision under review was "correct," but rather whether it was "reasonable."[295] In other words, the reviewing court cannot normally elect to substitute its own preferred outcome if the decision in question is among "a range of possible, acceptable outcomes which are defensible in respect of the facts and law."[296] Depending on the case and context, the range of reasonable outcomes may be quite broad, or quite narrow.[297] Immigration and refugee decisions are highly discretionary: two immigration officers looking at the same application, the same set of

294 Chris Baynes, "Government 'deported 7,000 foreign students after falsely accusing them of cheating in English language tests'" *The Independent* (2 May 2018) <https://www.independent.co.uk/news/uk/politics/home-office-mistakenly-deported-thousands-foreign-students-cheating-language-tests-theresa-may-a8331906.html>.

295 *Dunsmuir v New Brunswick*, 2008 SCC 9.

296 *Canada (Citizenship and Immigration) v Khosa*, 2009 SCC 12 at paragraph 59.

297 *Wilson v. Atomic Energy of Canada Ltd.*, 2016 SCC 29 at paragraph 35.

facts, and the same evidence may routinely arrive at entirely different outcomes.[298] As mentioned earlier in this report, when coupled with weak oversight or limited safeguards at this initial decision-making stage, the highly deferential standard applied by courts can become problematic from a human rights perspective.

Standard of review is already a complex[299] and somewhat controversial[300] area of the law. However, the "reasonableness" standard is likely to pose particularly difficult challenges where administrative decisions are rendered by (or with the assistance of) autonomous decision systems. In particular, it is not clear which specific aspect(s) of the decision-making process would be evaluated on the basis of reasonableness. At first glance, it could appear to be a simple question of whether the *outcome* rendered by an automated decision system is within that "range of possible, acceptable outcomes."[301] However, reasonable outcomes can result from decisions systems engineered according to an arbitrary or even fundamentally unreasonable logic. As an example, the US ICE uses a "Risk Classification Assessment" tool to conduct a statistical analysis meant to evaluate flight risk and threats to public safety, in determining whether an immigrant should be detained or released on bond.[302] However, this system was modified in 2017 such that the software would *only* ever recommend "detain," and never "release."[303] A system with only one potential output may result in decisions within the "range of reasonable outcomes" in certain cases (in the same way that even a broken clock is right twice a day) but it should not be afforded legal deference.

While this type of issue may be more appropriately evaluated as a matter of procedural fairness (rather than standard of review), the example serves to illustrate that reasonable outcomes alone are not enough. It also highlights the real risk that human decision-makers will sometimes behave in a highly deferential manner toward outcomes rendered by automated decision systems, even without a rational basis for doing so. It is clear that a decision-maker should not "fetter its discretion in such a way that it mechanically or blindly decides without analysing the particulars of the case and the relevant criteria."[304] Yet there is a real risk that—whether intentionally or subconsciously—decision-makers may be vulnerable to the cognitive bias that presumes technical systems will behave "scientifically," fairly, and accurately, even without any reasonable basis for that belief. In cases where an administrative decision-maker relies heavily on the outputs of an automated system (such as a risk scoring algorithm) to anchor their ultimate conclusion, the reviewing court may have a responsibility to more closely interrogate the nature of that system. In some cases, they may find that their deference—which forms part of the overarching basis for the court's application of the reasonableness standard—is not warranted.

---

298 See also Vic Satzewich, *Points of Entry: How Canada's Immigration Officers Decide Who Gets In* (Vancouver: UBC Press, 2015).

299 See for example, Paul Daly (2016), "Struggling Towards Coherence in Canadian Administrative Law? Recent Cases on Standard of Review and Reasonableness," *McGill Law Journal* 62:2 <http://lawjournal.mcgill.ca/userfiles/other/45507-ARTICLE__6_EMBEDDED__Daly.pdf>.

300 Hon. Justice David Stratas (2016), "The Canadian Law of Judicial Review: A Plea for Doctrinal Coherence and Consistency" <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733751>.

301 *Canada (Minister of Citizenship and Immigration) v Khosa*, 2009 SCC 12 at paragraph 59.

302 Mica Rosenberg, and Reade Levinson, "Trump's catch-and-detain policy snares many who have long called U.S. home," *Reuters* (20 June 2018) <https://www.reuters.com/investigates/special-report/usa-immigration-court/>

303 Ibid.

304 Guy Régimbald and Maththew Estabrooks, "Administrative Law (2018 Reissue)", *Halsbury's Laws of Canada* (Canada: LexisNexis Canada, 2018) (Quicklaw), Section IV 2(2)(b)(iii): Fettering Discretion, HAD-66.

Other Systemic Challenges and Impacts

The previous sections of this report discussed the ways in which government adoption of automated decision systems for the purpose of either replacing or assisting human decision-makers may raise human rights and administrative law challenges. This section addresses five additional systemic issues for policymakers to consider prior to adopting these technologies. They include concerns related to access to justice, risks to public confidence in the justice system, challenges surrounding private sector accountability, limits in technical capability, and the potential for problematic international impacts.

Access to Justice

The use of automated decision systems in administrative law raises particular access to justice issues. Emerging technologies related to AI (like chatbots[305]) may streamline access to government services, increase accessibility, and shorten delay for those interfacing with the immigration and refugee system. In other cases, they may exacerbate existing barriers to access. The net impact of these technologies will depend on how and why they are implemented, who they serve, and the frameworks that govern their use.[306]

The use of automated decision systems and predictive analytics for the purpose of legal research and analysis may be particularly problematic. For example, the recent RFI document related to the IRCC-DOJ pilot project seeks the use of "historical data to predict the likelihood of a case being successfully litigated" as a key functionality.[307] The system's proposed input data would include "published court decisions and general case factors, and, in future, possibly departmental applicant records (both structured and unstructured) contained in its system/database of record."[308] Yet beyond the merits of an individual case, there may be many intervening variables that contribute to determining whether the government's case against an individual succeeds. One of the most important factors is likely to be whether that individual has access to adequate legal advice. A government system designed to screen for "winnable" cases based on historical patterns may end up simply identifying those cases where the individual is self-represented or otherwise particularly vulnerable. Moreover, ordinary immigration and refugee lawyers may not have access to the same types of sophisticated technology (or technical advice) in the course of their own work. Unrepresented individuals will have even less insight and expertise. As a result, there is a real risk that these technologies may ultimately exacerbate the preexisting asymmetries of power and information between the government and the people seeking protection in Canada.[309]

---

305 Treasury Board of Canada Secretariat, "Responsible Artificial Intelligence in the Government of Canada," *Digital Disruption White Paper Series*, 10 April 2018 at page 11 et. seq. <https://docs.google.com/document/d/1Sn-qBZUXEUG4dVk909eSg5qvfbpNlRhzIefWPtBwbxY/edit>.

306 For a general discussion of this issue, see Bob Tarantino, "Should Justice be Delivered by AI?" *Policy Options* (4 April 2018) <http://policyoptions.irpp.org/magazines/april-2018/should-justice-be-delivered-by-ai/>; Agnese Smith, "Automating Justice," CBA National (Spring 2018) <http://nationalmagazine.ca/Articles/Spring-2018/Automating-justice.aspx>; John Zeleznikow, "Don't fear robo-justice. Algorithms could help more people access legal advice," *The Conversation* (22 October 2017) <https://theconversation.com/dont-fear-robo-justice-algorithms-could-help-more-people-access-legal-advice-85395>.

307 Public Works and Government Services Canada, "Artificial Intelligence Solution (B8607-180311/A)," Tender Notice (13 April 2018, amended 23 May 2018) <https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EE-017-33462>.

308 Ibid.

309 Bruno Lepri et al. (2017), "Fair transparent and accountable algorithmic decision-making processes" *Philosophy & Technology*

The introduction of automated decision systems into more areas of the law may also increase costs for claimants and litigants in the immigration and refugee system. Acquiring appropriate technical advice, analysis, and expert reports can be costly and require a high degree of specialized knowledge. This becomes particularly problematic where courts operate under the default presumption that these technologies are accurate and fair, placing the burden to prove that a system exhibits error, bias, or discriminatory effects on the applicant's shoulders. As Professor Scassa has written:

> The decision in *Ewert* suggests that in order to establish discrimination, it will be necessary either to demonstrate discriminatory impacts or effects, or to show how the algorithm itself and/or the data used to develop it incorporate biases or discriminatory assumptions. Establishing any of these things will impose a significant evidentiary burden on the party raising the issue of discrimination. Even where the *Charter* does not apply and individuals must rely upon human rights legislation, establishing discrimination with complex (and likely inaccessible or non-transparent algorithms and data) will be highly burdensome.[310]

Despite the fact that potential issues of error and bias may disproportionately affect groups that are already vulnerable or marginalized, the ability to challenge decisions made by these systems may only be available to those with significant financial resources. As courts begin to develop jurisprudence in this area, they must be sensitive to matters of cost, expertise, and complexity.

It is also unclear how the market will respond to these new modes of administrative decision-making. The private sector is already developing a number of products and services for use by prospective immigrants to Canada. For example, an immigration chat bot called Botler was launched in 2017 to help applicants in the skilled temporary foreign worker category (Programme de l'expérience Québécoise) and international students in Quebec. It uses Quebec's immigration department guidelines and "was trained on anonymized data from real cases."[311] Another prototype is Destin, "your best artificially & emotionally intelligent virtual immigration advisor," purporting to "create a pleasant experience for everyone on their new journey to Canada."[312] Not yet launched, it promises to assist with many types of immigration applications including Permanent Residence, Visitor Visas, Family Class Immigration, Startup Visas, and Investment Visas. It is unclear what data is being fed to Destin to support its analysis, but the vendor claims the product is trained for detecting eligibility, preparing documents, answering questions, and connecting applicants with immigration lawyers.[313] The result of these private sector developments may be greater access to justice and a more level playing field. The alternative is that as these systems become more sophisticated, they may

---

<http://www.nuriaoliver.com/papers/Philosophy_and_Technology_final.pdf> at page 9.

310 Teresa Scassa, "Supreme Court of Canada Decision Has Relevance for Addressing Bias in Algorithmic Decision-Making" (14 June 2018) <http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=278:supreme-court-of-canada-decision-has-relevance-for-addressing-bias-in-algorithmic-decision-making&Itemid=80>.

311 Murad Hemmadi, "Meet Botler, an A.I. chatbot that helps people immigrate to Canada," *Canadian Business* (8 February 2017) <http://www.canadianbusiness.com/innovation/botler-immigration-chatbot/>.

312 Destin AI <https://destin.ai/>.

313 Ibid.

provoke a kind of "arms race" between user-side systems designed to maximize outcomes for prospective immigrants, and government-side systems designed to prevent unfair "gaming" of its decision systems, which may add its own further collateral damage where "gaming" is inaccurately defined or identified. In that case, the net result may be increased cost and system complexity rather than improved access to justice.

As a result, there is a real risk that these technologies may ultimately exacerbate the preexisting asymmetries of power and information between the government and the people seeking protection in Canada.

Public Confidence in the Administration of Justice

The use of automated decision systems may impact public confidence in the justice system. The legal truism that justice must not only be done, but "it must also be seen to be done" is perhaps particularly true in times of significant social or technological change.[314] It is critical that choices about whether and how to adopt new technologies account for the way those technologies will be perceived by the public. As Vic Satzewich has stated in a *Toronto Star* interview, "if Canadians lose confidence in the system, their support for immigration goes down."[315]

On one hand, automated systems may strengthen the transparency, regularity, and explainability of administrative decision-making in some cases. There are a number of scientific studies that demonstrate that even when decision-makers are not specifically biased against a particular group or individual, myriad factors unrelated to the case may have an influence on outcome—including whether the decision-maker was hungry.[316] As the TBCS White Paper notes, the "capacities [of automated systems] for decision-making are not adversely affected by physical fatigue or the natural emotional and relational situations people face based on their natural makeup."[317] To the extent that automated decision systems may correct against these types of environmental and physical factors, they may help guard against a public perception of arbitrariness. At the same time, if the public develops the perception that these technologies are coloured by bias—or if a lack of transparency makes them feel more analogous to a lottery system or "magic eight ball" than fair and reasoned processes—the impact on public confidence in the administration of justice may be both disastrous and challenging to repair.

---

314 Tom R. Tyler (2000), "Social Justice: Outcome and Procedure," *International Journal of Psychology* 35:2 <https://onlinelibrary.wiley.com/doi/epdf/10.1080/002075900399411>

315 Nicholas Keung, "Canadian immigration applications could soon be assessed by computers," *Toronto Star* (5 January 2017) <https://www.thestar.com/news/immigration/2017/01/05/immigration-applications-could-soon-be-assessed-by-computers.html>.

316 See Zoe Corbyn, "Hungry judges dispense rough justice," *Nature* (11 April 2011) <https://www.nature.com/news/2011/110411/full/news.2011.227.html>.

317 Treasury Board of Canada Secretariat, "Responsible Artificial Intelligence in the Government of Canada," *Digital Disruption White Paper Series* (10 April 2018) <https://docs.google.com/document/d/1Sn-qBZUXEUG4dVk909eSg5qvfbpNlRhzIefWPtBwbxY/edit> at pages 5-6.

There are also strong normative, social, and philosophical values at play in this debate. Some decisions—no matter how transparently articulated or carefully audited—may never be seen as "legitimate" without the involvement of a human decision-maker. This is one reason among many that both Article 22 of the GDPR[318] and many civil society proposals for AIAs require that a human decision-maker be personally involved in, and accountable for, all decisions that impact a party's legal rights and "similarly significant" interests.

Specialized, independent bodies with the capability to provide informed analysis and binding oversight may also help to maintain public confidence in these systems. In response to the proposed move toward "predictive analytics" by IRCC, Andrew Griffith (the retired Director General of the Immigration Department within IRCC) recommended the creation of such an oversight body, emphasizing that "the challenge is not to embed biases into the system and create extra barriers for applicants."[319] Such an oversight body is being explored in New York City, which is the first city in the United States to establish an Automated Decision Systems Task Force to examine how the city uses algorithms.[320] Unfortunately, no such organization with a clear mandate to provide oversight and respond to complaints of data bias or algorithmic design currently exists in Canada.[321]

Private Sector Accountability

Private sector businesses have an independent responsibility to ensure that the technologies they develop do not violate international human rights.[322] They also have clear legal obligations to comply with Canadian law, including privacy and human rights legislation, in the development of their products and services. Technologists, developers, and engineers responsible for building this technology also have special ethical obligations[323] to ensure that their work does not facilitate human rights violations.

Unfortunately, government surveillance, policing, immigrations enforcement, and border security programs can incentivize and reward industry for developing rights-infringing technologies.[324] Among them is Amazon's "Rekognition" surveillance and facial recognition system, which is being marketed explicitly for use by law

---

318 Article 22, General Data Protection Regulation (GDPR) (EU) 2016/679 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>.

319 Nicholas Keung, "Canadian immigration applications could soon be assessed by computers," *Toronto Star* (5 January 2017) <https://www.thestar.com/news/immigration/2017/01/05/immigration-applications-could-soon-be-assessed-by-computers.html>.

320 New York City Office of the Mayor, "Mayor de Blasio Announces First-In-Nation Task Force To Examine Automated Decision Systems Used By The City" (16 May 2018) <http://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by>

321 Treasury Board of Canada Secretariat, "Responsible Artificial Intelligence in the Government of Canada," *Digital Disruption White Paper Series*, 10 April 2018 at pages 32-33 <https://docs.google.com/document/d/1Sn-qBZUXEUG4dVk909eSg5qvfbpNlRhzIefWPtBwbxY/edit>.

322 United Nations Human Rights Office of the High Commissioner (2011), "Guiding Principles on Businesses and Human Rights: 135 Implementing the United Nations "Protect, Respect and Remedy" Framework" at pages 13-16 <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

323 Kirsten E. Martin (2018), "Ethical Implications and Accountability of Algorithms," *Journal of Business Ethics* <https://www.researchgate.net/publication/324896361>

324 Natasha Duarte, "ICE Finds Out It Can't Automate Immigration Vetting. Now What?," *CDT* (22 May 2018) <https://cdt.org/blog/ice-cant-automate-immigration-vetting/>.

enforcement.[325] Using deep learning techniques, Rekognition is able to identify, track, and analyze individuals in real time; recognize up to 100 people in a single image; and analyze collected information against mass databases of faces. In particular, through this "person tracking" service, the government will able to identify, investigate, and monitor "people of interest," including in crowded group photos and in public places such as airports.[326] The technology has come under fire from the American Civil Liberties Union (ACLU), which has demanded that Amazon stop allowing governments to use the technology, citing "profound civil liberties and civil rights concerns."[327] A number of Amazon shareholders have also criticized the company's sale of the technology, citing long-standing issues of bias in facial recognition software, the threat of false positives, and the risk that markets for the technology would expand to include authoritarian regimes abroad—all of which may impact the company's stock valuation and increase financial risk.[328] Amazon's own workforce has led this call, as well as demanded that Amazon cut its ties with controversial data analytics firm called Palantir Technologies.[329] Palantir is responsible for providing the technology that supports the detention and deportation programs run by the US Immigration and Customs Enforcement (ICE) and the Department of Homeland Security (DHS), which Amazon workers have decried as an "immoral U.S. policy," and part of "the U.S.'s increasingly inhumane treatment of refugees and immigrants."[330]

Microsoft employees have also taken a stand against the use of private sector technology to facilitate abuses conducted by the US government, calling on the Microsoft CEO Satya Nadella to cancel its $19.4 million (US) contract with ICE as well as contracts with clients directly related to ICE.[331] A letter signed by over a hundred Microsoft workers in June reads, "as the people who build the technologies that Microsoft profits from, we refuse to be complicit."[332] By the end of the following month, 500 Microsoft employees and over 300,000 others had signed a petition reinforcing the demand.[333] Over 60 technical contributors to GitHub—the largest source code repository in the world, recently acquired by Microsoft for $7.5 billion—have also called on Microsoft to choose between dropping the contract or losing its contributors.[334]

---

325 Matt Cagle and Nocle Ozer, "Amazon Teams Up With Law Enforcement to Deploy Dangerous New Face Recognition Technology," *American Civil Liberties Union Northern California* (22 May 2018) <https://www.aclunc.org/blog/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology>

326 Ibid.

327 Ibid.

328 Letter to Jeffrey P. Bezos, "Re: Fiduciary Oversight: Rekognition and AMZN Shareholders," *ACLU Blog* (15 June 2018) <https://www.aclu.org/letter/letter-shareholders-amazon-ceo-jeff-bezos-regarding-rekognition>.

329 Kate Conger, "Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts With Law Enforcement," *Gizmodo* (21 June 2018) <https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognitio-1827037509>.

330 Ibid.

331 Letter to Satya Nadella, *New York Times* (19 June 2018) <https://int.nyt.com/data/documenthelper/46-microsoft-employee-letter-ice/323507fcbddb9d0c59ff/optimized/full.pdf#page=1>, in Sheera Fenkel, "Microsoft Employees Protest Work With ICE, as Tech Industry Mobilizes Over Immigration" *New York Times* (19 June 2018) <https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html>.

332 Ibid.

333 Sheera Frenkel, "Microsoft Employees Question C.E.O. Over Company's Contract With ICE," *New York Times* (26 July 2018) <https://www.nytimes.com/2018/07/26/technology/microsoft-ice-immigration.html>.

334 Dell Cameron, "GitHub Coders to Microsoft: Cut Ties With ICE or We'll 'Take Our Projects Elsewhere'," *Gizmodo* (21 June 2018) <https://gizmodo.com/github-coders-to-microsoft-cut-ties-with-ice-or-well-t-1827032609>.

This opposition from Amazon and Microsoft workers is part of a larger movement of technology sector workers seeking to ensure that their products and services do not contribute to human rights abuses. Other examples include resistance to AI-driven automated weapons technology from the research community[335] and the successful campaign against Google's Project Maven, an artificial intelligence surveillance engine designed for the US Department of Defense.[336] In response to public pressure and an open letter from over 4,500 Google employees declaring that the company "should not be in the business of war,"[337] the company decided not to renew its contract for the following year, and adopted a new set of new governing principles to limit the company's development of AI for weapons.[338]

Many major private sector companies are also beginning to develop codes of conduct and technical standards,[339] and participate in industry consortia and coalitions,[340] in order to better navigate the challenges raised by these technologies. Canadian businesses, notably including the Toronto-based Integrate.ai,[341] are also beginning to set out guiding principles for the responsible development of AI technology. Emerging technologies raise complex legal and ethical issues for businesses and engineers alike. What is clear is that companies engaged in the sale of automated decision system technology cannot turn a blind eye to how it will ultimately be used, or its potential threat to human rights.

Lack of Technical Capacity

In many cases, private sector companies—whether massive multinationals or small, local startups—will be responsible for the development of automated decision systems used by government. Government departments and agencies engaged in technology procurement have a responsibility to do careful due diligence to ensure that these companies are capable of designing rights-respecting technology and willing to meet stringent requirements to safeguard data. The Canadian federal government already has a complex framework of standards and guidelines in place for procurement activities, but the purchase of automated decision systems and services may raise particular challenges.

---

335 See for example, James Vincent, "Leading AI researchers threaten Korean university with boycott over its work on 'killer robots'," *The Verge* (4 April 2018) <https://www.theverge.com/2018/4/4/17196818/ai-boycot-killer-robots-kaist-university-hanwha>.

336 Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End" *United States Department of Defense News* (21 July 2017) <https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/>; Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times* (4 April 2018) <https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html>.

337 Letter to Google CEO Sundar Pichai, April 2018, hosted at *New York Times* <https://static01.nyt.com/files/2018/technology/googleletter.pdf> in Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times* (4 April 2018) <https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html>.

338 Tom Simonite, "Google Sets Limits on Its Use of AI but Allows Defense Work," *Wired* (7 June 2018) <https://www.wired.com/story/google-sets-limits-on-its-use-of-ai-but-allows-defense-work/>; Sundar Pichai, "AI at Google: our principles," Google Blog (7 June 2018) <https://www.blog.google/technology/ai/ai-principles/>.

339 See for example, Institute of Electrical and Electronics Engineers (IEEE), "IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems," (2018) <https://ethicsinaction.ieee.org/>.

340 Partnership on AI, <https://www.partnershiponai.org/about/>.

341 Integrate AI, "Responsible AI in Consumer Enterprise" (2018) <https://d1x0mwiac2rqwt.cloudfront.net/HyzJkRoYc5DUHtHbg_AMyo4gk1MGM3QUlssSk-I3TpwLPecIgrWocjUeVJ9wtp4x/by/903235/as/IntegrateAI_Responsible_AI_White_Paper_1_.pdf>.

Yet even established technologies which respond to "solved problems" (like payroll processing) have proven extremely challenging for the federal government.[342] Adopting emerging and complex tools at the bleeding edge of scientific development without in-house talent capable of understanding, evaluating, and managing these technologies is irresponsible from an engineering perspective, as well as a legal and ethical one. In the case of automated decision systems that impact individuals' immigration or refugee status, error and system failure also pose a threat to human rights. As the TBCS white paper notes: "If the government has to make decisions based on models that they don't understand or have access to, it hands some decision-making power to a private company with a black box. It is important that institutions have full understanding of the tools that they are using for decision support."[343]

A lack of technical capacity within government can lead to a potentially inappropriate reliance on the private sector.

As with many large software projects, in the case of automated decision system technology there may be strong commercial incentives for vendors to impose licensing conditions that keep source code closed, opaque, and unavailable for public scrutiny. Similarly, there may be vendor interest in using input or training data provided by government for other commercial purposes beyond the government's own use case (for example, to improve and train the vendor's unrelated products and services), raising privacy concerns.

There are also difficult questions regarding the ultimate business models of vendors in this sector. For example, Destin AI plans to launch an "emotionally intelligent" chatbot service that will help individuals prepare visa applications and other immigration-related documents.[344] Curiously, Destin AI is also listed as one of the "Interested Suppliers" in response to the RFI seeking an "Artificial Intelligence Solution" for the DOJ, ESDC, and IRCC—suggesting that the company is interested in playing "both sides" of the immigration equation.[345] Whether the Canadian government is meaningfully equipped to navigate this complex emerging market and to exercise rigorous technical oversight of these private sector tools is an open question.

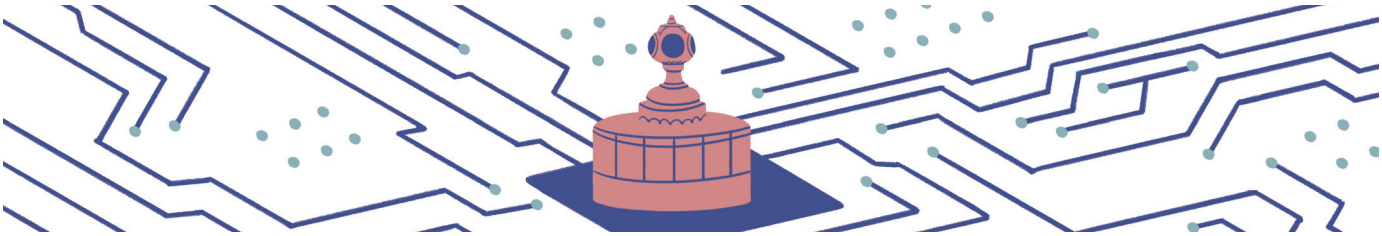
342 "Senate committee 'not confident' government has learned lessons from Phoenix," *CBC News* (31 July 2018) <https://www.cbc.ca/news/politics/senate-committee-phoenix-report-1.4767997>.

343 Treasury Board of Canada Secretariat, "Responsible Artificial Intelligence in the Government of Canada," *Digital Disruption White Paper Series* (10 April 2018) at page 29 <https://docs.google.com/document/d/1Sn-qBZUXEUG4dVk909eSg5qvfbpNlRhzIefWPtBwbxY/edit>.

344 Destin AI <https://destin.ai/>.

345 Public Works and Government Services Canada, "List of Interested Suppliers for Artificial Intelligence Solution (B8607-180311/A)" <https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EE-017-33462/list-of-interested-suppliers>.

Global and International Impacts



Technology travels. Whether in the private or public sector, a country's decision to implement particular technologies can set an example for other countries to follow. This is doubly true if Canada continues to present itself as a leader both in AI[346] as well as in human rights.[347] Machine learning and predictive analytics in the immigration space is already being explored in various jurisdictions across the world, as well as by international agencies that manage migration, such as the UN. Canada has a unique opportunity to develop international standards that regulate the use of these technologies in accordance with domestic and international human rights obligations. It is particularly important to set a clear example for countries with more problematic human rights records and weaker rule of law, as insufficient ethical standards and weak accounting for human rights impacts can create a slippery slope internationally. Canada may also be responsible for managing the export of these technologies to countries more willing to experiment on non-citizens, and infringe the rights of vulnerable groups with few ramifications.[348]

These power dynamics are crucial to interrogate in the migration space, where private sector interventions increasingly proliferate, as seen in the recent growth of countless apps for[349] and about[350] refugees. However, in the push to make people on the move knowable, intelligible, and trackable,[351] technologies that predict refugee flows can entrench xenophobia, as well as encourage discriminatory practices, deprivations of liberty, and denial of due process and procedural safeguards. With the increasing use of technologies to augment or replace immigration decisions, who benefits from these technologies and what does success look like? While efficiency may be valuable, those responsible for human lives should not pursue efficiency at the expense of fairness—fundamental human rights must hold a central place in this discussion. By placing human rights at the centre, the careful and critical use of these new technologies in immigration and refugee decisions can benefit both Canada's immigration system as well as the people applying to make their new home here.

---

346 Canada.ai, "New Canada.ai platform showcases Canada's global leadership in artificial intelligence," *Cision* (16 January 2018) <https://www.newswire.ca/news-releases/new-canadaai-platform-showcases-canadas-global-leadership-in-artificial-intelligence-669535743.html>

347 The Government of Canada, "Canada's approach to advancing human rights," amended 13 June 2017 <http://international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/advancing_rights-promouvoir_droits.aspx?lang=eng>

348 For an example of this issue in another context, see the way in which Canada allows the export of Internet filtering technology: Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert, "Planet Netsweeper: Executive Summary" *The Citizen Lab* (25 April 2018) <https://citizenlab.ca/2018/04/planet-netsweeper/>

349 Amy Weiss-Meyer, "Apps for Refugees" *The Atlantic* (May 2017) <https://www.theatlantic.com/magazine/archive/2017/05/apps-for-refugees/521466/>

350 Olivia De Backer, "Big Data and International Migration" *United Nations Global Pulse: Pulse Lab Diaries* (16 June 2014) <https://www.unglobalpulse.org/big-data-migration>

351 Anirudh V. S. Ruhil , " Millions of refugees could benefit from big data – but we're not using it," *The Conversation* (29 January 2018) <https://theconversation.com/millions-of-refugees-could-benefit-from-big-data-but-were-not-using-it-86286>

Recommendations

1. **Publish** a complete and detailed report, to be maintained on an ongoing basis, of all automated decision systems currently in use within Canada's immigration and refugee system, whether by IRCC, CBSA, or any other federal departments or agencies. Disclosure about each system should include, at minimum:
    a. The purpose for which the system is used;
    b. The names of the individual(s) and offices within government who hold ultimate responsibility for the adoption, use, and outcomes of the system;
    c. A detailed description of the training data used, as well as information regarding all selection, review, and auditing mechanisms for that training data;
    d. Full disclosure of the training set, where such disclosure is both supported and supervised by the Office of the Privacy Commissioner and raises no credible privacy risk, whether directly or indirectly;
    e. A detailed description of the inputs, factors, and criteria weighed by the system;
    f. An indication of the extent to which the system replaces, modifies, or augments a formerly human-led decision-making process;
    g. Information concerning whether the system (or part of the system) is a product or service of a private vendor, and if so, information about that vendor and the nature of the contractual relationship between the parties, including ownership of intellectual property related to the algorithm(s), as well as ownership and custody of, and accountability for, all collected data;
    h. The metrics used to evaluate the system's accuracy, efficiency, fairness, and ability to achieve government objectives, including specifically any efforts undertaken to test the automated decision-making system's potential impact on marginalized and vulnerable groups;
    i. The system's rate of error (including the likely rate of false positives as well as false negatives);
    j. Any Privacy Impact Assessment (PIA) associated with the system;
    k. Any documentation related to the independent scientific validation or peer review of the system or elements of the system.

2. **Freeze** all efforts to procure, develop, or adopt any new automated decision system technology, including the "Artificial Intelligence Solution" technology contemplated in the April 2018 Request for Information from DOJ, IRCC, and ESDC[352], until existing systems fully comply with a government-wide Standard or Directive governing the responsible use of these technologies.

352 Public Works and Government Services Canada, "Artificial Intelligence Solution (B8607-180311/A)," Tender Notice (13 April 2018, amended 23 May 2018) <https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EE-017-33462>.

3. **Adopt** a binding, government-wide Standard or Directive for the use of automated decision systems, which should apply to all new automated decision systems *as well as those currently in use* by the federal government, that:
    a. Requires all automated decision systems to operate in strict compliance with Canada's international human rights obligations and the *Charter*, and to be accompanied by a statement which "lay[s] out the government's principled position regarding how, on a balance of probabilities, the [automated decision system] complies with the purposes and provisions of the *Charter;*"[353]
    b. Provides for a robust framework of procedural fairness and due process in administrative decision-making, including, but not limited to, requirements for:
        i. Clear notice to individuals that a decision, including profiling, concerning their rights and interests that produces legal or similarly significant effects will be made in full or with the support of an automated decision system;
        ii. Meaningful explanation in the form of written reasons for any decision that relies in full or is made in part with the support of an automated decision system, including details regarding the provision of meaningful information regarding the underlying logic involved and criteria relied upon in any automated component of the decision;
        iii. Access to fair and transparent review and appeals procedures, including discovery mechanisms and obligations that ensure that affected individuals are capable of meaningfully challenging any automated decision systems relied upon;
        iv. Create a mechanism for the inclusion of amici or similarly independent parties with subject-matter specific expertise where automated decision-making mechanisms are implicated in review or appeal proceedings.
    c. Requires that any body of government which makes use of an automated decision system also provides for clear processes to facilitate complaint, review, redress, and appeal (and notice to all individuals impacted by those systems that these processes are available);
    d. Requires the completion of a full Algorithmic Impact Assessment for every system (including retroactive assessments of existing systems) according to a standardized, public framework which explicitly evaluates for compliance with international human rights law and the *Charter;*
    e. Establishes a framework for ongoing monitoring and periodic formal reviews, as well as a formal documentation process for all known errors and incidents;

353 The Canadian Civil Liberties Association, "Charter First: A Blueprint for Prioritizing Rights in Canadian Lawmaking" (September 2016) <https://ccla.org/cclanewsite/wp-content/uploads/2016/09/Charter-First-Report-CCLA.pdf>.

f. Sets out robust requirements for independent,[354] academic peer-review and scientific validation of all automated decision system technologies (and/or their component technologies) used by government prior to their adoption;
g. Explicitly requires independent, academic peer-review and scientific validation to ensure that automated decision system technologies do not result in either direct or indirect discrimination on the basis of race, national or ethnic origin, colour, religion, sex, age or mental or physical disability in their use or effects;
h. Requires that in every case where an automated decision system is used, that a human-led contingency framework or backup system is adopted to ensure that in the case of system failure or restrictions on use, individuals impacted by that system will have a non-prejudicial alternative;
i. Requires that when accounting for potential error in automated decision system design or implementation, that the system is designed to err on the side of the more minimally rights-impairing outcome;
j. Guarantees that no decision which prejudicially impacts the rights or interests of an individual is made by an automated decision system alone;
k. Ensures that all individuals responsible for using an automated decision system in the course of their work are adequately trained, and that their training includes a detailed review of how a given system functions as well as its limitations;
l. Includes statistical tracking and periodic reporting mechanisms tracking the frequency in which outcomes suggested by automated decision systems ultimately align with final decisions;
m. All automated decision-systems should favour implementation in a manner that ameliorates conditions of disadvantaged or marginalized individuals or groups.

4. **Establish** an independent, arms-length body with the power to engage in all aspects of oversight and review of all use of automated decision systems by the federal government, and in particular with the ability to review, test, and audit source code and training data which cannot be made public for reasons of national security and/or privacy.

5. **Create** a rational, transparent, and public methodology for determining the types of administrative processes and systems which are appropriate for the experimental use of automated decision system technologies, and which are not. This framework must:
    a. Recognize that there are spectrums of potential *impact* on individuals' rights and interests (including those protected under international human

354 And in particular, not affiliated with any potential third-party vendor in any manner.

rights law and the *Charter*), of potential *harm* (sometimes irreparable) to those rights and interests, and of potential *complexity* in system design.

b. Acknowledge that many machine learning and artificial intelligence technologies remain in their infancies, and that government adoption should follow the state of the discipline: i.e., from a purely computer science perspective, applications which are rote, repeatable, and easy to correct may already be responsible use cases for automated decision systems, whereas those which are discretionary, complex, and require a high degree of subjective judgment will not.
c. Accept that there some decisions which may never be appropriately or lawfully made by an automated system.

6. **Commit** to making complete source code for all federal government automated decision systems—regardless of whether they are developed internally or by the private sector—public and open source by default, subject only to limited exceptions for reasons of privacy and national security.

7. **Launch** a federal Task Force that brings key government stakeholders (including OPC, TBSC, IRCC, DOJ, ISED, GAC, PSC, and CBSA) alongside academia and civil society to better understand the current and prospective impacts of automated decision system technologies on human rights and the public interest more broadly.

APPENDIX A
ACCESS TO INFORMATION REQUESTS

Access to Information Requests

The IHRP and the Citizen Lab have submitted 27 separate Access to Information (ATI) requests to the Government of Canada, including to the CBSA, IRCC, CSIS, Shared Services Canada (SSC), Public Safety and Emergency Preparedness (PSEP), Global Affairs Canada (GAC), Innovation, Science and Economic Development (ISED), and the Royal Canadian Mounted Police (RCMP). As of publication of this report, the authors continue to await data in response to these requests and intend to publish results in full as they become available.

The following requests were submitted in April 2018.

CANADA BORDER SERVICES AGENCY
All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in screening immigration and refugee applicants by CBSA officers.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the enforcement of deportation and removal proceedings (and all determinations and/or related decision-making).**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **for the purpose of border security at all ports of entry.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the context of immigration detention (and all related determinations and/or decision-making).**

IMMIGRATION, REFUGEES, AND CITIZENSHIP CANADA
All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and

external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Express Entry Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Startup Visa Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Self-Employed Person in Cultural or Athletic Activities or as a Farm Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Provincial Nominees Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Caregivers Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Atlantic Immigration Pilot Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics,

algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Family Sponsorship Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Immigrant Investors Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Quebec Selected Skilled Workers Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the Temporary Foreign Worker Program.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in admissibility / inadmissibility assessments and determinations made on grounds of security.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in admissibility / inadmissibility assessments and determinations made on grounds of criminality.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning in admissibility / inadmissibility assessments and determinations made on grounds of medical inadmissibility.

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the questionnaire used by the Royal Canadian Mounted Police to collect information on asylum seekers who arrived irregularly at the border (i.e., the questionnaire described in this article: https://www.thestar.com/news/canada/2017/11/27/rcmp-will-redact-more-than-5000-records-collected-using-questionnaire-targeting-muslim-asylum-seekers.html), and specifically:

- The questionnaire itself;
- All records related to the design and drafting of the questionnaire;
- All records synthesizing, organizing, or aggregating the information collected using the questionnaire;
- All records related to the past, current, planned or potential use, storage, retention, destruction, and analysis of the information collected;
- All records related to the past, current, planned or potential disclosure and sharing of the information collected to any other Canadian government agency, private entity, or foreign government.

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **for the purpose of assessing or making determinations related to "risk" of immigration and refugee applicants to Canada.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **for the purpose of assessing or making determinations related to the existence and/or likelihood of "fraud" and/or "misrepresentation" by immigration and refugee applicants to Canada.**

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **in the context of security certificate proceedings.**

SHARED SERVICES CANADA

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to

the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **by the Canadian federal government.**

CANADIAN SECURITY INTELLIGENCE SERVICE
All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **for the purpose of assessing or making determinations related to "risk" of immigration and refugee applicants to Canada.**

GLOBAL AFFAIRS CANADA
All records held by Global Affairs Canada (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **by the Canadian federal government.**

INNOVATION, SCIENCE AND ECONOMIC DEVELOPMENT CANADA
All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to **Canadian companies engaged in the development and/or sale of products or services related to "big data" analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning technologies for use by government clients, whether in Canada or abroad.**

ROYAL CANADIAN MOUNTED POLICE
All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the questionnaire used by the Royal Canadian Mounted Police to collect information on asylum seekers who arrived irregularly at the border (i.e., the questionnaire described in this article: https://www.thestar.com/news/canada/2017/11/27/rcmp-will-redact-more-than-5000-records-collected-using-questionnaire-targeting-muslim-asylum-seekers.html), and specifically:

- The questionnaire itself;
- All records related to the authorization, design, and drafting of the questionnaire;
- All records synthesizing, organizing, or aggregating the information collected using the questionnaire;
- All records related to the past, current, planned or potential use, storage, retention, destruction, and analysis of the information collected;

- All records related to the past, current, planned or potential disclosure and sharing of the information collected to any other Canadian government agency, private entity, or foreign government.

All records (including but not limited to draft and final policies, guidelines, privacy impact assessments, meeting notes, technical specifications, training documents, bulletins, memoranda, and all internal and external correspondence, including e-mail) for the period between January 1, 2013 and April 1, 2018 related to the use (or potential use) of "big data," big data analysis, algorithmic decision-making, algorithmic analytics, algorithmic analysis, "predictive analytics," predictive analysis, and/or machine learning **for the purpose of assessing or making determinations related to "risk" of immigration and refugee applicants to Canada.**

APPENDIX B
RCMP QUESTIONNAIRE

In 2017, the RCMP collected the following questionnaire from over 5,000 asylum seekers near the unofficial border crossing between the United States and Quebec at Roxham Road.

NOM / NAME:

DDN / DOB:

CITOYENNETÉ / CITIZENSHIP:

ENTREVUE / INTERVIEW

Demandez aux gens s'ils ont fait eux-mêmes leur valise et que tout le contenu leur appartient? Au même titre pour les ordinateurs de poche. Vous pouvez leur dire que tout ce que vous trouverez pourrait servir de preuve contre eux.	Ask people if they have loaded their suitcases themselves and whether all of the contents belong to them? In the same way for handheld computers. You can tell them that anything you find could serve as proof against them.

1. D'où venez-vous? / Where do you come from?

2. Pourquoi ne vous êtes-vous pas présentés à un poste frontalier? / Why did you not come to a border crossing?

3. Depuis combien de temps demeurez-vous aux États-Unis? / How long have you been in the United States?

4. Qu'est-ce qui vous motive à quitter les États-Unis? What motivated you to leave the United States?

5. Que faisiez-vous aux États-Unis pendant tout ce temps? / What were you doing in the United States all this time?

6. À quel endroit demeuriez-vous? / Where did you stay?

7. Avec qui? Nom(s) et DDN(s) / With whom? Name(s) and DOB(s)?

8. De quoi viviez-vous? (ex. emploi, famille, gouvernement) / What were you living off of? (ex. work, family, government)

9. Qu'est-ce qui vous motive à venir au Canada? / What motivated you to come to Canada?

10. Avez-vous appliqué pour un statut d'immigration ou de réfugié aux États-Unis? /
Have you applied for refugee status in the United States or to immigrate to the United States?

11. Quels sont les résultats de votre demande? / What were the results of your application?

12. Aviez-vous un emploi? Si oui, quel était votre métier? / Did you have an employment? If so, what was it?

13. Avec qui voyagez-vous? / Who did do you travel with?

14. Avez-vous de la famille au Canada? Nom(s) et DDN(s)? Où sont-ils? Que font-ils? /
Do you have family in Canada? Names and DOBs? Where are they? What do they do?

Membre famille / Familly Member	DDN / DOB	Métier / Occupation	Ville / City

15. Comment est votre santé? / How is your health?

Membre / Member:

Reg. / Reg #:

Heure / Time: Date:

Signature du détenu / ~~Detainee~~'s signature

16. Qui vous a informé sur la façon de vous rendre au Canada? / Who informed you about how to get to Canada?

17. Que vous a-t'on dit? / What were you told?

18. Est-ce que l'on vous a chargé quelque chose? Si oui, combien. / Have you been charged with anything? If so, how much?

19. Avez-vous manipulé des armes à feu par le passé? / Have you handled firearms in the past?

20. Avez-vous servi dans l'armée? / Have you served in the army?

21. Avez-vous des affiliations à des groupes politiques? / Do you have affiliations with political groups?

22. Avez-vous déjà subventionné des organisations ou des groupes politiques? / Have you ever contributed to organizations or political groups?

23. Connaissez-vous quelqu'un affilié à un groupe politique ou extrémiste? / Do you know someone affiliated with a political or extremist group?

24. Quelle est votre opinion sur les attaques terroristes? / What is your opinion about terrorist attacks?

25. Quelle est votre opinion à propos du groupe État islamique (EI, EII, ISIS, DAESH), des Talibans, etc. ?/ What is your opinion about the group Islamic State (EI, EII, ISIS, DAESH), the Talibans, etc. ?

26. Avez-vous déjà commis une infraction criminelle? / Have you ever committed a criminal offense?

27. Avez-vous déjà été arrêté? / Have you ever been arrested?

28. Êtes-vous recherchés par les autorités policières de votre ou d'un autre pays? / Are you being sought by the police or other government authorities from your or any other country?

29. Avez-vous des intentions criminelles durant votre séjour au Canada? / Do you have any criminal intentions while in Canada?

30. Avez-vous des intentions de protester au Canada au sujet des événements qui se produisent dans votre pays? / Do you have any intentions to protest in Canada about the events that are taking place in your country?

31. Le Canada est un pays très libéral qui croit à la liberté de la pratique religieuse et de l'égalité entre les hommes et les femmes. Quelle est votre opinion sur ce sujet? Comment vous sentiriez-vous si votre patron était une femme? Comment vous sentez-vous par rapport aux femmes qui ne portent pas le Hijab (couvre la tête), Dupatta (couvre la tête et les épaules), Chador (couvre la tête et le corps), Niqab (couvre la tête, la figure et le corps), Burka (couvre tout le corps, incluant les yeux)?

31. Canada is a very liberal country that believes in freedom of religious practice and equality between men and women. What is your opinion on this subject? How would you feel if your boss was a woman? How do you feel about women who do not wear the Hijab (covers the head), Dupatta (covers head and shoulders), Chador (covers head and body), Niqab (covers head, face and body), Burka (covers the entire body, including the eyes)?

Membre / Member:

Reg. / Reg #:

Heure / Time: Date:

Signature du détenu / Detainee's signature

32. Si une personne de votre entourage commet une infraction ou un acte réprimandable que feriez-vous? / If someone around you commits an offense or a reprimandable act what would you do?

33. Le dénonceriez-vous? / Would you denounce him or her?

34. Quelle est votre religion? / What is your religion?

35. Pratiquez-vous votre religion, si oui, à quelle fréquence? / Do you practice your religion, if so, how often?

36. Avez-vous utilisé un passeport d'une autre nationalité pour voyager? / Did you use a passport of another nationality to travel?

37. Avez-vous de la famille, des amis ou contacts aux États-Unis? / Do you have any family, friends or contacts in the USA?

Nom / Name	Sexe / Gender	Relation / Relationship	Ville / City

38. Qui vous a aidé pour voyager aux États-Unis et au Canada? / Who helped you to travel to the USA and Canada?

39. Combien d'argent avez-vous avec vous? Combien d'argent avez-vous de disponible tel que les cartes de crédit, compte bancaire, etc.? / How much money do you have with you? How much money do you have available such as credit cards, bank account, etc.?

40. Avez-vous des affiliations avec des groupes extremistes? / Do you have affiliations with extremist groups?

Commentaires additionnels / Additional Comments :

Membre / Member:

Reg. / Reg #:

Heure / Time:

Date:

Signature du détenu / Detainee's signature