Centre on Migration, Policy and Society

Working Paper No. 149
University of Oxford, 2020

Efficient Discrimination: On How Governments Use Artificial Intelligence in the Immigration Sphere to Create and Fortify 'Invisible Border Walls'.

Roxana Akhmetova

WP-20-149

Abstract

Artificial intelligence (AI) promises to revolutionize how government agencies do their work. Governments like Canada have been implementing and testing AI-powered technologies in their immigration systems since at least 2014. In this working paper I focus on Canada and argue that since Canada does not have a robust governing and legal structure to oversee the use of AI, there is a potential for AI to be used as a scapegoat for wrongful government decision-making or as another form of non-entrée policy aimed at reinforcing a discriminatory Canadian migration system that contributes to the racialization of the citizenry. AI technologies have yet to reduce or eliminate bias and discrimination that plagues human decision-making. As such, the current use of AI and related new technologies has a great potential to increase the efficiency of producing discriminatory decisions in the immigration sphere. To support my argument, I begin to develop and advance the concept of the 'invisible border wall'. This wall has the potential to mask abuse, exploitation, and exclusion of vulnerable groups of people like asylum seekers and stateless migrants, which stands contrary to the values of many countries like Canada as being a welcoming nation that offers equal opportunities and equality under the law.

Author: Roxana Akhmetova, roxana.akhmetova@keble.ox.ac.uk

Keywords: artificial intelligence, human rights, immigrants, asylum seekers, 'invisible border wall'.

Disclaimer: The views expressed in this document are those of its author and should not be regarded as representing the views of COMPAS.

Introduction

Artificial intelligence (AI) promises to revolutionize how government agencies make decisions and conduct routine tasks (Ferguson, 2017). Recent developments in AI have the potential to not only secure data but make greater use of it, improve the quality of decisions, and reduce the cost of some governance functions, thus promising to make governments more efficient, accountable, and effective (Ferguson, 2017). Examples of AI include AI-powered lie detectors that operate in airports and at border crossings (Gallagher and Jona, 2019), automated decision-making systems used to make decisions on immigration applications (Molnar and Gill, 2018), and drone surveillance (Pedrozo, 2017). Despite the increasing use of AI in government decision-making and a growing amount of attention in the public and academic spheres on the potential benefits of these technologies, there is an insufficient amount of information on why government agencies use AI systems beyond a few surface-level descriptions. In this working paper, I begin to address some of these gaps by focusing on the Canadian government's increasing reliance on AI in the immigration and border control spheres.

Several reasons motivate the choice of selecting Canada as the case study of this working paper. First is the paradoxical juxtaposition of Canada's image as a country that welcomes refugees and humanitarian migrants and the policies it uses to limit how many of these individuals reach its territory. The 'generosity' of the Canadian government towards asylum seekers has been acknowledged on several occasions, once by the Nansen Medal which was awarded to Canada in 1986 for its work with refugees as well as the praise it received by the United Nations (U.N.) for the number of Syrian refugees it welcomed between 2015-2019 (Basok and Simmons, 1993; Cecco, 2019). Despite these accomplishments, the Canadian refugee and immigration system contains a number of non-entrée policies which continue to generate a lot of critique from human rights groups (Lacroix, 2004). Moreover, some argue that Canada's refugee and immigration policies are some of the most controversial and highly debated political and social issues (Lacroix, 2004).

In light of the above, it is particularly important to investigate the ways in which Canadian immigration and border control agencies are beginning to use AI like automated decision-making systems and risk-assessment technologies. Most of these technologies are in their nascence and are experimental in nature, thus their impacts on human rights are not fully known. Despite many unknowns, it is worthy to consider why Canada continues to 'experiment' with test and pilot AI technologies on vulnerable groups of people like

humanitarian migrants. AI can be a political tool used to insulate governments from liability while presenting the immigration procedure as liberal and non-biased (Aradau and Tazzioli, 2020). AI is not inherently democratic and can reduce government accountability and transparency while validating the expansion of Canada's immigration detention powers, exporting border violence outside of Canada by its own agents and in collaboration with other enforcement regimes, and limiting the scope of protection available to humanitarian migrants under Canadian law.

The main argument of this working paper is that as long as AI technologies continue to be used in the current immigration system, which actively relies on non-entrée policies to fortify an 'invisible border wall', AI might not reduce or eliminate bias and discrimination that plague human decision-making. Rather, the use of AI has the potential to increase the efficiency of producing discriminatory decisions in the immigration sphere by governments, especially if they continue to lack a robust regulatory framework to oversee the use of these technologies. Non-entrée policies, such as visa controls, safe third-country mechanisms, and interdiction at sea of refugees are public measures and are more 'visible' and more open to public scrutiny. The proprietary algorithms of many AI technologies that are being increasingly used to make governance decisions can make border and immigration control even more invisible and can further reduce governments' accountability and transparency. There are two main reasons for this. First, using AI in the immigration sphere can be ethically challenging not only because asylum and immigration-related evaluations can be highly discretionary, but also because these decisions can have significant impacts on the lives of individuals seeking refuge. The second issue is algorithmic bias. Depending on the way the algorithm is designed to sort data and make decisions, algorithmic bias can lead to unintended discrimination or negative feedback loops that reinforce and exacerbate existing inequalities and discriminatory practices (Ng, 2017).

I begin to develop my argument by providing background information on some AI technologies that are used in the Canadian immigration and border control sphere. The lack of clear and robust national governing and legal standards in Canada has the potential to result in unethical use of AI by governments. I then move on to discuss the increasing role of AI technologies in the construction and fortification of what I call 'invisible border walls'. I argue that these technologies can externalize and expel 'undesirable' migrants (such as humanitarian and non-economic). I also discuss the reasons why the use of AI in the immigration sphere is highly problematic and might not immediately lead to accountable and bias-free immigration systems.

AI technologies

AI is the programming and training of a computer using statistical models to do tasks typically reserved for human intelligence (Calo, 2017). One of the main goals of AI is to formalize knowledge and mechanize reasoning in all areas of human endeavors in order to make working with computers 'as easy as' working with people (Tecuci, 2012). AI algorithms draw on vast amounts of data to learn and make inferences about patterns and future behaviour and their developers promise great potential not only in forecasting, managing, and controlling migratory flows but also in mass surveillance and automated decision-making (Beduschi, 2018; IOM, 2018; Rango, 2015). AI is especially beneficial for making predictions, sorting data, and finding patterns. Computer algorithms are powerful tools for automating many aspects of life, especially those that require step-by-step routines such as organizing and digitizing operational and administrative tasks making them more consistent and faster (Bansak et al., 2018). The ever-increasing amount of data and computing power have reached a point where it has become very useful to develop new technologies which can pick up patterns that humans may otherwise miss (UKGOS, 2016).

The use of AI not only includes the 'management' of migration and borders but also surveillance, decision-making on migration-related applications, and prediction of migration patterns. Governments collect large amounts of data and use AI technologies to analyse it, find patterns, and make decisions based on patterns that the algorithms find. Some states use AI technologies to predict the next wave of migration by analysing data from Google Trends, Wi-Fi positioning, and data collected from social media (Connor, 2017). This data may also be collected from social media activity or from private companies like telecommunications companies which collect information on call duration, Wi-Fi-positioning, among other information. This information is typically stripped of identifiers like names and addresses; however, it is possible to re-identify individuals (Na et al., 2018). For example, United Nations High Commissioner for Refugees (UNHCR) used Food and Agriculture Organization's data to discover that the drop in the price of goats in one Ethiopian region and a spike in the price in another region could be used to track the migration of internally displaced people as they were buying new goats to replace the ones they sold before leaving (UNHCR Innovation Service, 2019).

Central to the interest around AI is the potential it offers for autonomous decision-making. Many algorithmic processes can be used to make decisions without human input and even

learn continuously and make deductions without human assistance (Margetts and Dorobantu, 2019). One such example is the U.S. Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) which uses AI algorithms to make decisions on the rate of recidivism of individuals based on decisions and data from previous cases (Margetts and Dorobantu, 2019). Analysing data gathered by AI can help government agencies to better prepare for the influx of migrants and make more informed decisions on how to receive individuals by identifying inefficiencies in state-provided facilities. These gaps could include a lack of sufficient housing spaces, lack of staff to process asylum claims, or a lack of funding to support migrants as they settle in their receiving country. For example, Switzerland is testing an algorithm based on techniques like machine learning to predict the next 'migration crisis' and to improve refugee integration, while the revised Schengen Information System in the European Union is being geared to use DNA, facial recognition, and biometric data to assist with illegal migration (Bansak et al., 2018; Carammia and Dummont, 2018).

Despite the few actual and many promised positive benefits, the current use of AI-powered technologies by government agencies in relation to migration can be unethical at times. One of the reasons for this is because the use of AI in many countries, including Canada is not governed by clear and robust governing ethical and legal standards. If managed well, AI tools can modernize public administration and bureaucracy resulting in more accurate, efficient, and equitable forms of state action. If these technologies are not managed properly, their use can result in wrong decision-making, widen the public-private technology gap (meaning that the private sector innovates while governments lag behind in updating their technologies), increase the potential of arbitrary government action and decision-making, enable surveillance that could threaten privacy and civil liberties, further disempower marginalized groups, and increase the role that domestic and foreign technology companies play in government decision-making. The use of AI technologies has significant implications for the fundamental rights of those subjected to them; thus, proper use of AI by government agencies is gravely important.

Most AI technologies are novel, experimental, and controversial yet their use by governments and other actors is growing. Due to the novelty of these technologies, many of their impacts are unknown and their use is not yet governed by a set of international and very few national legal standards. As a result, the use of technologies like digital IDs, biometrics, mass surveillance, blockchain, automated decision-making systems, among other technologies present ethical concerns. Examples of problematic overreliance on AI can be found around

the world. The 'Extreme Vetting Initiative' is one of many such examples. The U.S. Immigration and Customs Enforcement (ICE) unveiled this program in 2017 (Harwell and Miroff, 2018). This program was meant to make the manual vetting process centralized and streamlined by using government agency and law enforcement databases and collect data from public information found on social media websites. The goal was to automatically determine the probability that an applicant would be a positively contributing member to society and to national interests and predict whether the individual intends to commit criminal or terrorist acts after entering the country (Harwell and Miroff, 2018). The project was abandoned in 2018 in part due to the complications such as how to define what a 'positively contributing member of society' is and how to accurately predict the probability of being a 'good citizen' based on data collected on social media websites and other publicly available online sources. Further, this initiative has the potential to affect free speech because potential migrants might be afraid of posting information about themselves on social media knowing that the U.S. government might gather this data.

Another example occurred in 2014, when 7,000 students were wrongfully deported from the U.K. because an algorithm wrongly accused them of cheating on a language test (Baynes, 2018). While in 2020, an algorithm was used to more accurately predict how U.K. test-takers would have performed on final exams which did not occur due a global pandemic (Walsh, 2020). The algorithm was also used to compensate for the tendency of teachers to inflate the expected performance of their students. Around 40 per cent of the predicted performances were downgraded, mostly of those students with high grades from less-advantaged schools, while students from richer schools were more likely to have their scores raised (Walsh, 2020). This is just one of many examples of how attempting to make decisions using AI raises serious concerns for the protection of human rights for vulnerable individuals like non-citizens, asylum seekers, and marginalized individuals.

Canada's use of AI

The Canadian federal government has been testing and introducing algorithms into its immigration decision-making focusing on such tasks such as determine the completeness of the application; assess if an applicant poses a risk or filed a fraudulent application; help determine the likelihood that an application is fraudulent; check the probability that a marriage is genuine; or the probability that the child is biologically or legally that of the applicant (Molnar and Gill, 2018). In 2018, the Canadian federal government launched two pilot projects that

use AI to process temporary resident visa applications from China and India (Wright, 2018). The Canada Border Services Agency (CBSA) is also expanding its reliance on AI by testing AI-powered technologies like AVATAR which can tell if passengers are lying about their motives to travel (Daniels, 2018).

Further, section 109.1 of the Immigration and Refugee Protection Act (IRPA) determines which countries should be placed on the Designated Countries of Origin list (DCO), which contains a predictive algorithm to assess whether a country is 'safe' based on past grant rates of refugee status (IRPA, 2001). The overarching provision includes "countries that do not normally produce refugees and respect human rights and offer state protection" (Molnar and Gill, 2018). The DCO list has been widely criticized as discriminatory and based on an incomplete definition of safety as it does not take into consideration vulnerabilities and identities that might be associated with mixed migration and those which may make a country unsafe for certain groups of people, such as women fleeing domestic violence or members of the LGBTQ+ community. Throughout the deportation proceedings, the Canada Border Services Agency (CBSA) may collect data that could be shared with other departments and may prevent individuals from being able to enter Canada in the future (Molnar and Gill, 2018). The collection of data as stated above may also be shared with the applicant's country of origin which could put them in danger if the individual is escaping persecution.

Canadian privacy laws and judicial authorization required by the Criminal Code have been limiting the government from gathering big data and conducting expansive surveillance of its citizens, which has become increasingly common in the U.S. This recently changed as the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (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 created the *Communications Security Establishment Act*. The bill involves changes related to the collection, use, and disclosure of information about individuals. The bill introduces several much-needed reforms and a new review framework; however, it also further entrenches the controversial surveillance practices of both CSIS and CSE, including the mass and untargeted 'bulk collection' of electronic data. Despite serious concerns from the international human rights law community with regard to this practice, where the subjects of surveillance are non-Canadian persons outside of Canada, no meaningful safeguards to protect their right to privacy exist (UNHCR, 2014).

Canada's immigration and refugee law are closely interconnected with its national security apparatus. Under the authority of the *CSIS Act*, Canada's intelligence agencies have broad 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*. 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 and by CSE can influence certain immigration-related automated decision-making systems.

Using AI can help to process an ever-growing number of routine cases quicker. However, what remains unclear is exactly how these automated systems are used, what criteria is used to define and assess 'fraud', 'risk', and 'misrepresentation'; what kind of data is fed into algorithms; and who has access to it and with what other agencies or governments this information is shared. Further, it is unclear what the government considers to be an acceptable margin of error for these systems and what the grounds of appeal are if the technology rejects the application. The use of these technologies has alarming implications for the fundamental human rights of those subjected to their use and there is a need to consider the potential and actual impacts of increased reliance of AI by governments.

Having clear answers to these questions is important as they would allow governments to be held accountable for their decision-making. However, allowing AI-based immigration decisions to be up for scrutiny and review can create an issue between governments' transparency and accountability and protecting the data and algorithms that are used to make decisions. Making the algorithm public can allow for scrutiny but this can also reduce immigration decisions to a predetermined step-by-step process that can be 'played' by some applicants who may try to gain points either by pursuing a certain job or course of study. On the other hand, if algorithms remain closed to scrutiny, many parts of the immigration system can become obscure and it could be challenging to keep the government accountable and understand if the right decisions were made. Given the already limited safeguards and procedural justice protections in immigration and refugee decisions, the use of potentially discriminatory and biased algorithms have profound ramifications on a person's safety, life, liberty, security, and mobility. Attempting to reduce human mobility into an algorithm is not easy and there are no external metrics for accuracy in regard to refugee and status determination.

In light of the above, a lack of a legal framework to guide the Canadian government's use of AI can have several interrelated implications such as bias and data issues and an increasing role of private companies in immigration-related governance, all of which can contribute to the abuse of human rights. By assuming that these technologies are unbiased and cannot perpetuate discriminatory practices, AI technologies risk reducing government's accountability for the decisions it makes on asylum and immigration applications. These issues can increase the 'fortification' of 'invisible border walls' and can act as additional non-entrée tactics that are used to exclude 'undesirable' migration.

Limitations of AI

AI bias

The use of AI technologies in the immigration sphere promises to significantly reduce or even eliminate conscious and subconscious forms of human bias which can lead to unwanted outcomes. Notwithstanding the many concerns that AI technologies pose, pilot AI technologies continue to be tested on vulnerable groups of people, such as asylum seekers, non-economic and humanitarian migrants. As discussed above, algorithmic bias is when AI technologies arrive at decisions that are discriminatory despite them being designed to be impartial. There are several sources of algorithmic bias, such as bias autonomously generated by the algorithm, human bias and issues with the way data was collected.

Bias autonomously generated by algorithms occurs when automated decision-making systems, which are built by analyzing thousands of past applications and their outcomes, semi-autonomously 'learn' by detecting patterns in the data (Keung, 2017). Due to the semi-autonomous nature of algorithms, they can diverge from their intended purpose; this issue can pose significant challenges especially if this problem goes undetected. The obscure nature of immigration and refugee decision-making creates an environment that can be perfect for such algorithmic discrimination. Further, AI has the capacity to become racializing, in part because AI can compound already entrenched disadvantages and even develop new ways to discriminate.

Human bias and issues with the way data was collected are already occurring in Canada. In 2017, without any clear rationale and apparently on its own initiative, the Royal Canadian Mounted Police (RCMP) collected questionnaires from around 5,438 asylum seekers featuring questions clearly coloured by Islamophobic stereotypes (Peritz and Leblanc, 2017; Shepherd,

2017). 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 (Shepherd, 2017). The questions targeted Muslim individuals crossing the border, as no questions were included about other religious practices or terrorist groups (Shepherd, 2017). The collected answers were entered into an RCMP database which could be shared with CBSA and "other security partners" (Shepherd, 2017).

Yet another example of unethical data collection occurred in 2018, when it was reported that the CBSA used private third-party DNA services such as Ancestry.com to establish the nationality of individuals subject to potential deportation (Khandaker, 2018). This is deeply concerning for several reasons. First, one's DNA is not related to nationality and should bear no impact on one's application. The second concern is the coercive nature of privacy invasion - individuals who submitted their DNA samples to these companies might not have given consent or knew that their data could be used by governments. Further, there is no certainty that the data and DNA given by individuals is accurate and is theirs. As such, collecting and basing immigration and border control decisions on data collected by private companies can be unethical as they can be based on inaccurate information. Even if the Canadian government is not using this method of data collection anymore, DNA samples could provide us with new information in the future and it could be used by governments in ways that we cannot imagine today.

This CBSA example also presents issues of making sense of copious amounts of data and the need for advanced analytical capacities to process and filter data – in other words – the political economy of 'datafication'. This includes the collection of large volumes of data, and the extent to which Canadian government agencies outsource technologies for surveillance and border control and buy technologies and data from private domestic and foreign companies. Where such capacities exist, private companies typically own them, and this also presents issues around accountability, sovereignty, privacy, and data ownership. Statistics and data are often attributed the quality of offering transparency, and thus, insight and true knowledge. Upon further analysis, Hansen (2015) contends that numbers are not always identical to the world they are trying to depict and are rather forms of abstractions. Drucker and Grumpet (2007) and Roberts (2009) suggest that full transparency – meaning unmediated and unfiltered human access to reality – is an illusion. Data and numbers are signs, similar to words and photographs, which can represent people, objects, and relationships, with

implications for those who take the authority of the representations for granted and for those who contest them. For example, Google Inc. makes a large amount of data available for public use. However, the calculations and the algorithms that determine what its search engine presents on our screens is hidden. This brings up questions on what is kept secret by private companies that design AI and collect data.

Earlier, it was mentioned that algorithms can be political in nature, which is in part due to the data that they are built with. Data and AI algorithms have the capacity to have an instrumentally oriented angle, an ensemble of policy-relevant mechanisms that are embedded in coercive, economic, institutional and normative forms of power and authority structures. Numerical descriptions of certain social phenomena entail an objectification of these phenomena. Depending on the situation, data and algorithms may serve to depoliticize particular matters, but they can also help to re-politicize social issues, by making visible injustice and facilitating criticism (Bruno et al., 2014). Considering revelations made in the history of numbers, media and surveillance studies, and theories of governance, suggest that numerical operations constitute a tool for governing the present (Hacking, 2007; Miller and Rose, 2008). Future research needs to focus on the link between numerical operations and the forms of transparency they produce, as well as how and what exactly these operations make transparent.

Finally, collection of data and its storage in a centralized database can pose a risk as governments or private companies could request or steal access to the databases and repurpose it for law enforcement, surveillance, or national security screening (Idris, 2019). Data could also be sold for profit by hackers or used to publicly embarrass and undermine humanitarian and legitimate government efforts. For example, Edward Snowden revealed that U.S. and U.K. intelligence agencies targeted humanitarian organisations like UNICEF, UNDP, and Medecins du Monde for surveillance (BBC, 2014). As such, there is a debate on not only who owns the data, but who is responsible for protecting it.

Public- private partnerships

The private sector plays an important role during a migrant's journey from origin to their destination. The private sector, which not only includes cybersecurity and technology companies, but also financial institutions, recruitment agencies, private education and training institutions, telecommunications services, transport providers, to name a few, all play a role not only in influencing migration patterns but also either help migrants generate data or they

collect migrants' data. Private actors have at least four roles in relation to migration: to provide goods and services to migrants and asylum seekers; to provide services to governments in support of migration governance and in some cases on behalf of the government; to provide employment to migrants; and to lobby to influence migration policies and legislation thus influencing migration governance. Despite the benefits that this sector brings to migrants, there is a serious risk that continues to exist around the role private companies are taking in migration governance through the use of AI technologies.

The lack of technical capacity within governments and the public sector can lead to potentially inappropriate over-reliance on technology companies that designs AI. The first issue to be mindful of is the extent to which government agencies outsource technologies for surveillance and border control and buy technologies and data from private domestic and foreign companies. This issue can pose additional concerns for governments such as accountability, sovereignty, privacy, data ownership, and transparency. When using AI technologies, it is vital to know who is responsible for each element of decision-making; who handles and has access to the data, the algorithms, and the technology; and how the designers and owners of the technology will be held accountable for the misuse of the data and for wrongful decision-making.

The increasing number of collaborations between Canadian government immigration agencies and foreign technology companies can create opportunities not only for espionage but also increase the influence of foreign governments on the Canadian immigration system. For example, Palantir Technologies, a controversial U.S. software company partnered up with the Canadian Department of National Defense to provide data analytics software for the Canadian Forces Special Operations Command and the Calgary Police Department to integrate their database (Braga, 2017; Hemmadi, 2019). This partnership is problematic as Palantir's chairman and co-founder Peter Thiel is an adviser to the U.S. President. Further, Palantir recently set up an office in Canada and hired David MacNaughton, the former Canadian ambassador to the United States (2016-2019), as the head of the Canadian wing of Palantir. A United Arab Emirates-based private tech company that focuses on cybersecurity, DarkMatter, also set up an office in Toronto, Canada in 2016 (DarkMatter, 2016). DarkMatter is also a controversial company and is currently under investigation by the U.S. Federal Bureau of Investigation for engaging in crimes related to espionage, murder, and incarceration of foreign nationals (Mazzetti et al., 2019).

In 2014, the Canadian Cyber Incident Response Centre (CCIRC) reported that the Canadian government partnered up with an unnamed private foreign company which was housing a significant number of Canadians' personal data (for unknown reasons), experienced a cyber attack (Ling, 2015). The malware creators demanded an undisclosed sum of money for the information on 5,000 Canadian passport applicants in the process and threatened to encrypt the data forever if the demands were not met. The CCIRC indicated that recovering files was not likely to happen and paying the ransom would not guarantee the retrieval of the files. The report did not indicate what happened to the 5,000 passport applications nor why the IRCC, the department responsible for passport applications gave this private foreign company access to this data.

Rather than developing their own AI algorithms and technologies, governments can subcontract the development and maintenance of these technologies to the private sector. This, however, will increase the participation of domestic and foreign private companies in migration governance. Technologies and algorithms created by private companies are often proprietary (closed-source software) and protected as trade secrets. This can create issues of ownership and ethical decision-making, thus resulting in obstacles to harnessing the potential of big data for public policy. Since AI tools are essentially black boxes, it can be difficult to evaluate and correct for any potential biases they may perpetuate. Developing 'in-house' AI programs and decision-making systems can reduce the number of non-governmental agencies that have access to the data and algorithms as well as the role that private companies have in migration governance. Further, this can increase government expertise in project and operation management, helping the government to ensure that the principles and standards of regulation of public service delivery are open for scrutiny, potentially leading to greater accountability for decision-making.

AI and 'invisible border walls'

The discussions presented above converge in the main argument of this working paper – introducing AI into the decision-making on immigration and border control has the potential to supplement Canada's non-entrée policies, such as visa control and extradition practices, to fortify 'invisible border walls' – a new generation of non-entrée strategies. The overarching logic of this new generation of non-entrée strategies can be to insulate governments from liability, the legal responsibilities for refugee protection and accountability for decision-making, while presenting its immigration system as one that is based on the use of AI technologies

that eliminate human bias. The end result is that deterrence of unwanted migration is achieved while liability is generally avoided.

The issues of bias and the role of private companies have the potential to culminate in the making of the Canadian immigration and refugee system that is a high-risk experiment which can pose great problems for human rights violations. A lot of government work is discretionary in nature; attempting to make decisions using AI raises serious concerns for the protection of human rights for vulnerable individuals like non-citizens, asylum seekers, and marginalized individuals who often have weak human rights protections and few resources that they can use to defend their rights. Decisions that are based on AI might be either challenging to explain or can have undetected biases. As such, when considering the use of AI technologies, it is important to consider the 'explainability' of the technology used - if the government cannot explain how the technology reached a particular decision, there is a potential for accountability issues. This may place highly vulnerable individuals at risk of being subjected to unjust and unlawful processes in a way that threatens to violate Canada's domestic and international human rights obligations.

AI build on previous cases (precedents) to predict and generate new decisions which risks the perpetuation of discriminatory and flawed reasoning, especially if these technologies and their algorithms are not continuously scrutinized. It is gravely important that the Canadian government develops a framework for transparency and accountability to address bias in relation to the use of AI not only because these technologies can perpetuate human bias but they can develop their own ways of discriminating. However, greater transparency might not lead to greater civic involvement and response. The problem is that too often in practice greater transparency simply means shifting responsibility for oversight and accountability to individuals already limited in time and resources. Further, the consequences of using AI in the sphere of immigration and refugee law and policy are far-reaching and may aid in the expulsion and externalization of asylum seekers and 'undesirable' migrants, while a data breach can harm applicants by exploiting and exacerbating their vulnerabilities in crisis situations.

Few governments have national regulations for the use of AI and there is no robust international document that governs the use of these technologies in the humanitarian sphere (Gammeltoft-Hansen and Hathaway, 2015). A lack of such policies has the potential to allow for the abuse of AI technologies to assist with the reinforcement of non-entrée practices which are forbidden by Article 33 of the *1951 Refugee Convention*. AI could become a political

tool that is used to reinforce state practices that are aimed at curbing international migration and preventing certain individuals from reaching state territories. For example, the UNHCR began sharing records including fingerprints, iris scans, and facial biometrics of refugees it recommended for resettlement consideration in the U.S. with the country's Citizenship and Immigration Services (Burt, 2019). UNHCR sent tens of thousands of profiles to U.S. federal agencies each year, including those who did not actually come to the U.S. (Burt, 2019). What the U.S. government does with the profiles of those who never make it to its territories is unclear. Further, the risk of breaches grows with the number of organizations and jurisdictions that ask for access to the data to provide humanitarian and government services. Considering this, the use of these technologies should be halted until they are no longer experimental in nature and robust governing standards are established on national and international levels.

Using AI without having a robust regulatory and legal framework to oversee the use of AI can result in the fortification of a border wall that is aimed at preventing certain type of migration into Canada. If the Canadian government uses algorithms that are impossible to explain, this border wall can become invisible and be closed to public scrutiny. The Canadian government already uses a number of policies to control who enters and gains the privileges of being a member of the Canadian community by expelling unwanted migrants, externalizing borders, scrutinizing people on the move, implementing visa regimes, practicing containment, and adopting safe third country agreements. Using AI can modernise Canada's non-entrée policies by making them high-tech and more efficient at making discriminatory decisions, thus potentially erecting 'invisible border walls'. Using automated decision-making systems can hide Canada's immigration system behind the veil of accountable, fair, and unbiased AI technologies and algorithms. Paradoxically, migrants fleeing their country of origin for fear of persecution are ultimately stripped of even more of their human rights when met with unethical AI-based immigration enforcement practices.

As the Canadian government continues to seek new AI technologies designed to surveil, make decisions on immigration-related applications, and manage borders, migration has the potential to become even more unequal for some groups. Unfortunately, some prospective migrants never reach the step of risk analysis in the visa system or at the border. Being part of the 'Five Eyes' group, Canada shares applicant information such as visa rejections with the U.S., the U.K., Australia, and New Zealand (Greenfield, 2020). These governments use AI to create hypothetical risk profiles based on unwanted behaviour such as crimes or visa overstays. These profiles might mask systemic discrimination against specific groups of people

(Arbel, 2013). In addition, these countries share 'risky profiles' with contracted visa processors and consulates as guidance for the types of travellers that should be rejected or flagged prior to even obtaining a visa. Without even knowing it, a potential traveller's proximity to such profiles can unfairly keep them from accessing regular channels of migration. Sharing such information with other countries might be problematic considering the differences in how governments screen asylum applications and who they deem to be an unwanted and risky migrant.

While the collection and sharing of large amounts of data poses concerns for migrants, information precarity also separates those who can be mobile and those who cannot. Information precarity can affect potential migrants who do not have enough data on them to share in order to migrate and seek asylum. This is of great concern to those who do not have internationally accepted identification documents or lack financial records, disproportionately affecting the elderly, women, more rural, and less formally educated people in developing and poorer countries which are already disadvantaged by the global AI-divide. However, even those who have internationally recognized identification and enough information about them can also face challenges as their data can match too closely to the algorithm-created risk profile. Risk analysis is predicated on perceived and anticipatory threat; if one government's algorithm assumes this, a negative decision may be shared with another government, especially as these programs become more integrated as is the case with the 'Five Eyes' allies.

Additionally, the degree of personal information that AI technologies give government agencies can put vulnerable individuals, such as asylum seekers and migrants at a greater risk of invasion of privacy, especially if these individuals are not fully aware of their rights. Making asylum seekers and migrants aware of the risks that AI-powered technologies like digital identities and digital cash transfers bring may either not be possible or may be challenging for several reasons. Even if these individuals are asked for consent, for many it might be a difficult choice to make – either give up personal data and risk it being stolen and/or used for surveillance or refuse refuge. In such situations, consent might no longer be freely given as there would be a strong incentive to agree to give away one's personal data. In many current uses of AI government agencies do not ask for consent.

Despite the increasing use of AI and related technologies in the immigration space at national and international levels, Canada lacks a dedicated network of stakeholders that are tasked with investigating the potential of new data sources for the analysis of migration-related

activities. While the regulations must be robust enough to limit data breaches, privacy issues, and ensure accountability, there must also be ethical standards by which the use of these technologies is governed. In May 2019, the Minister of Innovation, Science and Economic Development announced the launch of the Advisory Council on Artificial Intelligence. While this is a start to developing Canada's robust approach to using AI by immigration agencies, there is no Canadian third-party ethics oversight agency that supervises the use of automated decision systems by the Canadian government. This body must be impartial and at arms-length and be allowed to oversee all aspects of the system as well as test and audit algorithms and source codes.

In addition to an oversight body, there must be a set of regulations that would govern the use of AI technologies and how the Canadian government partners up not only with private companies but also with humanitarian agencies. It is important to consider how the Canadian government works with humanitarian agencies not only because the humanitarian sector also lacks a robust set of ethical and legal standards by which to govern the use of AI, but also because in 2019, the UNHCR launched its first global strategy on digital ID in partnership with IRCC (UNHCR, 2019). In 2020-2021, IRCC will test a digital service channel aimed at improving client communications and at increasing IRCC's ability to digitally capture client data. This project intends to enhance the identification of risks and trends and lead to improved data integrity and efficiency. The lack of robust governing standards and an oversight body that is accountable to Canadians is especially problematic since the impacts of AI are not fully known on human rights.

Further research can address if using AI technologies, can address the fundamental issues with an immigration system, especially one that actively relies on non-entrée policies. This is deeply problematic and an issue of human rights that goes beyond the lack of privacy of data, accountability, and the increasing role of private companies.

Conclusion

As the Canadian federal government continues to invest in the use of AI technologies in the immigration sphere, there are many benefits to be gained from their use. However, without proper oversight, AI can produce discriminatory and stereotypical decisions that will perpetuate and/or create new biases based on appearance, religion, or travel patterns, leading to erroneous and misleading proxies for more relevant data, thus entrenching bias into a seemingly 'neutral' tool. The nuanced and complex nature of many refugee and immigration

claims may be lost on these automated technological decision-makers, leading to serious breaches of internationally and domestically protected human rights, such as the right to privacy and consent, the right to due process, and the right to be free from discrimination. Continuing to experiment with AI on vulnerable groups of people without implementing a human rights-centered framework and an agency that will oversee the use of AI impact assessments is a high-risk problem that can severely tarnish Canada's reputation as a refugee welcoming country and strip migrants of even more of their human rights. perhaps AI might never achieve the goal of being bias-free as long as it continues to be used in the current immigration system, which some consider to be fundamentally discriminatory and biased (Dauvergne, 2004; Macklin, 2005; Gammeltoft-Hansen and Hathaway, 2015).

References Cited

Arbel, E. 2013. Shifting borders and the boundaries of rights: Examining the Safe Third Country Agreement between Canada and the United States. *International Journal of Refugee Law*, 25(1): 65-86.

Bansak, K. et al. 2018. Improving refugee integration through data-driven algorithmic assignment. *Science*, 359(6373): 325-329.

Basok T. and Simmons A. 1993. "A review of the politics of Canadian refugee selection", in Robinson V. (ed.). *The International Refugee Crisis.* London: Palgrave Macmillan, 132-157

Baynes, C. 2018. "Government 'deported 7,000 foreign students after falsely accusing them of cheating in English language tests'". *Independent.co.uk*. Available at: https://www.independent.co.uk/news/uk/politics/home-office-mistakenly-deported-thousands-foreign-students-cheating-language-tests-theresa-may-a8331906.html [Accessed 5 July 2020].

BBC. 2014. "Edward Snowden: Leaks that exposed US spy programme". *BBC*. Available from: https://www.bbc.co.uk/news/world-us-canada-23123964 [Accessed 12 May 2020].

Beduschi, A. 2018. "The big data of international migration: Opportunities and challenges for states under international human rights law". *Georgetown Journal of International Law*, 49(2): 982-1017.

Braga, M. 2017. "A secretive Silicon Valley tech giant set up shop in Canada. But what does it do?". CBC.ca. *CBC/Radio-Canada*. Available at: https://www.cbc.ca/news/technology/palantir-silicon-valley-technology-giant-data-canada-1.4111163/ [Accessed 1 June 2020].

Bruno, I. et al. 2014. Statactivism: forms of action between disclosure and affirmation. *Partecipazione e Conflitto* 7(2): 198–220.

Burt, C. 2019. "DHS to store tens of thousands of refugee biometric records from UNHCR". Biometric Update. *Biometrics Research Group*. Available at: https://www.biometricupdate.com/201908/dhs-to-store-tens-of-thousands-of-refugee-biometric-records-from-unhcr [Accessed 16 May 2020].

Calo, R. 2017. Artificial Intelligence policy: A primer and roadmap. *UC Davis Law Review*, 51: 399-435.

Carammia, M. and Dumont, J.-C. 2018. "Can we anticipate future migration flows?" *Paris: OECD*. Available at: https://www.oecd.org/els/mig/migration-policy-debate-16.pdf [Accessed 2 July 2020].

Cecco, L. 2019. "Canada took in more refugees than any other country in 2018, UN says". *The Guardian*. Available at: https://www.theguardian.com/world/2019/jun/19/canada-refugees-resettlement-un-report-2018 [Accessed 3 July 2020].

Connor, P. 2017. The Digital Footprint of Europe's Refugees. Washington D.C.: Pew Research Center. Available at: https://www.pewresearch.org/global/2017/06/08/digital-footprint-of-europes-refugees/ [Accessed 4 July 2020].

DarkMatter. 2016. "DarkMatter inaugurates R&D centre based in Toronto, Canada". Newswire.ca. *CNW Group Ltd*. Available at: https://www.newswire.ca/news-releases/darkmatter-inaugurates-rd-centre-based-in-toronto-canada-575528221.html [Accessed 4 June 2020].

Dauvergne, C. 2004. *Humanitarianism, identity, and nation: Migration laws in Canada and Australia*. Vancouver: UBC Press.

Ferguson, A. 2017. *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York: NYU Press.

Gallagher, R. and Jona, L. 2019. We Tested Europe's New Lie Detector for Travelers - And Immediately Triggered A False Positive. Theintercept.com. *First Look Media*. Available At: https://theintercept.com/2019/07/26/Europe-Border-Control-Ai-Lie-Detector/ [Accessed 21 September 2020].

Gammeltoft-Hansen, T. and Hathaway, J. C. 2015. Non-refoulement in a world of cooperative deterrence. *Columbia Journal of Transnational Law*, 53(2): 235-284.

Greenfield, C. 2020. "As governments build advanced surveillance systems to push borders out, will travel and migration become unequal for some groups?". Migrationpolicy.org. *Migration Policy Institute*. Available at: https://www.migrationpolicy.org/article/governments-build-advanced-surveillance-systems [Accessed 23 June 2020].

Hacking, I. 2007. Kinds of people: moving targets. *Proceedings of the British Academy*, 151: 285-318.

Hansen, H. K. 2015. Numerical operations, transparency illusions and the datafication of governance. *European Journal of Social Theory*, 18(2): 203–220.

Harwell, D. and Miroff, N. 2018. "ICE just abandoned its dream of 'extreme vetting' software that could predict whether a foreign visitor would become a terrorist". *The Washington Post.* Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/ [Accessed 2 May 2020].

Hemmadi, M. 2019. Controversial data-mining firm Palantir signs million-dollar deal with defense department". TheLogic.co. *The Logic Inc.* Available at: https://thelogic.co/news/exclusive/controversial-data-mining-firm-palantir-signs-million-dollar-deal-with-defence-department/ [Accessed 1 June 2020].

Idris, I. 2019. "Benefits and risks of Big Data Analytics in fragile and conflict affected states". *Helpdesk Report.* Available at: https://reliefweb.int/sites/reliefweb.int/files/resources/605_Benefits_and_Risks_of_Big_Data_Analytics_in_Fragile_and_Conflict_Affected_States__FCAS_.pdf [Accessed 12 May 2020].

IOM. 2018. "Big Data and Migration. Geneva: IOM". Available at: https://publications.iom.int/books/data-bulletin-informing-global-compact-migration-big-data-and-migration-issue-5-february-2018 [Accessed 4 July 2020].

Keung, N. 2017. "Canadian immigration applications could soon be assessed by computers". *Toronto Star*. Available at: https://www.thestar.com/news/immigration/2017/01/05/immigration-applications-could-soon-be-assessed-by-computers.html [Accessed 16 May 2020].

Khandaker, T. 2018. "Canada is using ancestry DNA websites to help it deport people". *Vice*. Available at: https://www.vice.com/en_ca/article/wjkxmy/canada-is-using-ancestry-dna-websites-to-help-it-deport-people [Accessed 3 July 2020].

Lacroix, M. 2004. Canadian refugee policy and the social construction of the refugee claimant subjectivity: Understanding refugeeness. *Journal of Refugee Studies*, 17(2): 147-166.

Ling, J. 2015. "Hackers held data on 5,000 Canadians hostage and the government didn't tell anyone". *Vice*. Available at: https://www.vice.com/en_us/article/ney34z/hackers-held-data-on-5000-canadians-hostage-and-the-government-didnt-tell-anyone [Accessed 10 June 2020].

Margetts, H. and Dorobantu, C. 2019. Rethink government with AI. *Nature*, 568(7751): 163-165.

Mazzetti, M. et al. 2019. "A new age of warfare: How Internet mercenaries do battle for authoritarian governments". Nytimes.com. *The New York Times Company*. Available at: https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.htm [Accessed 5 June 2020].

Miller, P. and Rose, N. 2008. *Governing the Present*. Cambridge: Polity Press.

Molnar, P. and Gill, L. 2018. "Bots at the gate: A human rights analysis of automated decision-making in Canada's immigration and refugee system". *International Human Rights Program and the Citizen Lab*. Available at: https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf [Accessed 25 May 2020].

Na, L. et al. 2018. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. *Journal of the American Medical Association, 1(8): 1-13*.

Ng, V. 2017. "Algorithmic decision-making and human rights". *The human rights, big data, and technology project*. Available at: https://www.hrbdt.ac.uk/algorithmic-decision-making-and-human-rights/ [Accessed 17 May 2020].

Pedrozo, S. 2017. Swiss military drones and the border space: a critical study of the surveillance exercised by border guards. *Geographica Helvetica*, 72(1): 97–107.

Rango, M. 2015. "How big data can help migrants" (Washington D.C., 2015). Available at: https://www.weforum.org/agenda/2015/10/how-big-data-can-help-migrants [Accessed 23 April 2020].

Tecuci, G., 2012. Artificial intelligence. *Wiley Interdisciplinary Reviews: Computational Statistics*, 4(2): 168-180.

UKGOS. 2016. "Artificial intelligence: Opportunities and implications for the future of decision making". *The Government of United Kingdom*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf [Accessed 1 May 2020].

UNHCR Innovation Service. 2019. "A goat story". *Medium*. Available at: https://medium.com/unhcr-innovation-service/a-goat-story-3ed6bdd2b237 [Accessed 2 May 2020].

UNHCR. 2014. "The right to privacy in the digital age". A/HRC/27/37 Available at: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf [Accessed 23 June 2020].

UNHCR. 2019. "Global virtual summit on digital identity for refugees". *UNHCR.org*. Available at: https://www.unhcr.org/idecosystem/wp-content/uploads/sites/69/2019/12/Conclusions_and_Recommendations.pdf [Accessed 22 June 2020].

Walsh, B. 2020. "How an AI grading system ignited a national controversy in the U.K". *Axios Media*. Available from: https://www.axios.com/england-exams-algorithm-grading-4f728465-a3bf-476b-9127-9df036525c22.html [Accessed 23 September 2020].

Wright, T. 2018. "Canada's use of artificial intelligence in immigration could lead to break of human rights: Study". Available at: https://globalnews.ca/news/4487724/canada-artificial-intelligence-human-rights/ [Accessed 25 June 2020].

Macklin, A. 2005. Disappearing refugees: Reflections on the Canada-Us Safe Third Country Agreement. *Columbia Human Rights Law Review*, 36: 365-426.

Drucker, S. J. and Gumpert, G. 2007. Through the looking glass: illusions of transparency and the cult of information. *Journal of Management Development,* 26(5): 493–98.

Roberts, J. 2009. No one is perfect: the limits of transparency and an ethic for 'intelligent' accountability. *Accounting, Organization and Society,* 34(2009): 957–70.

Shepherd, M. 2017. "RCMP will redact more than 5,000 records collected using questionnaire targeting Muslim asylum seekers". *Toronto Star*. Available at: https://www.thestar.com/news/canada/2017/11/27/rcmp-will-redact-more-than-5000-

records-collected-using-questionnaire-targeting-muslim-asylum-seekers.html [Accessed 2 June 2020].

Peritz, I. and Leblanc, D. 2017. "RCMP accused of racial profiling over 'interview guide' targeting Muslim border crossers", *The Globe and Mail*. Available at: https://www.theglobeandmail.com/news/national/rcmp-halts-use-of-screening-questionnaire-aimed-at-muslim-asylum-seekers/article36560918/ [Accessed 10 June 2020].

Immigration and Refugee Protection Act (IRPA) [Canada], SC 2001, c. 27, 1 November 2001. Available at: https://www.refworld.org/docid/4f0dc8f12.html [Accessed 31 May 2020].

Daniels, J. 2018. "Lie-detecting computer kiosks equipped with artificial intelligence look like the future of border security". *CNBC*. NBCUniversal. Available at: https://www.cnbc.com/2018/05/15/lie-detectors-with-artificial-intelligence-are-future-of-border-security.html

Aradau, C. and Tazzioli, M. 2020. Biopolitics Multiple: Migration, Extraction, Subtraction. *Millennium*, 48(2): 198-220.