Facial Recognition at a Crossroads: Transformation at our Borders & Beyond

Report Overview

Tamir Israel, Staff Lawyer
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (**CIPPIC**)

September 2020

Electronic version first published by the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic.

Version 1.2, September 30, 2020

An electronic version of this overview can be obtained at:
https://cippic.ca/uploads/FR_Transforming_Borders-OVERVIEW.pdf

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic

University of Ottawa, Faculty of Law, Common Law Section
57 Louis Pasteur Street
Ottawa, ON K1N 6N5
Website: https://cippic.ca
Email: admin@cippic.ca
Twitter: @cippic

ABOUT THE AUTHOR & CIPPIC

Tamir Israel is Staff Lawyer at the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), a technology law clinic based at the University of Ottawa, Centre for Law & Technology.

ABOUT THIS REPORT

This overview consists of key and unaltered excerpts from the primary report by the same title. Internal references to page numbers and sections are to the primary report, which can be found at: https://cippic.ca/uploads/FR_Transforming_Borders.pdf

CORRECTIONS & QUESTIONS

Please send all questions and corrections to the author directly, at: tisrael@cippic.ca

KEY TERMS & ABBREVIATIONS

Biometric	A numerical representation of a biographic feature of an individual, such as their face, their fingerprint or their voice.
Facial Identification	The act of identifying an individual on the basis of facial biometric information.
Facial Verification or Authentication	The act of verifying or authenticating an individual's identity on the basis of facial biometric information against an identification claim such as that contained in a passport or identification badge.
Facial Recognition	The task of identification or verification on the basis of facial biometrics.
Facial Image Template	A numerical representation of an individual's face generated from a live or recorded image.
Facial Image Probe	An individual's facial template used to query a facial recognition system and compared against one or many historically stored facial reference samples.
Facial Reference Sample	An individual's historical facial template stored with associated enrollment data.
Enrollment data	Data, typically identification data (name, address, passport number) associated with a facial reference sample.
Facial Capture	Recording a facial sample, either directly from an individual (i.e. through a digital camera) or from a representation of an individual (a certified photograph sent by the individual).
Face Detection	An automated algorithmic process designed to identify and isolate faces in static images or live video recordings.
Facial Recognition Claim	A claim that an individual is or is not the source of a facial reference sample or, alternatively, that the individual traveler could not be matched.
Facial capture subject [traveller]	The 'capture subject' refers to an individual that the facial recognition system is attempting to compare to a facial reference sample in order to determine whether said individual is the source of the reference sample. Often referred to as 'traveller' in the context of this report.
False Match Rate (FMR)	The rate at which a matching algorithm generates false positives by comparing two facial images and incorrectly indicating both are from the same individual.
False Non-Match Rate (FNMR)	The rate at which a matching algorithm generates false negatives by comparing two facial images and incorrectly indicating that they are not from the same individual.
False Positive Identification Rate (FPIR)	The rate at which a matching algorithm generates false positives by comparing one facial image probe to a series of facial image reference samples, incorrectly indicating that the facial probe and one of the reference samples are from the same individual.
False Negative Identification Rate (FNIR)	The rate at which a matching algorithm generates false positives by comparing one facial image probe to a series of facial image reference samples, incorrectly indicating that the facial probe and one of the reference samples are not from the same individual.
False Positive	Within the context of this report, the term false positive is used inclusively, without distinction as to whether FMR or FPIR are at issue.

False Negative	Within the context of this report, the term false negative is used inclusively, without distinction as to whether FNMR or FNIR are at issue.
Failure to Acquire Rate (FtAR)	The rate at which a facial recognition system fails to detect or capture a facial image of sufficient quality to attempt a comparison. Image quality thresholds are set by policy. FtAR is subsumed within FNMR and FNIR.
Operational Rejection Rate (ORR)	The rate at which travellers are referred to manual processing, regardless of the cause. This includes considerations extraneous to facial recognition itself, such as the number of travellers who are not enrolled in a system and the number who must be manually processed due to legal reasons. It provides a complete measure of the efficiency of an automated processing system that is reliant on facial recognition.
True Acceptance Rate (TAR)	The rate at which travellers are accurately matched to their images by a facial recognition system. TAR is the inverse of a system's false negative rate.
Automated Border Control Systems (ABC)	Automated Border Control systems refer to any physical infrastructure that forms a component of a recognition-enabled border control system.
e-Gate	In this report, 'e-Gate' is specifically used to refer to automated physical barriers with an integrated facial recognition capability.
Primary Inspection Kiosk (PIK)	A facial recognition-enabled booth used specifically in Canadian border crossings to automate customs and immigration processing.
CBP	*United States Customs and Border Protection*
CBSA	*Canadian Border Services Agency*
DHS	United States Department of Homeland Security
eu-LISA	*European Union Agency for Large-Scale IT Systems in the Area of Freedom, Security and Justice*
FRONTEX	*European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union*
International Civil Aviation Organization (ICAO)	A United Nations specialized agency that develops consensus on international standards, norms and recommended practices relating to, among other things, travel documents.
IRCC	*Immigration, Refugee and Citizenship Canada*
IRPA	*Immigration and Refugee Protection Act*
IRPR	*Immigration and Refugee Protection Regulations*, issued under the *Immigration and Refugee Protection Act*
NIST	*United States, Department of Commerce, National Institute of Standards and Technology*

Overview & Key Observations

Facial recognition is currently experiencing rapid levels of adoption and expansion in border control contexts. The technology has serious potential for negative impact on human rights. In many jurisdictions, facial recognition systems adopted at the border are in the process of being repurposed to achieve many unrelated public and private sector objectives. While steps can be taken to mitigate the detrimental impact of facial recognition at the border and beyond, the significant negative impacts of the technology strongly suggest that current and ongoing use of facial recognition in border control contexts is disproportionate.

Key Findings

Facial recognition is an inherently invasive biometric system that can have wide-ranging implications for human rights through its ability to identify otherwise anonymous individuals and pervasively link them to rich digital profiles. The surreptitiousness of the technology and its ability to operate from a distance creates a powerful identification capability. Facial recognition also provides a means of mapping digital functionality to the physical world by providing the means by which individuals can be persistently identified at a distance.

The technology remains prone to errors and racial biases, while maintaining sufficient levels of accuracy and obscurity in operation to generate a level of trust that becomes difficult to dislodge. Depending on the context of its employment, the results of this paradigm can exacerbate historical prejudices at a systemic level while having devastating impact on individuals who are misidentified. When adopted in border control settings, facial recognition technologies are too often repurposed to achieve a range of broader public and private objectives. At the same time, the benefits and efficiencies of facial recognition systems in border control contexts are often overstated. The proportionality of adopting new facial recognition systems is difficult to establish and the justification for existing systems must be rigorously re-evaluated.

Facial recognition is currently enjoying rapid deployment in border crossings around the world. Driving the current push for greater adoption are a number of social and technological factors. Technologically, the cost of high-quality video cameras has become sufficiently low as to allow their wide-spread deployment. At the same time, facial recognition capabilities have advanced to provide sufficient levels of accuracy to justify their use in terms of efficiency. Socially, it is perceived that facial recognition generally enjoys lower resistance than other forms of biometrics. In part, this is due to the fact that facial recognition systems can be developed and applied remotely, with minimal active involvement by the individuals being recognized. Facial recognition systems also lack the association between criminal suspicion and biometric enrolment that is evoked by other biometrics (e.g.

fingerprinting) for individuals in some jurisdictions. There is, additionally, the perception that public acceptance of these technologies has improved, a change in sentiment that is often attributed to broader consumer adoption of biometric authentication in handheld devices. [Section 2][pages 79-80]

> **“ Facial recognition benefits from the wide availability of high-performance, low-cost, and commercially available camera systems that could be extended, in collaboration with aviation security partners, across the entire passenger experience from reservation to boarding.**
>
> **– United States Government, TSA Biometric Roadmap, September 2018**

The benefits of facial recognition will depend on the specific border control task the technology is called upon to facilitate. Frequently, the goal is greater efficiency in processing travellers, an objective where facial recognition can achieve tangible benefits in border control settings. These efficiency gains are largely achieved by automating manual travel document verification, reducing staffing costs and allowing for more rapid processing of travellers. However, these efficiency gains are often overstated when the proportionality of the technology is assessed. Often, gains in efficiency are assessed without consideration of alternative, less invasive steps that can be taken to improve efficiency. The real-world operation environment for these systems is also often discounted. A facial recognition system that is theoretically capable of accurately verifying the travel documents of 98% of travellers may only be able to process 85% of all real-world travellers. The discrepancy may result from an inability to accurately process various age groups (younger and older travellers are often categorically excluded) or immigration requirements that require manual vetting. While some of these factors may be extraneous to the facial recognition system itself, they nonetheless directly impact its ability to provide real-world efficiency and cannot be ignored when assessing the proportionality of a proposal. Real-world scale is also a factor—a 2% error rate will yield thousands of false outcomes per day if applied to all travellers [Sections 1.3.5 and 1.3.6]

Against these drivers, facial recognition technologies are presented as providing more efficient border control and enhanced security. While the deployment of facial recognition technologies in border control scenarios can lead to some efficiency gains, the threat posed by facial recognition systems to privacy and other human rights is both tangible and insidious.

> **“ Face recognition … takes the risks inherent in other biometrics to a new level because it is much more difficult to prevent the collection of an image of your face. We expose our faces to public view every time we go outside,**

> **and many of us share images of our faces online with almost no restrictions on who may access them. Face recognition therefore allows for covert, remote, and mass capture and identification of images.**
>
> **– Electronic Frontier Foundation, "Face Off", February 2018**

All biometric techniques raise privacy concerns, arising from their potential to persistently and universally identify individuals. Facial recognition has potential for higher levels of invasiveness than other forms of biometric recognition (premised on DNA, fingerprints, or iris scans, for example), which are more difficult to implement in a manner that is at once fully automated, surreptitious and pervasive. For example, fingerprint-based border controls are disruptive in their collection in that individuals must actively provide fingerprints whereas facial images are already a standard component of most passports. Fingerprint-based controls are also disruptive to implement, as fingerprints cannot be collected from a distance in the same manner as facial images and the act of fingerprinting all travellers is labour intensive. By contrast facial recognition can be applied *en masse* to individuals without their awareness. Also in contrast to other biometrics, facial recognition can be applied to any historical image, live video feed or online profile. The techniques used to train facial recognition algorithms are also intrusive, often enlisting the private data of thousands or millions without obtaining lawful and meaningful consent. In its operation, some modes of facial recognition will similarly use millions of images in response to each individual query in order to identify one unknown individual. [Sections 1.4, 1.6 and 3.2.2][pages 79-80]

> **"The Fourth Industrial Revolution fuses the physical and digital worlds while revolutionizing the way global leaders think about security and global connectivity. This has prompted a rise in border automation technology, enabling the more efficient processing of travellers at points of exit and entry. Beyond automation, the capabilities of advanced technologies such as biometrics and predictive analytics make possible a complete redesign of traveller-screening processes, increasing the ability to screen passengers in advance and clear low-risk travellers at a rate faster than ever before.**
>
> **– World Economic Forum, The Known Traveller, January 2018**

While the border control context has always entailed a higher level of surveillance than is commonly tolerated in a free and democratic society, facial recognition technologies are transforming ports of entry and exit into true panopticons, identifying travellers at numerous

points throughout their border control journey and tracking them by linking identification points that were previously distinct. Facial recognition is also increasingly integrated into mobile devices and web-based portals, extending the reach of invasive border control initiatives well beyond the border itself. [Section 2.3]

> **“ The passenger uses his/her biometric(s) as a single token at all touchpoints across the end-to-end journey, including departure, transfers and arrivals, and where possible including the return trip. This should include, but is not limited to, bag drop, secure area access, security screening, outbound border control, lounge access, boarding, inbound border control. It assumes that all these touchpoints are biometrically enabled to verify the passenger’s identity, where possible without breaking stride.**
>
> **– International Air Transport Association, “One ID”, December 2018**

Facial recognition is also integral to a range of automation mechanisms that are transforming the border control journey. Automated baggage check, security triage gates and customs and immigration kiosks all increasingly rely on facial recognition to confirm travellers are who they claim to be. The goal is for facial recognition to displace other travel documents—your face will be your passport. This trend towards automation is particularly problematic given an emerging range of algorithmic decision-making tools, automated risk assessment mechanisms, and rich digital profiling that would be difficult to integrate into automated border control infrastructure absent the identification offered by facial recognition systems. Adoption of facial recognition systems at the border not only facilitates the use of these broader physical and judgemental automation mechanisms, but encourages the further reduction in manual processing that these mechanisms achieve by creating a general paradigm driven by efficiency and automation. [Section 2.2]

Accuracy is a challenge for facial recognition, and the technology remains far more prone to errors than other biometrics despite significant improvements in recent years. The anticipated speed at which border control facial recognition systems operate leads to more inaccuracies while even low error rates will mean that thousands of travellers are impacted daily. Facial recognition has reached a level of technological development where it is sufficiently accurate to allow for greater efficiency in processing, but not sufficiently accurate that errors will not occur, particularly when the technology is applied at the anticipated volumes at which most border control systems will need to operate. Facial recognition systems operate with sufficient levels of accuracy to develop levels of trust in border control officials that are inconsistent with the real-world accuracy of the

technology. Confidence in a biometric system can also extend to overconfidence in profile data that is incorrectly enrolled into a traveller's biometric profile due to administrative error. [Section 1.1.1 and 1.6]

> **"The … the present state of facial recognition (FR) technology as applied by government and the private sector … too often produces results demonstrating clear bias based on ethnic, racial, gender, and other human characteristics recognizable by computer systems. The consequences of such bias … frequently can and do extend well beyond inconvenience to profound injury, particularly to the lives, livelihoods and fundamental rights of individuals in specific demographic groups, including some of the most vulnerable populations in our society. Such bias and its effects are scientifically and socially unacceptable.**
>
> **– ACM, US Technology Policy Committee, Statement on Use of Unbiased Facial Recognition Technologies, June 2020**

In contrast to other biometrics technologies, facial recognition also remains prone to deep racial biases. These can be substantial, with members of marginalized groups experiencing error rates that are orders of magnitude higher. Even top performing algorithms will erroneously recognize images labelled 'Black women' 20 times more frequently than images labelled 'white men', whereas older or inferior algorithms will exhibit greater levels racial bias. When applied at scale, implementing facial recognition across all travellers systematizes racial biases inherent in the technology. At the least, it will mean that any efficiencies in traveller processing that emerge from the use of facial recognition may be unevenly distributed on the basis of racial bias, perpetuating and reinforcing negative stereotypes. More serious detrimental impacts of facial recognition errors are also likely to be unevenly distributed on the basis of racial and demographic biases, meaning that these impacts will fall most heavily on members of marginalized groups. As facial recognition becomes the means by which other automated decision-making processes are applied to travellers, the racial biases inherent in these other algorithmic tools will compound those in facial recognition systems. Facial recognition and other automated tools increasingly form the basis for border control decisions, acting as a means of differentiating the manner in which individual travellers are treated and, at times the degree to which they are submitted to greater levels of surveillance and privacy intrusion in their respective border crossings. In some border control contexts, facial recognition errors can lead to far more serious consequences such as deportation, refoulement or harms to reputation. [Box 4, Box 16 and Box 19][Sections 1.3.2, 1.3.4 and 2.2]

> **“ Ultimately, the [National Council for Canadian Muslims] concludes that the negative travel experiences at airports and/or border crossings for people who present as Muslim, Arab or West Asian are compounded by the lack of remedies available for what people perceive to be injustices. NCCM states that racial profiling in this context can result in ‘a life time of tarnished reputations, loss of dignity, and a collective distrust in law enforcement agencies.’**
>
> **– Ontario Human Rights Commission, “Under Suspicion”, April 2017**

There is also a tangible risk that facial recognition capabilities will not be contained to the border control contexts that justified their initial adoption, but will be the vanguard of new identity, data consolidation and public safety surveillance systems. The intrusive nature of the border control context, where legal protections are relatively lax, offers fewer barriers to the creation of high-quality facial recognition capabilities than other contexts. Border control interactions are hyper coercive, a factor that is also frequently relied upon to incentivize voluntary traveller enrollment in facial recognition systems that could not be legally imposed even at the border. Around the world, these systems have been extended to achieve private sector airport-related service objectives, repurposed by law enforcement agencies, and formed the basis for a persistent national identity. As it remains unclear whether legal and constitutional impediments to this form of repurposing are adequate, the risk of these potential secondary uses must be considered when systems of this nature are justified on the basis of border control objectives. [Sections 1.4, 1.6, 2.4, 2.5 and 2.6][Box 12, Box 13 and Box 14]

> **“ This Bill … make[s] Australian travel document data available for all the purposes of, and by the automated means intrinsic to, the identity-matching services … [such] as: preventing identity crime; general law enforcement; national security; protective security; community safety; road safety; and identity verification.**
>
> **– Australian Passports Amendment (Identity-Matching Services) Bill 2018, Explanatory Memorandum**

Facial recognition systems are increasingly recognized at law as being more intrusive, and biometric facial templates are frequently viewed as ‘sensitive data’. Adoption of facial recognition systems is frequently, but not consistently, accompanied by detailed and dedicated legislative regimes. In some jurisdictions or border control contexts, legislative action is required due to

human rights obligations or because existing border processing legislation does not contemplate automated processing. Imperfect forms of consent are at times relied upon to extend facial recognition use at the border beyond existing levels of authorization. In other contexts, lawful authority of a general nature is relied upon when facial recognition systems are adopted. In addition, commercially available facial recognition services have been used in border control contexts without any clear legal or institutional framework in place, and at times even on an ad hoc basis. Where legislative frameworks are employed, clearly established safeguards and limits have accompanied adoption of the technology. Safeguards can include the obligation to establish minimum accuracy thresholds, whereas limits can be placed on the types of facial recognition technologies adopted and on their permissible uses. Ultimately, current legal protections of general application do not provide sufficient safeguards to ensure facial recognition systems are adopted in a manner that is transparent, proportionate and accountable. [Box 17][Section 3.3]

Canada's adoption of facial recognition systems in border control contexts to date has been characterized by excessive secrecy and few safeguards to prevent repurposing. While many border control facial recognition systems have been accompanied by regulatory or legislative frameworks, these frameworks are silent on the need for periodic and transparent evaluation of the more pernicious potential of facial recognition technologies. Some evidence suggests that Canadian border control agencies appear to have been unaware of the racial biases inherent in these systems, and what little public information is available suggests that while these capabilities may have been assessed for general levels of inaccuracy, they have not been assessed for racial bias. Some preliminary data suggests that these systems are nonetheless susceptible to such bias and have contributed to differential treatment of travellers from certain countries of origin. Exacerbating these challenges, Canadian border control agencies have taken the position that publicly reporting error and accuracy ratings poses a threat to national security. Canada's historical record on facial recognition does not bode well for a current pilot program that Canada is undertaking with the Netherlands. The pilot program envisions a mobile device based facial recognition capacity that will leverage the coercive border control context in order to enlist travellers in a biometric system that is intended to be repurposed later as an open-ended national digital identification for public and private sector administrative purposes. [Sections 1.3.2, 1.6, 2.4, 2.5 & 2.6][Box 12]

> **"A Known Traveller Digital Identity shows great potential for use beyond travel, such as in healthcare, education, banking, humanitarian aid and voting. To raise the concept beyond occasional cross-border travel, the pilot must exploit the network effects associated with the platform economy and highlight to users the potential broad range of everyday applications. By**

> **2020, the Known Traveller Digital Identity concept should be ready to expand beyond the traveler journey and made available to a wide audience, noting that broad adoption is crucial for the success of the concept.**
>
> **– World Economic Forum, The Known Traveller, January 2018**

Pervasive facial recognition poses a pernicious threat to core democratic values such as anonymity and location privacy by creating a powerful and surreptitious surveillance capacity. Facial recognition is also increasingly the vehicle by which rich digital profiles are linked to individuals and other types of automated decision-making mechanisms are applied to them. To be fully automated in application, such mechanisms must first be able to identify the individuals they are attempting to process, and facial recognition systems are currently the most pragmatic tool for achieving that identification capability in real-world spaces. In terms of accuracy, facial recognition is currently sufficiently accurate to instill trust in its matching outcomes—trust that becomes all the more difficult to disrupt when an error does inevitably occur. The enduring racial and demographic biases of the technology all but ensure that its efficiencies and its harms will be distributed in a manner that is detrimental to members of marginalized groups. Collectively, the adoption of facial recognition systems—at the border, and beyond—can directly implicate broader concerns regarding due process, discriminatory decision-making, free expression and privacy. In light of this substantial invasive potential, adopting new facial recognition systems should not occur at this point, while the proportionality and justification of existing systems must be carefully reassessed.

Box 21: Key Findings

- Facial recognition technologies are inherently surreptitious and intrusive, operate with deep racial biases, and are highly susceptible to being repurposed when initially adopted in border control contexts.
- Facial recognition is currently enjoying rapid adoption at border control settings primarily driven by technological developments, perceived higher levels of social acceptance in comparison to other biometrics, and the need for more efficient traveller processing.
- Efficiency gains are generally achieved by automating manual travel document verification and relying on facial recognition to facilitate automation of other processes such as baggage check, customs and immigration processing and security risk assessment.
- Facial recognition is rapidly becoming the biometric of choice for automating several elements of the border crossing journey, providing the essential identification component necessary for applying a range of physical and analytical automated tools to travellers. The goal is to displace other travel documents—your face will be your passport.
- Efficiency gains are often overstated and fail to take into account an automated border control mechanism's true ability to process travellers relying instead on the theoretical matching accuracy of a facial recognition algorithm while ignoring real-world accuracy challenges and related but extraneous factors.
- Facial recognition is more invasive than many other biometric techniques—it retains the general biometric ability to persistently and universally identify individuals, but is able to do so far more surreptitiously and from a distance.

- Facial recognition remains less accurate than other forms of biometric recognition and is persistently challenged by deep racial biases. Adoption of facial recognition systematizes these biases, with the benefits and hazards of embedding such systems at the border unevenly distributed, to the detriment of marginalized groups.
- Where facial recognition is applied as a gate-keeping technology, travellers are excluded from border control mechanisms on the basis of race, gender and other demographic characteristics (e.g. country of origin). Frequently, this differential treatment will perpetuate negative stereotypes and amount to unjust discrimination.
- In some border control contexts, the errors and racial biases inherent in facial recognition technologies can lead to serious repercussions, with travellers erroneously subjected to more intrusive searches, deportation, refoulement and reputation harms.
- While border crossings have always been characterized by high levels of surveillance, facial recognition systems being adopted across the world are transforming ports into panopticons that increasingly extend well beyond the border by incorporating mobile devices.
- Facial recognition systems adopted in border control contexts are increasingly being repurposed for a range of digital identity management, data consolidation and public safety surveillance systems. The inherently coercive nature of the border context allows for lawful and at times voluntary adoption of these systems.
- The lack of clear legal safeguards allows for ongoing adoption of facial recognition technologies by border control agencies, and even by individual agents, on an ad hoc basis without dedicated lawful authorization or safeguards.
- Current general legal safeguards do not provide an adequate framework for ensuring facial recognition systems are adopted in a manner that is transparent, proportionate and accountable, with sufficient consideration of the racial biases and other implications of the technology.
- Canada's adoption of facial recognition systems has been characterized by excessive secrecy surrounding the accuracy and racial bias of these systems and few clear legal safeguards to prevent systems adopted through the coercive border control context from being repurposed more broadly.

Recommendations

New facial recognition systems should not be adopted at this time and the proportionality of existing systems should be re-examined. If a facial recognition system is adopted to achieve border control objectives despite the overall challenges and invasive potential of the technology, steps must be taken to mitigate its detrimental impact.

Facial recognition systems can operate in a centralized or de-centralized manner. Neither is immune from risk, and examples exist where both centralized and de-centralized architectures have faced security, accuracy and purpose limitation compromises. However, centralized systems are more susceptible to system-wide security breaches, data entry and inaccuracy errors, and mass querying or aggregation based on biometric identifiers for purposes unrelated to those that animated the initial creation of the facial recognition system. Generally speaking, a decentralized architecture is more difficult to compromise at a systemic level, easier to secure against inaccuracy, and less susceptible to being repurposed. [pages 6-11]

Data security can also be furthered by discarding all live recordings and facial images once a biometric template is extracted. While facial images are, to a degree, uniquely correlated with individuals, no standard method has emerged for creating biometric templates. As a result, facial templates are often unique only within the specific facial recognition system that generated them and, in the case of a breach, will not generally be usable by another system. By contrast if facial images or live recordings are retained, anyone who compromises the database in question will be able to retain the biometric capabilities of the system. Nonetheless, facial images and live recordings are sometimes be retained in order to facilitate quality assurance or interoperability across different facial recognition systems. [pages 12-14]

Despite substantial improvements in accuracy, facial recognition remains less accurate than other forms of biometric recognition such as fingerprints and iris scans. Image currency is one factor—historical facial images provide for less accurate matches and measures must be taken to ensure more current images are used. Image quality is a central factor, with levels of illumination, facial angle and other related image features impacting accuracy. While more expedient, images captured from a distance as travellers are in motion will produce more inaccuracies than 'stop and look' images, where travellers are prompted to pose for a photograph in front of a camera. Image quality assurance mechanisms can also be adopted to ensure that images enrolled into a facial recognition system are of sufficient quality to maximize accuracy. Inferior cameras and other image capture equipment can further undermine accuracy. Accuracy is also diminished by the use of larger reference datasets, as is frequently the case where one-to-many comparison methods are used in border control settings. [Sections 1.1.1, 1.2, 1.3.1, 1.3.3 and 1.3.4]

Racial, ethnic and gender biases continue to plague even the most accurate facial recognition systems, meaning that many of its benefits in terms of efficiency and the detrimental impacts will be unevenly distributed on the basis of race, ethnicity and gender, with members of marginalized groups particularly at risk of disadvantageous treatment. It does not appear that these disparities can be fully mitigated, some measures can be taken to account for cross-cutting biases. Some demographic groups, such as children under the age of 14 and elderly adults over the age of 79, are at times excluded altogether from facial recognition in border control settings due to persistently high error rates. Use of inferior matching algorithms, image capture equipment, poor lighting conditions or 'capture at a distance' recognition systems can all contribute to even greater degrees of racial bias. Ultimately, it may not be possible to fully mitigate the differential treatment resulting from racial bias these challenges continue to pervade even theoretical matching capabilities. Many uses of facial recognition in the border control context might need to be reconsidered. [Sections 1.3.2, 1.3.3, 1.3.4 and 1.3.6][page 149]

Including a so-called 'human in the decision-making loop' can mitigate the harms of a facial recognition system by ensuring that decisions are ultimately made manually. In many border control contexts, where efficiency through automation is the primary objective, human supervision can be counter-productive. Instead, most travellers are processed automatically, and those that cannot be recognized are directed to manual processing. As a result, travellers who cannot be recognized are excluded from many of the benefits and efficiencies provided by facial recognition systems. The opacity of the automated facial matching process also prevents human decision-makers from assessing why a system failed to match a traveller. This can lead to overconfidence in automated matching determinations, further undermining the mitigating impact that human supervision can have. Depending on the severity of the outcome that relies on facial recognition in its decision-making process, reliance on facial recognition can also undermine a traveller's right to reasons explaining a given determination. In light of the racial biases in facial recognition algorithms, this differential treatment will frequently impact members of marginalized groups most detrimentally. [Sections 1.6, 2.2 and 3.2.3]

A facial recognition system capable of identification is substantially more invasive than a system limited to verification capabilities. Facial verification operates by comparing the traveller's face to a historically verified image of the traveller, typically stored on the traveller's machine-readable biometric passport (a one-to-one [1:1] comparison). This requires the traveller to make an overt identity claim, which the facial recognition system then verifies or rejects. Facial identification, by contrast, can *discover* a traveller's identity by comparing the traveller's face against an image gallery pre-populated with historically identified facial images (a one-to-many [1:N] comparison). A 1:N system is inherently more intrusive, as it requires the creation of millions of centralized biometric profiles and, in its operation, searches *all* of these to produce its results. Second, while 1:1 verification systems embed many of the same inaccuracies and racial biases as identification systems, errors are far more pronounced in 1:N matching, where a traveller's facial image must be compared against a large gallery of images. Finally, the constraints of a 1:1 verification mechanism place some inherent limits on the invasive capacity of a facial recognition system, as 1:N comparison can operate from any live or historical image without individual interaction, including through CCTV cameras. While 1:1 systems have been repurposed to create powerfully invasive digital identity management tools in administrative and commercial contexts, the population wide identification-at-a-distance capability of 1:N systems poses an insidious threat to anonymity, private mobility and civil liberties. [Sections 1.3.1, 1.3.2, 2.1, 2.5 and 2.6]

Facial recognition systems require proportionality and impact assessments prior to adoption and on an ongoing basis. Prior to procurement, matching algorithms must be assessed through the use of pilot programs, as theoretical error and racial bias rates will always be lower than real-world results. It is particularly important to ensure that the racial biases of any chosen facial recognition algorithm are

assessed early and often. Procurement choices are critical, because racial and demographic groups will be impacted differentially depending on which algorithm is selected. Too frequently, matching algorithms are assessed solely on their overall accuracy, a practice which obscures their substantial impact on members of marginalized and other demographic groups. Nonetheless, procurement decisions implicitly include a choice between minimizing general traveller impact and minimizing impact on travellers from specific demographic communities. Assessment of errors and racial biases must continue to occur on a regular basis once a facial recognition system is put into place, as the quality of image capture equipment, lighting, evolving traffic loads and other changing conditions will affect error rates, detrimental impact on travellers, and the overall efficiency of the system. [Sections 1.3.2 and 1.3.6]

Adoption of *any* facial recognition system must be accompanied by a dedicated legislative framework. The need for legislative backing applies to border control implementations that rely on a form of consent (opt out or opt in). This legal framework must impose rigorous accuracy thresholds that encompass not only overall error rates, but also limits on errors experienced by racial and demographic groups. Thresholds must also be set for real-world efficiency and for operational impacts on travellers and racial groups, and these must be assessed in an ongoing basis. Initial (theoretical) error and efficiency ratings must be publicly reported before the adoption of any facial recognition system, and ongoing assessments must be published on an ongoing basis. Legislation must explicitly indicate the specific tasks that will be carried out by the anticipated facial recognition system and must prohibit any secondary access. Any secondary use must be explicitly prohibited, and any evidentiary use of facial recognition must also be explicitly prohibited. While atypical in Canadian legislation, given the particular challenges posed by facial recognition technologies the system must also indicate specific permissible technological parameters such as explicitly specifying whether facial verification or identification will be permitted. The legislation should also appoint an independent regulator—preferably the Privacy Commissioner of Canada—to identify core operational elements of the system and require regulatory approval before any changes are made to these core operational elements. [Section 3.3][Box 13]

Box 22: Recommendations

- New border control facial recognition systems should not be adopted at this time, while the proportionality and racial biases of existing systems should be re-evaluated.
- Legislation should specify that biometric data is sensitive and requires additional protection, prohibit the use of facial recognition systems in the absence of explicit lawful authority, and entrust the Office of the Privacy Commissioner of Canada with general oversight of recognition systems.
- While decentralized facial recognition reference datasets are not immune, centralized architectures are more susceptible to systemic compromise in terms of data security, data entry accuracy, and purpose limitation and are therefore less proportionate in nature.

- Once a biometric facial template is created, the underlying image or live recording from which it is generated should be discarded immediately to minimize data retention and harm in case of security breach.
- Travellers under 29 and over 70 years of age continue to pose challenges for facial recognition accuracy, and some programs categorically exclude travellers aged under 14 or over 79.
- Ageing continues to pose a challenge for facial recognition accuracy, and a facial recognition system must be designed to ensure only relatively current images (5-10 years old) are used.
- Image quality remains a central factor in a facial recognition system's overall accuracy. 'Stop and look' image capture is slower, entailing an efficiency trade off, but yields higher quality images than those captured from a distance while travellers are in motion.
- Image quality assurance mechanisms can be incorporated into facial recognition systems to ensure enrolled images are of sufficient quality to maximize accuracy.
- Racial bias remains a challenge for facial recognition systems, and can be exacerbated by the adoption of particularly biased face matching or detection algorithms, the use of inferior image capture equipment, deployment under poor lighting conditions, and reliance on 'capture at a distance' techniques.
- Despite mitigation, racial bias continues to pervade facial recognition capabilities at even a theoretical level, and will continue to pervade all elements of facial recognition systems (image capture, face detection, face matching, etc.).
- Including a 'human in the decision-making loop' can mitigate some of the inaccuracies of a facial recognition system, but attempts to maximize automation efficiency and a tendency for decision-makers to develop an over confidence in automated determinations can substantially undermine the mitigating impact of human supervision.
- Adoption of 1:N systems is substantially more intrusive than 1:1 systems. Each 1:N query typically entails searching millions of biometric-enabled profiles in a centralized reference dataset and yields higher levels of inaccuracy and racial bias. The population wide identification-at-a-distance capacity of most 1:N systems is particularly insidious.
- As 1:1 systems also embed racial bias and inaccuracy and have been repurposed to create powerfully invasive digital identity management tools in administrative and commercial contexts, any and all facial recognition systems must undergo rigorous proportionality and impact assessments prior to adoption and on an ongoing basis.
- Real world use will always yield higher error rates and racial bias than theoretical testing. Assessing a system's anticipated proportional impact must anticipate, as much as possible, actual conditions (speed of processing, volume of travellers, image quality, etc.), perhaps through the use of pilot programs, and periodically following adoption.
- Assessment of a facial recognition system must be rigorously transparent. Error and racial bias rates, efficiency assessments and full human rights and privacy impact assessments must be made public prior to the system's adoption, and on an annual basis following adoption.
- Facial recognition systems must only be adopted with legislative backing that includes strict explicit limits on any repurposing, on any use of the system for evidentiary purposes, on the specific technical capabilities of the system (e.g. verification or identification), and, subject to independent regulatory approval, on any changes to core operational elements.
- Legislation or regulation must also establish minimum accuracy and bias thresholds and obligations to assess and report error, racial bias and efficiency rates on an ongoing basis.

Section 1. Terms & Operational Considerations

Facial recognition is a biometric mode that is primarily deployed for automated identification or verification/authentication purposes. It operates by analyzing and extracting biometric information in the form of key facial features in a manner that allows for comparison between two representations of an individual's face.

It is helpful to think of facial recognition systems in a compartmentalized manner. First, a number of datasets are necessary for the creation and operation of a facial recognition system. A reference dataset provides the underlying basis against which travellers' live facial images are matched, while testing and training datasets are used to teach a recognition algorithm how to recognize faces. Second, a facial recognition system can operate in different ways and with varying constituent elements.

Each of these components exhibit design features and choices that can affect the impact of a facial recognition system, and are relevant to understanding its functionality. This section therefore provides a brief outline of these components, while introducing key terminology and technical concepts.

Note that a complete description of competing technological models that might be employed by a facial recognition system is beyond the scope of this report. We do not delve into the nuances of different neural networks, for example. Such differences are only referenced to the extent that they impact the broader implementation or privacy challenges described in more detail in further sections of this paper.[1]

Technologically, facial recognition continues to be in a stage of rapid development. The empirical assessment of facial recognition systems is characterized by equally rapid change. Despite this ongoing dynamic, this section attempts to distill some stable features that are likely to remain important to assessing the impact of facial recognition systems in the near future.

The operational and analytical descriptions below are organized by different elements of the facial recognition process. This is largely because failures at each stage of these disparate processes can compound the overall accuracy of a facial recognition system. However, it is helpful to distill some key and cross-cutting findings at this point.

While some facial recognition systems have achieved high levels of real-world accuracy, this is not universal. It is important to rigorously assess the specific characteristics of a given algorithm prior to procurement and implementation. This assessment must take into account the real-world context for which the system is intended, including the volume of anticipated travellers that will be processed and the quality of images that will be submitted to the system.

More importantly, racial and demographic bias is a cross-cutting factor that continues to effect facial recognition systems, allowing population-wide accuracy ratings to obscure the often severe impact experienced by marginalized communities and other demographic groups. Members of these groups will frequently experience substantially higher error rates than the general population, and as a result the detrimental impact of adopting a facial recognition system will tend to fall most heavily on members of these groups. The prevalence of this bias has led many in the technical community to question whether there should be a general moratorium on the use of facial recognition systems until these bias challenges can be addressed. For example, the Association for Computing Machinery's United States Technology Policy Committee (USTPC) adopted a statement recognizing that facial recognition technologies have not overcome their racial, ethnic and gender biases, and that the effects of these biases "are scientifically and socially unacceptable."[2] USTPC's adopted statement specifically finds that facial recognition technology "is not sufficiently mature and reliable to be safely and fairly utilized without appropriate safeguards against adversely impacting individuals, particularly those in vulnerable populations" and urges an immediate suspension of all facial recognition use where it is likely to undermine human and legal rights.[3]

Box 4: The Impact of Recognition Errors—False Positives v False Negatives

Facial recognition errors can be generally classified as false positives and false negatives. False positives occur where an individual is incorrectly matched to a facial image, whereas false negatives occur where a facial recognition system fails to recognize that two images are from the same individual.

Other types of facial analytics generate more task-specific types of errors (such as miscategorising gender, or failing to detect a face in an image or a person).

The impact of each type of error will be different depending on the border control context in which it occurs.

Some jurisdictions, including Australia and the United Kingdom, have begun using facial recognition-enabled criminal watch lists at border control settings. False positives in criminal investigative contexts have led to erroneous arrests.[4]

In 2016, the United Kingdom developed a portal for online passport applications. Before individuals submitted their application, a face analytic algorithm would inform applicants if the facial image they had submitted was in line with specification requirements for passport photos. In 2019, it was reported that the face detection algorithm had been erroneously rejected images of individuals with darker skin tones, rendering the online platform effectively unusable for many applicants of colour.

Canada has recently deployed facial recognition in Primary Inspection Kiosks (PIKs), which verify travellers' travel documents by comparing facial images encoded on their passports with live photographs taken by the kiosks. In this context, a 'false positive' represents a security threat, in that an individual using a false passport might be verified erroneously and permitted to enter Canada. Imposters can be expected to roughly emulate the age, gender and demographics of the identity they are trying to impersonate.

Travellers experiencing false negatives, by contrast, will experience differential treatment at border crossings and may be subjected to increased suspicion and scrutiny on the basis that the PIK was unable to verify their passport. One study of PIKs suggested a potential correlation between false facial recognition matches at PIKs and higher levels of enhanced screening referrals for individuals from Iran, Jamaica, Chad, the Philippines and Nigeria.

Where this differential treatment is systemized across all border crossings, it can embed racial bias, compound historical inequities and perpetuate negative stereotypes.

Canada uses facial recognition when processing visa and passport applications. False negatives can cast suspicion on asylum seekers, undermining their claims. False positives have led to individuals being publicly accused of crimes without concrete confirmation of identity.[5]

The impact of errors on travellers can be serious and wide-ranging, and will depend on the nature of the error (e.g. if a traveller is incorrectly matched to another's profile as opposed to if a facial recognition system fails to match a traveller against their enrolled image) and the context in which the facial recognition system in question is implemented. Where facial recognition is embedded into border control systems designed to increase efficiency, travellers who cannot be recognized due to racially biased systems may find themselves excluded from the benefits of efficient processing on the basis of race. An erroneous failure to recognize a traveller can cast suspicion on their identity and generally contribute to more enhanced scrutiny. Where this differential treatment results from racial bias in the facial recognition system, it can compound historical power imbalances experienced by marginalized groups and perpetuate negative stereotypes. Facial recognition systems can also be used to identify travellers in the immigration context, where incorrect identification has led to serious reputational harms and can lead to refoulement of asylum seekers.

Assessing any facial recognition system must take into account the real-world setting in which the system is to operate. Factors such as airport lighting, positioning and quality of cameras, and the anticipated volume of travellers will all affect the detrimental impacts of a facial recognition system by magnifying inaccuracies and racial biases. In the context of border control, the sheer volume of travellers processed by facial recognition on a regular basis can mean that even small error rates or biases will impact many. Assessment of these real-world impacts must occur prior to the adoption of any facial recognition system and must continue on a periodic basis if implementation occurs.

Privacy considerations are implicated at several elements of the facial recognition process. Facial recognition algorithms must 'learn' to recognize faces, and this requires the use of many facial images. Most of the facial images used in this algorithmic training process have been collected without meaningful consent or approval of the individuals whose images are included. Moreover, the surreptitious nature of facial recognition sets it apart from other forms of biometric identification. Travellers can be enrolled into a facial recognition system or subjected to facial recognition from a distance and without any awareness. The right of consent or refusal becomes difficult to exercise in such contexts. Finally, once created, a facial recognition system is subject to repurposing and can become a powerful threat to anonymity. This threat has led several technology companies (including Microsoft and Amazon) and a number of municipalities to announce moratoriums on the use of their facial recognition systems by law enforcement while IBM has ceased all research, development and production of facial recognition systems.[6]

Box 1: Centralized & De-Centralized Reference Datasets

- **Technical Security & Accessibility:** Centralized & decentralized architectures can both pose a risk to security. Systemic weaknesses have been exposed in decentralized systems in the past, exposing personal data to this within sufficient proximity to remotely interact with RFID chips embedded on passports.[7] Centralized reference datasets, by contrast, are vulnerable to more wide-ranging compromise, and entire facial recognition databases have been breached exposing the biometrics of hundreds of thousands of individuals.[8] Centralized reference datasets also need to develop secure and robustly consistent network access across a diverse range of implementation locations.
- **Data Accuracy:** While inaccuracies in the biometric image and enrollment data encoded on decentralized architectures are possible, data entry errors have been more widely documented in centralized systems.[9] Decentralized systems can reduce the opportunities for error. Electronic data on ICAO compliant biometric passports, for example, is only written once upon issuance, and not modified for the duration of the passport's validity.[10] By contrast data entry in centralized systems is often an ongoing process. Strict quality assurance measures can mitigate, but not wholly remove, errors in centralized systems.[11]
- **Secondary Purposes:** Both decentralized and centralized systems can be repurposed for administrative, crime control, and digital identification purposes, with systemic implications.[12] Centralized systems, however, can be repurposed for mass querying without the involvement, or even knowledge, of impacted individual.[13] Centralized reference datasets are also susceptible to mass aggregation with other biometrically enabled reference datasets on the basis of the biometric identifier alone.[14] In some jurisdictions, centralization is legally precluded without independent lawful justification.[15]
- Generally speaking, a decentralized architecture is more difficult to compromise at a systemic level, easier to secure against inaccuracy, and less susceptible to being repurposed.

Various design choices can mitigate the privacy impact and potential for inaccuracy inherent in facial recognition systems. Reference datasets can be centralized or de-centralized. While both architectures are susceptible to data security breaches, inaccurate enrollment data and repurposing, centralized architectures allow for compromise on a systematic level, leading to farther ranging harm. Additionally, facial recognition systems extract biometric templates from facial images and live recordings. Once these templates are extracted, the underlying images and recordings are no longer required and should be discarded expeditiously to minimize the impact of a compromise. A facial recognition system must also include mechanisms to ensure images used by the system are of sufficient quality and currency, as low quality or older images undermine accuracy. While requiring travellers to stop and pose for facial image capture at border crossings may increase traveller processing time, it also generates higher quality images than 'capture from a distance' implementations, where pose and lighting are more variable and images can be blurry. Finally, meaningful and explicit individual consent can be employed when facial recognition systems are generated as well as when they are operated.

The opaque manner in which facial recognition systems generate their results can make it difficult to correct errors and biases. Designing border control systems that rely on humans as the final decision-makers can mitigate the inherent fallibility of facial recognition systems to some degree. In some contexts, however, border control officials have developed high levels of trust in biometric recognition

systems, creating a level of suspicion that travellers find difficult to overcome. In part, this results from the opacity and 'scientific mystique' of the automated facial matching process. Human decision-makers are unable to understand the basis for a facial 'match' or 'no match' decision, and therefore find it difficult to second guess the outcome.

The covert and invasive potential of facial recognition systems allows for their non-transparent adoption, whereas their deployment is at times accompanied by government policies of secrecy and opacity that are designed to shield the operation of these systems from public scrutiny. The Canada Border Services Agency, for example, has claimed that it cannot publicly report error rates and racial bias levels for its facial recognition system on the basis that doing so would undermine national security.[16] Given the well-documented problems inherent in facial recognition systems and their deep capacity for privacy invasion and racial injustice, non-transparent adoption threatens the legitimacy and social license of these tools and the agencies that deploy them.

Section 1: Summary of Key Points

Box 2: Reference, Training & Testing Datasets—Policy Implications

- **Decentralized:** A decentralized architecture offers more opportunities for individual participation, while reducing risk that facial recognition systems will be compromised or repurposed at a systemic level.
- **Discarding Facial Images:** Retaining facial images in a reference dataset facilitates interoperability, but leads to greater risk that the facial recognition system will be repurposed or abused if breached.
- **Accuracy:** Facial recognition systems must include rigorous quality assurance mechanisms to ensure the facial samples and related enrollment reference data is accurate, and that errors can be corrected when discovered.
- **Dataset Diversity:** Training and testing datasets of sufficient size and variety in facial dimensions are more readily available than was historically the case, but publicly available datasets lack demographic diversity which contributing to racial bias in facial recognition capabilities.

Box 3: Facial Recognition in Operation—Implications & Considerations

- Accuracy is more difficult where images are taken in less constrained environments, and facial angles, lighting, expression, occlusion and image quality are less predictable.
- 'Stop and look' facial image capture mechanisms (e.g. kiosks) will yield higher quality results than 'capture at a distance' approaches where images are captured from travellers in motion, but will entail an efficiency trade off.
- Facial images and any underlying recordings are no longer necessary once a facial template has been extracted and image capture systems should be designed to discard these images once extraction has occurred.
- Larger reference datasets impede the effectiveness and accuracy of facial recognition systems. One-to-one comparison or smaller reference datasets will generally be more accurate, whereas one-to-many comparison using large reference datasets will require active human participation and cannot be fully automated.

Box 5: Gauging Algorithmic Accuracy, Efficiency & Racial Bias

- Facial recognition accuracy in general must be rigorously assessed prior to implementation, taking into account the context in which a facial recognition system will operate so its full impact can be taken into account, including the impact of volume, lighting, and image capture apparatus quality.
- Some age groups may need to be wholly excluded from automated facial recognition processing due to unacceptable error rates. The categorical exclusion of certain age groups must be taken into account when assessing the anticipated efficiency and proportionate impact of adopting facial recognition at the border.
- Factors unrelated to facial recognition (e.g. the inability to automatically process a proportion or travellers due to security or immigration requirements) can undermine the anticipated efficiency of the system if it precludes automated processing and cannot be disregarded when calculating the benefits of adopting a system.
- Racial, ethnic and gender bias is a pervasive factor common to most facial recognition algorithms. The anticipated impact on marginalized groups in particular must be rigorously measured so that the overall proportionality of a facial recognition proposal in question can be assessed prior to its adoption.
- Racial bias can occur or at or be compounded by many constituent elements of the facial recognition process, including through use of biased face detection algorithms, biased image quality assurance mechanisms, inferior image capture equipment and poor lighting, and biased comparison algorithms.
- If adopted, facial recognition systems must be calibrated in the real-world settings in which they will be operating so that trade-offs between false positives and negatives are reflective of actual operational error rates.
- If adopted, facial recognition systems need to be continually tested and audited after implementation for efficiency, accuracy and racial bias to account for variations in real-world environments, capture equipment, the size of the reference dataset, the volume of travellers impacted, and other border control parameters.
- Facial recognition using 1:N comparison with large reference datasets is generally less accurate than 1:1 comparison and cannot achieve sufficient accuracy without active human intervention and is therefore inappropriate in fully automated contexts.

Box 6: Individual Participation & Choice

- Facial recognition systems can incorporate voluntariness at the enrollment stage, when a system is altered or expanded, and at the 'use' stage, but choice must be meaningful to be considered voluntary.
- Opt-in mechanisms are more robust where they require active traveller enrollment in voluntary programs than when travellers are enrolled while crossing borders.
- Training and testing datasets have been criticized and face legal challenges for including facial images of individuals without their meaningful consent or even awareness, while opt-out mechanisms have proven ineffective, when available.
- When alternatives to facial recognition exist at border crossings, travellers are often unaware of these alternatives—or even that they are being subjected to facial recognition at all. Use of dedicated 'facial recognition' and 'manual' processing lanes can provide clear notification and choice.

Box 7: Overview of Transparency Challenges

- Facial recognition is more surreptitious than other forms of biometric recognition, and it is less self-evident to travellers that they are enrolling or participating in an automated biometric comparison process.
- The opacity of facial recognition algorithms lends credibility to determinations rendered by these systems, resulting in automation bias and overconfidence by border control officials and other decision-makers. This undermines any mitigating impact that human supervision of automated facial recognition might have.
- In some jurisdictions, the onus has been placed on asylum seekers to dispute border control biometric determinations, despite general awareness that such systems are opaque in operation and fallible.
- Obscuring error rates and racial bias data can seriously undermine public trust in facial recognition systems and the border control agencies that operate them, particularly in the marginalized communities that are most deeply and frequently impacted by their use.

Endnotes.

[1] It is not relevant, for example, what particular architecture is employed by a given deep network to train its facial recognition model. While different architectures may have differing levels of accuracy or efficiency. By contrast, the general tendency of many deep network methods to operate in a manner that is opaque is a feature that impacts many deep network methods, and this can have negative impacts on transparency. Another feature that is cross-cutting across many facial recognition models is the concept of comparison scores and as such this concept is described to the extent it is necessary to understand accuracy impacts. The general concept of training data is likewise described to the degree necessary to understand the potential impacts on visible minorities.

[2] Association for Computing Machinery, US Technology Policy Committee (USTPC), "Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies", June 30, 2020:

> The ACM U.S. Technology Policy Committee (USTPC) has assessed the present state of facial recognition (FR) technology as applied by government and the private sector. The Committee concludes that, when rigorously evaluated, the technology too often produces results demonstrating clear bias based on ethnic, racial, gender, and other human characteristics recognizable by computer systems. The consequences of such bias, USTPC notes, frequently can and do extend well beyond inconvenience to profound injury, particularly to the lives, livelihoods and fundamental rights of individuals in specific demographic groups, including some of the most vulnerable populations in our society.
>
> Such bias and its effects are scientifically and socially unacceptable.

[3] Association for Computing Machinery, US Technology Policy Committee (USTPC), "Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies", June 30, 2020.

[4] Kashmir Hill, "Wrongfully Accused by an Algorithm", *New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[5] Jeremy C Fox, "Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect", *The Boston Globe*, April 28, 2019, https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html; Stewart Bell and Andrew Russell, "Facial Recognition 'Confirmed' Ajaz Developer Was Wanted Crime Boss, but CBSA Couldn't Prove It", *Global News*, December 19, 2019, https://globalnews.ca/news/6301100/confirmed-facial-recognition-but-did-not-proceed-documents/.

[6] Arvind Krishna, Chief Executive Officer, IBM, Letter to Congress, June 8, 2020, https://www.ibm.com/blogs/policy/wp-content/uploads/2020/06/Letter-from-IBM.pdf:

> IBM no longer offers general purpose IBM facial recognition or analysis software. IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values and Principles of Trust and Transparency. We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies.

See also: Jay Greene, "Microsoft Won't Sell Police its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM", *The Washington Post*, June 11, 2020, https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/; Jay Greene, "Amazon Bans Police Use of its Facial-Recognition Technology for a Year", *The Washington Post*, June 10, 2020, https://www.washingtonpost.com/technology/2020/06/10/amazon-rekognition-police/;

Electronic Frontier Foundation, "Bans, Bills and Moratoria", last accessed September 30, 2020, https://www.eff.org/aboutface/bans-bills-and-moratoria.

[7] The specifics of these various attacks are beyond the scope of this paper. An overview of historical attacks can be found in: Wikipedia, Biometric Passports, Section 2: Attacks, (last accessed December 12, 2019), https://en.wikipedia.org/wiki/Biometric_passport#Attacks.

[8] For example, a private sector biometric database used widely by a number of United Kingdom government agencies for facial recognition purposes was breached, exposing the biometric identification data of over 1 million people.

Josh Taylor, "Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms", August 14, 2019, *The Guardian*, https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

It was also discovered that a company contracted by US and Canadian border control agencies for the purpose of automatically identifying license plates near land borders had accumulated its own facial recognition database of travellers (without authorization) and, moreover, this database had been breached exposing the license plate and facial biometrics of 100,000 individuals.

Drew Harwell & Geoffrey A Fowler, "US Customs and Border Protection Says Photos of Travelers Were Taken in a Data Breach", June 10, 2019, *The Washington Post*, https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/; Joseph Cox, "Here Are Images of Drivers Hacked from a US Border Protection Contractor", June 13, 2019, *VICE*, https://www.vice.com/en_us/article/43j5wm/here-are-images-of-drivers-hacked-from-a-us-border-protection-contractor-on-the-dark-web-perceptics; Catharine Tunney & Slvène Gilchrist, "Border Agency Still Using Licence Plate Reader Linked to US Hack", June 25, 2019, *CBC News*, https://www.cbc.ca/news/investigates/cbsa-perceptics-licence-plate-still-using-1.5187540.

[9] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, pp 82-87.

[10] Government of Canada, "The ePassport", last updated July 13, 2017, https://www.canada.ca/en/immigration-refugees-citizenship/services/canadian-passports/help-centre/e-passport.html,

> ... The only biometric information stored in the Canadian ePassport is the photo of the passport holder's face. The other information stored on the chip is the same as the information found on page 2. Once this information is locked on the chip, no information can be added or removed.

[11] European Union, Fundamental Rights Agency, "Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security", May 2017, p 32.

[12] For an example of a decentralized biometric border control system that is designed to be repurposed, see: Box 12, which describes the World Economic Forum's Known Traveller Digital Identity initiative. For an example of a centralized biometric border control system that is being broadly repurposed, see: Box 13, which describes Australia's Identity Matching Services initiative.

[13] See footnotes 19-21 of the primary report and accompanying text.

[14] The European Union is currently undertaking a wide-ranging aggregation initiative of this type: European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, p 9:

> … the European Commission ... proposals also suggest establishing a common identity repository (CIR) with core biographical data of persons whose data are stored in the different IT systems, and adding a multiple identity detector (MID) to create links between different identities of the same person stored in the CIR.

[15] *Schwarz v City of Bochum*, Case C-291/12, (2013, Court of Justice of the European Union Fourth Chamber), paras 58-63:

> ... the referring court is uncertain ... whether Article 1(2) of Regulation No 2252/2004 is proportionate in view of the risk that, once fingerprints have been taken pursuant to that provision, the – extremely high quality – data will be stored, perhaps centrally, and used for purposes other than those provided for by that regulation. ... The regulation not providing for any other form or method of storing those fingerprints, it cannot in and of itself, as is pointed out by recital 5 of Regulation No 444/2009, be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the European Union.

See also: European Data Protection Supervisor, Opinion 9/2017, para 14; European Commission, Twentieth Progress Report Towards an Effective and Genuine Security Union, COM(2019)552, October 20, 2019, p 4.

[16] Evan Dyer, "Bias at the Border? CBSA Study Finds Travellers from Some Countries Face More Delays", *CBC News*, April 24, 2019, https://www.cbc.ca/news/politics/cbsa-screening-discrimination-passports-1.5104385:

> CBC News also obtained a report entitled "Facial Matching at Primary Inspection Kiosks" that discusses 'false match' rates. False matches include 'false positives' — innocent travellers incorrectly flagged as posing problems — and 'false negatives' — a failure by the machine to detect such problems as fake documents or passport photos that don't match the individual.
>
> The documents released were heavily redacted, with entire pages blanked out. "The CBSA will not speak to details of this report out of interests of national security and integrity of the border process," the agency's Nicholas Dorion said.

Section 2. Transformation at the Border & Beyond

Facial recognition is currently experiencing rapid adoption in numerous border control settings around the world and to accomplish a variety of functions.

The nature and impact of a given facial recognition system will depend on a number of factors, ranging from the level of automation being facilitated to the location where facial recognition is being included. This section seeks to present an indicative, rather than complete, catalogue of the types of border control tasks that are incorporating facial recognition systems, with a focus on factors that are transforming border crossings for travellers.

Border control systems can adopt different core recognition functions (verification, identification or screening) and can use different comparison methods. In operation, a one-to-many [1:N] identification capability, where a traveller's facial images is compared against *all* images in a pre-populated image galleries, is generally more invasive than a one-to-one [1:1] approach, where a traveller's facial image is merely compared against a single image. Facial verification [1:1] requires travellers to make an identity claim, typically by presenting a passport or other biometrically enabled identification. A 1:1 system will then compare the traveller's face to an image associated with that passport. By contrast, 1:N systems are able to discover an unknown identity by comparing a traveller's face to millions of pre-enrolled profiles in the system's facial image gallery. This open-ended 1:N identification capability is more intrusive in nature and can be readily repurposed into a mass surveillance tool. By contrast, 1:1 systems have also been repurposed as general purpose digital identification, which are also intrusive, but do not pose as wide-ranging a threat to anonymity as an open-ended identification capability.

Automation is transforming the border control journey, supplementing the activities of human border control functions and, in many instances, replacing them altogether. Automation frequently relies on some form of biometric recognition so that border control infrastructure can verify traveller identity without human intervention. Facial recognition is rapidly becoming the biometric of choice for automation and other border control objectives—the ultimate goal is for faces to displace passports. Facial recognition is free of the stigma associated with other biometrics such as fingerprinting, is faster than other biometrics, and its inherent surreptitiousness will mean that travellers will frequently remain unaware that they are being biometrically recognized. Automation of physical border control infrastructure also encourages greater reliance on automated decision-making tools to further reduce manual processing and maximize the utility of automation. These automated decision-making tools are subject to additional racial biases, which can compound biases in facial recognition systems.

The location in which facial recognition systems are employed can affect the proportionality and intrusiveness of a given implementation. Facial recognition is frequently used to extend the frequency with which travellers are identified by adding multiple 'touchpoints' at locations throughout an airport, transforming various ports of entry/exit into effective panopticons. Facial recognition is also used to link identification points and record these in rich profiles that track a traveller as they navigate their way through the airport. The use of mobile devices and web-based portals allows for this tracking to extend beyond the airport itself.

Box 12: WEF's Known Traveller Digital Identity
Biometrically-Enabled Digital Identification Begins at the Border

Canada is in the process of piloting the World Economic Forum's Known Traveller Digital Identity (KTDI) proposal,[1] which incorporates facial recognition as a central component of the digital trust rating system it seeks to develop. The proposed system would permit travellers to build trust in a digital identity, which can then be used to reliably interact with border control entities and to avoid travel "pain points" by unlocking access to expedited border control processes. (p18) Once established as a stable digital identity mechanism in the border control context, it is envisioned that the project will form the basis for a wider range of identity management between individuals and the "wider public- and private-sector ecosystem". (p35)

Participation for the voluntary program begins when a traveller creates a KTDI profile on their mobile device and registers with an enrolment officer who verifies their identity. The profile is initially populated with the traveller's passport information (including an ICAO-compliant facial sample). Travellers will also be prompted to include other details in their profile, such as their driver's license numbers and credit card details.

To further bolster their trust scores, travellers will be incentivized to interact with various private entities such as banks, hotels, medical providers and education institutes – each successful interaction will register an identity attestation on the traveller's KTDI profile. Travellers will also have the option of allowing private institutions to populate their KTDI profile with additional trust-enhancing information such as credit ratings from their bank, educational credentials from their Universities, vaccination confirmations from their doctors, and hotel-verified travel itineraries. (Table 9 and Fig 5) Finally, travellers will be able to respond to in-app queries from border officials in advance of an anticipated border crossing.

Known travellers can use the KTDI framework to apply for visa authorizations via their mobile devices, to access automated border control functionality such as e-gates and baggage drop-off, and to submit to pre-screening risk assessments in advance of international travel. Travellers can build a richer KTDI profile by accumulating data and a greater volume of identity attestations. Travellers can then selectively share more KTDI information with border control agents in order to qualify for higher trust scores, (p17, Sec D) leading to successful algorithmic risk assessments, advance security screening, and visa applications.

The KTDI proposal relies on facial verification as one of its central enabling technologies. It provides the primary basis by which travellers can be linked to their digital profiles with ease and a degree of accuracy – as one presentation of a KTDI pilot project notes, "Your face is the key".[2] Facial verification permits enrollment officials to reliably verify a traveller's identity when first establishing a KTDI profile. It permits border control entities to verify pre-cleared KTDI travellers, transforming the KTDI profile into a travel document.

Officials will be able to facially scan crowds of travellers to identify specific KTDI travellers pre-selected for secondary screening, and automated e-gates will be able to facially verify KTDI travellers that have been deemed 'lower risk' or 'trusted', granting access to expedited security zones.

"[KTDI] shows great potential for use beyond travel, such as in healthcare, education, banking, humanitarian aid and voting. … broad adoption is crucial for the success of the concept. (p37)

While a voluntary program, if the proposal becomes embedded in travel and private sector interactions, it may become effectively infeasible for citizens to opt out.

Many facial recognition borer control programs are fully optional in operation. Travellers who are able to qualify as 'lower risk' can successfully enroll in these programs and are then provided expedited security processing when crossing border control junctures. Biometric recognition (increasingly, facial recognition) is used by these programs to robustly identify 'trusted' travellers at border crossings. Against the backdrop of greater intrusion and coercion that generally characterizes border control, these 'trusted traveller' programs can offer a compelling value proposition to many travellers.

Box 13: Australia's Identity Matching Service: Universal Identifier & Generalized Surveillance Tool

Australia is in the process of adopting a wide-ranging facial recognition capability that relies heavily on carefully vetted biometric profiles established in the border control context.

The roots of Australia's national facial recognition initiative can be found in an Intergovernmental Agreement (IGA) on Identity Matching Services (IMS) entered into by all federal, state and territorial governments in 2017. Since finalization of this agreement, various national and regional governments have sought to enact authorizing legislation (most recently, the 2019 IMS Bill).

The IMS Bill creates an interoperability hub (Hub) offering a range of services including a 1:1 Face Verification Service (FVS) and a 1:N Face Identification Service (FIS). The Hub is essentially a querying system—entities can submit facial images and query biometrically-enabled identity profiles operated by other participating government agencies.

While the IMS initiative would rely on a number of government issued identification databases (e.g. driver's licenses) border control related identity profiles are relied upon heavily in practice. The 1:1 FV Service launched in 2016, before the IGA was even finalized, relying solely on immigration-related images. Biometric immigration and travel documents will be central to the Hub.

Under the IMS Bill, government agencies must have independent lawful authority to submit facial recognition queries. But biometric databases added to the Hub are authorized to respond to queries for broadly defined identity or community protection purposes.[3] Absent this authorization, the Australian *Privacy Act* would limit sensitive biometric profiles from being repurposed.[4]

Under the rubric of identity protection, the FVS envisions a government-wide capability that can be used in the general delivery of government services to confirm identity claims made by individuals. Private sector entities will also be able to query the FVS with consent or to meet regulatory obligations. FVS may also be used in road safety contexts, including in random traffic stops. As a result, the initiative creates a *de facto* new national identification system with facial recognition as its core universal identifier.

The more intrusive FIS, capable of identifying unknown individuals in person or from CCTV camera stills, is available to specific agencies for a range of law enforcement and national security objectives. The FIS 1:N capability has been criticized for applying to non-serious offences, for failing to prohibit the use of FIS matches as evidence of identity in court, and for lacking an individualized suspicion-based judicial authorization requirement.

Emerging practice strongly suggests that facial recognition systems created in the border control context will not be constrained or limited to that context for long, with many examples of border control systems being repurposed to achieve various other objectives. These objectives range broadly and can include domestic law enforcement and public safety concerns, fraud prevention, road safety, and national security. Facial recognition profiles created at airports are also seen as a means of generating general purpose digital identification management mechanisms. In some contexts, the extraordinarily coercive border control context is actively used

to incentivize voluntary traveller enrollment in optional facial recognition systems, knowing that these systems are ultimately intended to achieve additional, unrelated objectives. In other contexts, facial recognition systems developed at the border with high quality reference images and vetted identity profiles are later repurposed.

Section 2: Summary of Key Points

Box 8: Facial Verification—Privacy & Policy Implications

- Where replicating existing manual tasks (e.g. passport verification), automated facial recognition can inject racial biases in ways that are systemic and opaque.
- Relative ease and growing socialization of automated verification removes practical barriers to more frequent identification requirements.
- Facial verification can operate as a powerful link, tying travellers to sophisticated digital identities and profiles.
- Facial verification is increasingly embedded in automated border control infrastructure (e.g. baggage drop-offs, electronic gates), allowing for greater implementation of automated border control decision-making.

Box 9: Facial Identification & Screening—Privacy & Policy Implications

- Use of a 1:N comparison system is inherently more intrusive than a 1:1 system even where the same task is being accomplished, because 1:N comparison systematically searches all reference images and can be repurposed.
- Facial identification can operate surreptitiously from a distance, as travellers need not submit any identifying information for verification—all that is required is a video or photograph of the individual's face.
- Biometric screening can lead to serious direct consequences for travellers, and is particularly invasive when automated given persistent error rates and racial bias in 1:N identification.
- Facial identification is an invasive capability that can be repurposed and poses an insidious threat to anonymity and civil liberties.

Box 10: Facial Recognition—Cornerstone to Border Control Automation

- Some form of biometric recognition is integral to automating border control functions. Facial recognition is currently the only biometric process that is sufficiently fast, surreptitious and non-disruptive, while lacking the stigma associated by some with the coercive state functions such as fingerprinting.
- Use of facial recognition as a primary biometric in automated infrastructure can make it more feasible to implement more intrusive biometric recognition (e.g. fingerprinting) as a secondary biometric. As only those travellers that cannot be recognized by their facial images due to errors will be subjected to fingerprinting, the time delay and population-wide objectionable character of fingerprinting is reduced.
- Automating border control infrastructure allows and even invites for the direct application of automated decision-making to travellers without the need for any human intervention.
- Racial, ethnic and gender bias in algorithmic decision-making mechanisms can compound errors in facial recognition, particularly where the same marginalized groups are subjected to the same biases by both algorithmic processes.

Box 11: Transforming Airports into Digital Panopticons

- Where facial recognition is adopted at established customs and immigration identification checkpoints, travellers entering a state are often enrolled into multi-purpose facial recognition systems with domestic, non-border objectives (e.g. general law enforcement).
- Implementation of facial recognition at airport locations where identity confirmation was not historically required must often rely on airlines and other private sector entities, as no established physical checkpoints exist.
- Facial recognition extends identification 'check-ins' to locations where no identification was historically conducted, adding new 'touchpoints' throughout airports. The addition of mobile and web-based applications can extend these 'touchpoints' beyond the airport, reaching into travellers' homes and hotels.
- Facial recognition is increasingly used to record and link locations where identity confirmation was historically conducted by discrete entities and often unrecorded, resulting in a sophisticated movement profile of travellers throughout the border crossing journey.

Box 14: Border Control Systems are Frequently Repurposed

- Facial recognition systems adopted at the border are increasingly repurposed for use beyond the border to achieve a range of public and private sector objectives.
- Many facial recognition systems created for border control objectives become accessible to law enforcement. At times law enforcement objectives are expressly incorporated into these systems as secondary objectives.
- Facial recognition border control systems have been transformed into a *de facto* universal identity, where the facial biometric is central to identity claims made by individuals in their interactions with government and corporate entities.
- Some facial recognition systems rely on the coercive border control context to incentivize voluntary traveller enrollment into facial recognition systems intended to operate as rich digital identity management profiles.

Endnotes.

[1] World Economic Forum, "The Known Traveller: Unlocking the Potential of Digital Identity for Secure and Seamless Travel", January 2018, http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.

[2] Canada, Netherlands & World Economic Forum, "Known Traveller Digital Identity: Pilot Project", June 18, 2019, Slide 11. See also World Economic Forum, "The Known Traveller: Unlocking the Potential of Digital Identity for Secure and Seamless Travel", January 2018, http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf, p 29, Table 8; and Canada Border Services Agency, "Chain of Trust Prototype", *CBSA – Blueprint 2020 Report – December 2018*, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/bp2020/2018/trust-confiance-eng.html.

[3] *IMS Bill*, sub-clause 17(2).

[4] *IMS Bill Digest*, p 17; *IMS Bill*, clause 14 and sub-clause 17(1)); *PJCIS Report*, paragraphs 3.112 – 3.116.

Section 3. Legal & Human Rights Implications

Legally, the border control context is highly coercive in nature. Border control agents are empowered to interfere with travellers in ways that would never be constitutionally acceptable in day to day life. Despite the latitude generally granted to border control entities, facial recognition can push the limits of what is legally permissible.

First, while intrusive searches are permitted at the border, in many contexts these types of searches cannot be applied in a generalized manner, and must be premised on individualized suspicion. As many border control facial recognition implementations are of general application, these could not be justified under the *Charter* if held to be sufficiently intrusive in character to require individualized grounds of suspicion.

Biometrics in general and facial recognition in particular is increasingly recognized as intrusive. On the one hand, biometric templates are often classified as sensitive information and their creation alone increasingly attracts independent and robust legal protection.[1] Even the ephemeral creation and use of a facial template has been held to involve the capture, storage and sensitive processing of personal data.[2] Automated facial comparison is also treated as a use of personal information regardless of whether it leads to the discovery of any new personal information, such as where it does not result in an identification match.[3] Some types of facial recognition searches—those employing a 1:N mode of comparison—will often involve searching the biometric templates of millions of individuals for each and every attempt to identify the individual associated with a facial image query.[4] More generally, the wide-ranging capabilities of facial recognition systems emphasize the intrusive nature of the technology.[5]

Second, despite the broad latitude granted to border control agencies, their services cannot unjustifiably discriminate between travellers on the basis of membership in a protected group.[6] As a technology, facial recognition remains prone to racial bias. When applied at scale, implementing facial recognition across all travellers systematizes any racial biases inherent in the system being employed, subjecting individuals to differential treatment on the basis of membership in a protected group while compounding historical stereotypes.[7] Facial recognition also provides a critical means for applying algorithmic decision-making tools directly to travellers. These various decision-making tools are also equally susceptible to racial biases, compounding any biases in the underlying facial recognition algorithm.[8]

The outcome of these biases will exclude many from the efficiencies and conveniences gained through the adoption of facial recognition technologies on the basis of their race while also undermining rights

to accurate data processing.[9] Travellers may also find themselves referred to more intrusive border control screening mechanisms as a result of these biases, exacerbating racial stereotypes and the stigma experienced by members of marginalized communities when crossing borders.[10] This alone may be sufficient to trigger statutory and constitutional prohibitions against unjust discrimination. In other border control contexts, the general propensity for errors in facial recognition technologies can have serious consequences, such as erroneous rejection of immigration applications,[11] putting at risk the life and security of asylum seekers whose identities are erroneously rejected,[12] or damaging the reputation of falsely identified migrants.[13] These contexts can trigger additional procedural and constitutional safeguards, such as the right to reasons, the right to an impartial decision-maker, and rules of evidence, some of which might be deeply undermined by the unfettered use of facial identification.[14] The impact of matching inaccuracy is all the worse in light of their propensity to fall disproportionately on members of marginalized groups.

The opaque operation of facial recognition systems poses additional legal challenges. While most facial recognition systems remain susceptible to errors and racial biases, there are substantial variations between different algorithms and different implementations.[15] However, Canadian border control agencies have to date refused to provide any transparency regarding error rates in the operation of some facial recognition systems, claiming that to do so would undermine national security.[16] This is inconsistent with transparency policies requiring agencies to publicly explain all components of a high-impact automated decision-making system and describe the nature of the training data that was used in its generation.[17] The impact of facial recognition systems on the rights and interests of individuals and communities will be high. Such systems rely on sensitive biometric data in their creation and operation, impact disproportionately on vulnerable and marginalized communities, involve the private sector in the creation and training of the recognition algorithm, the decision-making process is opaque and analyzes unstructured data (images), and while false negatives will often be subject to human oversight, the effectiveness of this oversight is unclear in the context of facial recognition systems.[18] This level of intrusiveness demands, at minimum, a commensurate level of transparency. In other jurisdictions, by contrast, legislative authorization for facial recognition systems includes explicit requirements for quality control and error thresholds and periodic monitoring requirements.[19]

In many jurisdictions, legislative models are relied upon heavily as legal justification for border control facial recognition. Often changes to legislative instruments are required to permit the use of automated facial recognition where manual processing of travel documents was historically required.[20] In some jurisdictions, human rights instruments or legislated procedural safeguards require a measure of lawful authorization as a precondition to the adoption of facial recognition systems in border control contexts.[21] At times, consent is relied upon as a means of operating outside or beyond a clear grant of authorization.[22] However, the border control context is highly coercive and, as a result, freely given and meaningful consent is difficult,[23] if not impossible, to achieve.[24] In other instances, private sector tools

have been relied upon by border control agencies or even by individual agents for facial recognition purposes on a fully ad hoc basis with no statutory or even institutional framework in place.[25]

Case Studies & Summary of Key Points:

Box 15: Facial Recognition—General Legal Considerations

- The creation, operation and constituent templates of facial recognition systems are increasingly viewed as intrusive and engaging sensitive personal data.
- A culture of secrecy among border control agencies compounds problems arising from the inherent opacity of facial recognition systems, rendering it difficult to assess their error rates, racial biases and overall impact.
- Persistent challenges with racial and demographic bias in facial recognition systems can transform relatively trivial border control applications into systemically biased sorting mechanisms that perpetuate historical stereotypes.
- Errors and bias rates can lead to serious real world harms when used in some border control contexts, such as when investigating the identity of asylum seekers or other migrants.
- In many jurisdictions, facial recognition relies heavily on detailed legislative regimes, often with overt transparency obligations regarding the assessment and publication of error rates.

Box 16: Case Study—Privacy & Systematic Identification at Border Crossings

State agencies are granted broad latitude when assessing traveller identity in border control contexts. Their routine traveller screening decisions do not typically trigger constitutional privacy protections unless these decisions lead to intrusive implications.

Facial recognition is often presented as having minimal privacy impact on the basis that facial images are already ubiquitously used in border control contexts.[26] However, automated facial recognition capabilities are intrusive in general, and categorically more intrusive then the routine collection of a facial image.[27]

Questionable privacy practices have been documented in the creation of datasets used to train many commercial comparison algorithms.[28] Arguably, the latitude granted to border control agencies does not extend to their use of algorithmic tools generated in violation of privacy laws.[29]

If adopted, facial recognition should employ rigorous safeguards and protective design choices. Centralized systems are more intrusive because they provide fewer technical obstacles in case of breach or if, in the future, the capability is expanded or repurposed.[30] Algorithms that can systematically search all images when seeking a match are also more intrusive than those that operate by comparing two known images.[31] The latter are limited to verifying known documents or profiles, whereas the former are capable of identifying anonymous individuals from a distance.

While accuracy has improved in facial recognition systems, challenges with racial bias persist. The *Privacy Act*'s accuracy requirements may require CBSA to ensure in advance and on an ongoing basis that the tools it uses meet certain baseline levels of accuracy in general, and persists despite racial bias.[32]

Facial recognition errors can impact substantial traveller and community interests (e.g. by contributing to discriminatory traveller enhanced screening referral), triggering expansive transparency and human supervision obligations.

Facial recognition systems also pose unique challenges for pseudonymous identities. The threat to undercover officers and witness protection programs created substantial cost overruns and delays in an Australian attempt to develop a facial recognition capability.[33] Asylum seekers also legitimately travel pseudonymously, either to avoid persecution in their country of origin or because they are unable to obtain necessary travel documents. Where facial recognition systems uncover pseudonyms prior to the lodging of an asylum claim, the traveller might be presumed to be acting without justification.[34]

Finally, some facial recognition proposals would extend beyond strict border control objectives. For example, a Canadian pilot program testing a mobile device-based facial recognition 'passport' is ultimately envisioned to become a "*de facto* universal identification system".[35] To the extent these broader outcomes are contemplated in the adoption of facial recognition at the border, they should impact the assessment of the system's general proportionality and legality.

Box 17: Case Study—Clearview AI & Facial Recognition Through the Private Sector

Clearview AI is a company based in California that has created a facial recognition tool that will compare facial images uploaded to its interface by licensed subscribers against its reference dataset of 3 billion facial images collected from social networking and other online sites. Clearview targets government agencies as its main customer base, and has been used by border control agencies in the United States as well as by policing agencies in Canada.

The Clearview service uses a 1:N comparison method. All or most of its 3 billion facial images are searched each time the system is queried with a facial image, and a gallery of the most similar images and related profile data is disclosed in response. Many of these images will also have been used by Clearview in its training dataset.

Clearview collects the images and accompanying profile details in its facial recognition dataset without obtaining meaningful consent. Its initial collection of facial images was accomplished without notice. An opt-out mechanism is available, but does not provide a meaningful form of consent. Absent evidence to the contrary, it can also be presumed that Clearview unlawfully used facial images of Canadians when training its matching algorithm to recognize faces, and continues to do so.

First, individuals have no opportunity to opt-out in a timely manner, as Clearview took no steps to notify individuals that their profile data will be or has been collected.[36] Individuals who do become aware of the opt-out mechanism may be deterred from employing it as Clearview conditions the opt-out on receipt of a driver's license or passport image. An opt-out that requires individuals to provide sensitive identification data to a service provider they have no other relationship with in the absence of documented fraud concerns is ineffective.[37]

Second, Clearview's third party face-matching application has no connection to the context that prompted participation in a social media platform, and cannot reasonably be within the expectations of individuals who have created profiles for social or professional purposes.[38] Clearview's stated mission—to "identify perpetrators and victims of crimes" and to "make communities safer"—has little connection to the primary social or professional purposes of the sites it scraped.[39]

Third, while users may or may not be aware that their profile images and data are public, most platforms prohibit third parties such as Clearview from scraping publicly available data of this nature in their platform terms of use, further bolstering the reasonable expectations of individuals that their data will not be repurposed.[40]

Finally, implied consent is not available where sensitive data or high risk processing are a factor.[41] By providing various public and private agencies with an open-ended identification tool, Clearview uses the facial images it collects to generate sensitive biometric templates and its use and disclosure of these images threatens digital and real-world anonymity in a fundamental manner.[42]

Clearview cannot rely on law enforcement-related PIPEDA exceptions to justify its collection of profile data and generation of facial templates, as this data processing occurs in the absence of any specific request from a state agency.[43] Nor can Clearview ensure that state agencies have sufficient lawful authority to trigger the use of its facial recognition capacity and subsequent disclosure of facial image profiles, as the *Charter* prevents law enforcement agencies from identifying individuals in the absence of probable grounds.[44] The limitless and systematic identification capability provided by Clearview is therefore disproportionate and hence inappropriate.[45]

Box 18: Case Study—Procedural Fairness in Identifying Asylum Seekers

Processing of asylum claims engages high stakes, as erroneous deportation can threaten the life and security of asylum seekers.[46] Facial recognition can be used as a means of disputing the identity presented by individuals including asylum seeker and as a means of denying refugee claims or of other findings of inadmissibility.

Where facial recognition becomes the basis for definitive identification, it can be difficult to meaningfully dispute despite well-documented error rates and biases.[47] Opacity regarding the underlying comparison mechanism and the 'scientific mystique' of automated biometric recognition create a presumption of accuracy that can be challenging for individual travellers to rebut.

While CBSA appears to use facial recognition in aspects of its admissibility assessment process, to date it has recognized the limitations of the technology at an institutional level and decided not to rely on facial recognition as definitive proof of identity.[48] Should this policy change,[49] courts will need to decide whether automated facial matches are sufficient to nullify individual identity claims and what procedural safeguards are demanded if individuals are to know the case they must rebut.[50]

Even where facial recognition is not determinative, its use by border control decision-makers can have implications for the reputation of impacted individuals despite its well-documented inaccuracy rating.[51]

Box 19: Case Study—Racial Bias in PIK Secondary Inspection Referrals

While border control agents are generally granted wide latitude when referring travellers to secondary inspection, the right to substantive equality precludes differential and discriminatory treatment on the basis of a protected ground.

Referral can be random, discretionary or mandatory.[52] Mandatory referrals are triggered by standard customs declarations (declaring food or tariffed imports), or through a negative Integrated Customs Enforcement System [ICES] designation, which is typically issued to CBSA border control officials on the basis of a point system associated with previous customs infractions recorded for the traveller.[53] Discretionary referrals occur where indicators suggest high risk that a border control law has been contravened.

Travellers can be referred to secondary inspection by a CBSA officer, or through an automated tool such as a Primary Inspection Kiosk (PIKs). PIKs automate elements of the customs and immigration process. Where a PIK refers a traveller to secondary inspection, this referral is generally subject to cursory review by a CBSA officer.

Secondary inspection is not considered to be intrusive, and referrals are routinely conducted on a generalized basis without any requirement for justification. The CBSA may theoretically subject all travellers to routine inspection, in practice only a small subset of travellers must contend with secondary screening. Secondary screening can be a discriminatory practice if membership in a protected group is a factor in the referral process.

Facial recognition can be used as a means of supporting manual identification at border control crossings, and is relied upon by PIKs to verify traveller's passports. While it is not clear what considerations drive secondary inspection referrals by PIKs, a failure to verify a traveller's passport may be a factor, even where this failure results from an error in the PIK's facial recognition system.

Even where PIK referrals are subject to review by border control officials, facial recognition errors may raise an undue level of suspicion, prompting more frequent overall referrals.[54] PIKs have been shown to drive selective referral of immigration applicants from Iran, Jamaica, Chad, the Philippines and Nigeria with disproportionate frequency, and despite CBSA manual vetting of these referrals.[55]

Proof of racial profiling is often challenging to establish. On the basis of social evidence, courts may take judicial notice of the general presence of racial prejudice in border control contexts.[56] As a technology, automated facial recognition has not generally overcome its propensity for bias on the basis of race, gender and country of origin. The ability to automatically recognize travellers at PIKs also facilitates the use of other automated assessment tools in the referral process, which are equally susceptible to racial bias.[57]

Facial recognition algorithms might contribute to a higher frequency of referrals resulting from racially biased failure-to-match rates. Their adoption systematically embeds racial bias as a contributing factor into the secondary referral process.

Box 20: Legislative & Regulatory Models

- Some immigration or customs requirements might expressly compel travellers to present travel documentation to border control officials, precluding automated facial recognition absent legislative or regulatory reform.
- Some statutory instruments will expressly place limitations on the adoption of facial recognition for border control objectives, effectively requiring additional legislative or regulatory action as a precondition.
- In the absence of a clear prohibition, a form of consent is sometimes relied upon to extend or adopt facial recognition to travellers or situations outside its legislative reach.
- In some jurisdictions, facial and other biometric recognition implicates human rights to the degree that explicit legislative authorization is required before facial recognition systems can be adopted or altered.
- Some statutory instruments impose detailed safeguards, including data quality requirements for facial images and maximum thresholds for error rates.

Endnotes.

[1] *Biometric Information Privacy Act*, 740 Ill Comp Stat 14/1 (State of Illinois); European Union, Regulation 2016/679, Article 9; Australia, *Privacy Act 1988*, No 119, 1988, section 6 "sensitive information" (d)-(e); *Gaughran v United Kingdom*, Application No 45245/15, February 13, 2020, (ECtHR, 1st Section), paras 69, 85-86); *R (Bridges) v Chief Constable of South Wales Police*, [2020] EWCA Civ 1058, paras 78, 82-94 (in the criminal law context, while noting that *covert* use of facial recognition would be even more invasive and the overt facial recognition surveillance at issue: paras 20, 63-64, 70 and 126).

[2] *R (Bridges) v Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin), para 59:

> The mere storing of biometric data is enough to trigger Article 8 and the subsequent use (or discarding) of the stored information has no bearing. Accordingly, the fact that the process involves the near instantaneous processing and discarding of a person's biometric data where there is no match with anyone on the watchlist (and such data is never seen by or available to a human agent) does not matter. The AFR process still necessarily involves the capture, storage and "sensitive processing" of an individual's biometric data before discarding.

Rev'd on other grounds: [2020] EWCA Civ 1058, paras 88-89.

[3] *R (Bridges) v Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin), para 59, rev'd on other grounds: [2020] EWCA Civ 1058, para 87.

[4] Office of the Privacy Commissioner of Canada, "Disclosure of Information About Complainant's Attempted Suicide to US Customs and Border Protection Not Authorized under the *Privacy Act*", *Complaint under the Privacy Act*, April 19, 2017, paras 85 and 101.

See also: Office of the Information & Privacy Commissioner for British Columbia, In Re Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia, [2012] BCIPCD No 5, Investigation Report F12-01, paras 106-112

And: *Szabó and Vissy v Hungary*, App No 37138/14, January 12, 2016 (ECtHR, 4th Section, 2016), concurring opinion of Judge Pinto de Albuquerque, para 5 (it is not enough to assess the impact of a mass surveillance capability on the individuals who become its targets, but the entirety of the capability must be assessed for its general proportionality).

[5] *Patel v Facebook Inc*, Case No 18-15982 (9th Circuit, 2019), p 17:

> ... the facial-recognition technology at issue here can obtain information that is "detailed, encyclopedic, and effortlessly compiled," which would be almost impossible without such technology. ... Taking into account the future development of such technology as suggested in *Carpenter*, *see* 138 S. Ct. at 2216, it seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cell phone. We conclude that the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests.

[6] *Canada (Attorney General) v Davis*, 2013 FC 40, paras 6-8 and 39-41 (many CBSA activities at the border are 'services' within the context of the *Canadian Human Rights Act*; *Canada (Canadian Human Rights Commission) v Canada (Attorney General)*, 2018 SCC 31, para 57.

[7] Ontario Human Rights Commission, "Under Suspicion: Research and Consultation Report on Racial Profiling in Ontario", April 2017, pp 58-60.

[8] Petra Molnar & Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System", September 26, 2018, *The Citizen Lab & International Human Rights Program*.

[9] *Canada (Attorney General) v Davis*, 2009 FC 1104, para 55, aff'd but not on this point, 2010 FCA 134; *Little Sisters Book and Art Emporium v Canada (Minister of Justice)*, 2000 SCC 69, para 120-121; *Privacy Act*, RSC 1985, c P-21, sub-section 6(2); *Ewert v Canada*, 2018 SCC 30, para 42; Office of the Privacy Commissioner of Canada, "Canada Border Services Agency—Scenario Based Targeting of Travelers—National Security", *Section 37 of the Privacy Act*, Final Report 2017, paras 29-30.

[10] *R v Le*, 2019 SCC 34, paras 97, 106; *R v Thompson*, 2020 ONCA 264, para 63; Ontario Human Rights Commission, "Under Suspicion: Research and Consultation Report on Racial Profiling in Ontario", April 2017, pp 58-60; Evan Dyer, "Bias at the Border? CBSA Study Finds Travellers from Some Countries Face More Delays", *CBC News*, April 24, 2019, https://www.cbc.ca/news/politics/cbsa-screening-discrimination-passports-1.5104385.

Opinion 1/15, *Draft Agreement Between Canada and the European Union – Transfer of Passenger Name Record Data*, July 26, 2017 (CJEU, Grand Chamber), paras 133-141, and in particular paras 164-174:

> ... the extent of the interference which automated analyses of PNR data entail in respect of the rights enshrined in Articles 7 and 8 of the Charter essentially depends on the pre-established models and criteria and on the databases on which that type of data processing is based. Consequently, ... the pre-established models and criteria should be specific and reliable, making it possible ... to arrive at results targeting individuals who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime and should be non-discriminatory.

[11] Petra Molnar and Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System", *The Citizen Lab & International Human Rights Program*, September 2018, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf, pp 52-53.

[12] European Union, Fundamental Rights Agency, "Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security", May 2017, p 78.

[13] Jeremy C Fox, "Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect", *The Boston Globe*, April 28, 2019, https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html; Stewart Bell and Andrew Russell, "Facial Recognition 'Confirmed' Ajaz Developer Was Wanted Crime Boss, but CBSA Couldn't Prove It", *Global News*, December 19, 2019, https://globalnews.ca/news/6301100/confirmed-facial-recognition-but-did-not-proceed-documents/.

[14] Petra Molnar and Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System", *The Citizen Lab & International Human Rights Program*, September 2018, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf, pp 52-53; European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, p 80.

[15] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 3: Demographic Effects", *NIST Interagency Report 8280*, December 2019, https://doi.org/10.6028/NIST.IR.8280.

[16] Evan Dyer, "Bias at the Border? CBSA Study Finds Travellers from Some Countries Face More Delays", *CBC News*, April 24, 2019, https://www.cbc.ca/news/politics/cbsa-screening-discrimination-passports-1.5104385.

[17] Treasury Board of Canada Secretariat, Directive on Automated Decision-Making, effective as of April 1, 2019, Section 6.2 and Appendix C: "Notice", Levels III and IV. For a critique of this tool, see: Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada", *The Citizen Lab & International Human Rights Program*, (September 2020).

[18] These factors have been identified as indicative of 'higher' level impact. See: Government of Canada, Algorithmic Impact Assessment, version 0.8, last modified June 3, 2020, https://canada-ca.github.io/aia-eia-js/.

[19] European Union, Regulations 2019/817 and 2019/818, establishing a framework for interoperability, May 20, 2019, Articles 13(3) and 37; European Union, Regulation 2017/2226, Entry/Exit System (EES), November 30, 2017, Articles 66(1)(a) and 36(b) and (g).

[20] See, for example, Australia, *Migration Amendment (Border Integrity) Bill 2006* and Australia, *Migration Amendment (Seamless Traveller) Regulations 2018*, https://www.legislation.gov.au/Details/F2018L01538; Australia, *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text.

[21] European Data Protection Supervisor, Opinion 9/2017, proposal for a Regulation on the eu-LISA, October 9, 2017, para 14; Council of Europe, High Level Expert Group on Information Systems and Interoperability, Final Report, May 8, 2017, p 12; Case 291/12, *Schwartz v Bochum*, October 17, 2013, (Court of Justice of the European Union, 4th Chamber), paras 35 and 58-61; United States, *Administrative Procedure Act* encoded at 5 USC 500 *et seq*; Harrison Rudolph, Laura M Moy & Alvaro M Bedoya, "Not Ready for Takeoff: Face Scans at Airport Departure Gates", December 21, 2017, *Center on Privacy & Technology*, p 7.

In the criminal context: *S and Marper v United Kingdom*, App Nos 30562/04 and 30566/04, (ECtHR Grand Chamber, 2008), para 99 (ultimately not deciding the matter on the ground of legality); *R (Bridges) v Chief Constable of South Wales Police*, [2020] EWCA Civ 1058, para 91.

[22] World Economic Forum, "The Known Traveller: Unlocking the Potential of Digital Identity for Secure and Seamless Travel", January 2018, http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf;

Canada, Netherlands & World Economic Forum, "Known Traveller Digital Identity: Pilot Project", June 18, 2019; and

Canada Border Services Agency, "Chain of Trust Prototype", *CBSA – Blueprint 2020 Report – December 2018*, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/bp2020/2018/trust-confiance-eng.html;

See also: Susan Wild, Member of Congress, et al, Letter to the Honorable Kevin McAleenan, Acting Secretary of Homeland Security, June 13, 2019 https://wild.house.gov/sites/wild.house.gov/files/CBP%20Facial%20Recognition%20Ltr.%20final.%20.pdf;

Harrison Rudolph, Laura M Moy & Alvaro M Bedoya, "Not Ready for Takeoff: Face Scans at Airport Departure Gates", December 21, 2017, *Center on Privacy & Technology*, p 7; and

Lori Aratani, "DHS Withdraws Proposal to Require Airport Facial Scans for US Citizens", December 5, 2019, *Washington Post*, https://www.washingtonpost.com/local/trafficandcommuting/dhs-withdraws-proposal-to-require-airport-facial-scans-for-us-citizens/2019/12/05/0bde63ae-1788-11ea-8406-df3c54b3253e_story.html.

[23] Office of the Privacy Commissioner of Canada, "MyDemocracy Website Not Designed in a Privacy Sensitive Way", *Complaint under the Privacy Act*, June 19, 2017, paras 63 and 68 (to be meaningful, consent must be premised on information provided in a manner sufficiently timely to allow for its consideration in the exercise of consent); and

European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, pp 33, 80; See also discussion in Section 1.6 of the primary report.

[24] Office of the Privacy Commissioner of Canada, "TV Show Raises Numerous Questions of Consent", *Complaint under the Privacy Act*, June 6, 2016, paras 91 and 97.

[25] Kate Allen, "Toronto Police Chief Halts Use of Controversial Facial Recognition Tool", *The Star*, February 13, 2020, https://www.thestar.com/news/gta/2020/02/13/toronto-police-used-clearview-ai-an-incredibly-controversial-facial-recognition-tool.html; and

Ryan Mac, Caroline Haskins & Logan McDonald, "Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart and the NBA", *BuzzFeed News*, February 27, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[26] Canada Border Services Agency, "Primary Inspection Kiosk–Privacy Impact Assessment: Executive Summary", March 14, 2017:

> While the kiosk and mobile app are new tools, the CBSA's collection of information from travellers arriving by air remains largely unchanged with the exception of the facial photo captured at the kiosk. In fact, by moving to an electronic declaration, the CBSA will be reducing the number of data elements captured to the minimum required for traveller processing.

[27] Automated biometric recognition is increasingly viewed as intrusive: The creation of biometric templates is increasingly receiving independent protection from the collection of facial images in legislation as well as in the application of existing privacy laws. (*Biometric Information Privacy Act*, 740 Ill Comp Stat 14/1 (State of Illinois); European Union, Regulation 2016/679, Article 9; Australia, *Privacy Act 1988*, No 119, 1988, section 6 "sensitive information" (d)-(e)).

Even ephemeral automated collection of live facial images as a probe for facial recognition has been held to implicate privacy rights. (*R (Bridges) v Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin), para 59: "The mere storing of biometric data is enough to trigger Article 8 and the subsequent use (or discarding) of the stored information has no bearing. Accordingly, the fact that the process involves the near instantaneous processing and discarding of a person's biometric data where there is no match with anyone on the watchlist (and such data is never seen by or available to a human agent) does not matter. The AFR process still necessarily involves the capture, storage and "sensitive processing" of an individual's biometric data before discarding." Rev'd on other grounds: [2020] EWCA Civ 1058, paras 87-89.

The European Court of Human Rights has held that enrolling facial images in a biometric recognition system is more intrusive than collection of these images alone. *Gaughran v United Kingdom*, Application No 45245/15, February 13, 2020, (ECtHR, 1st Section), paras 69, 85-86 and 96(technological ability to extract biometric can render indefinite retention of facial images disproportionate); *S and Marper v United Kingdom*, App Nos 30562/04 and 30566/04, (ECtHR Grand Chamber, 2008)(with respect to fingerprints in the criminal context), paras 80 and 82-84).

Facial recognition with systematic identification capabilities are particularly intrusive (*Patel v Facebook Inc*, Case No 18-15982 (9th Circuit, 2019), p 17 "the facial-recognition technology at issue here can obtain information that is "detailed, encyclopedic, and effortlessly compiled," which would be almost impossible without such technology. ... Taking into account the future development of such technology as suggested in *Carpenter*, *see* 138 S. Ct. at 2216, it seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cell phone."

[28] See discussion in Section 1.1.2, at pp 52-55 of the primary report.

[29] See *R v Spencer*, 2014 SCC 43; Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada", *The Citizen Lab & International Human Rights Program*, (September 2020); Petra Molnar and Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System", *The Citizen Lab & International Human Rights Program*, September 2018.

[30] Centralized systems offer greater opportunity for wide-ranging unauthorized access and use:

Office of the Privacy Commissioner of Canada, "Phoenix Pay System Compromised Public Servants' Privacy", June 8, 2017, *Complaint under the Privacy Act*, paras 51-55 an 73;

European Data Protection Supervisor, Opinion 9/2017, proposal for a Regulation on the eu-LISA, October 9, 2017, para 14; and

Case 291/12, *Schwartz v Bochum*, October 17, 2013, (Court of Justice of the European Union, 4th Chamber), para 61.

See also discussion in Section 1.1.1—System architecture: centralized or decentralized, at p 6 of the primary report.

[31] *PJCIS Report*, para 5.54:

> The Committee notes that the Face Identification Service is a one-to-many rather than a one-to-one matching system. It is a system that, in addition to the biometric data of a potential suspect in a crime, necessarily makes use of the biometric data of a number of wholly innocent people. As such, the Face Identification Service could be considered a more significant imposition on the privacy of many Australian citizens.

[32] *Privacy Act*, RSC 1985, c P-21, sub-section 6(2); *Ewert v Canada*, 2018 SCC 30.

[33] Australian National Audit Office, "The Australian Criminal Intelligence Commission's Administration of the Biometric Identification Services Project", *Auditor-General Report No 24*, January 2019, paras 2.18 – 2.22.

[34] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, pp 76-77.

[35] *Alberta v Hutterian Bretheren of Wilson County*, 2009 SCC 37, para 40. See Box 12 for a description of the World Economic Forum's Known Traveller Digital Identity proposal and Canada's ongoing pilot.

[36] In other contexts, conspicuous notification has been required in advance to any collection before an 'opt-out' mechanism can be meaningful: Office of the Privacy Commissioner of Canada, "Policy Position on Online Behavioural Advertising", December 2015:

> The conditions under which opt-out consent to OBA can be considered acceptable are: Individuals are made aware of the purposes for the practice in a manner that is clear and understandable – the purposes must be made obvious and cannot be buried in a privacy policy. ... Individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in OBA.

See also: PIPEDA Report of Findings #2015-002, June 5, 2015.

[37] PIPEDA Report of Findings #2015-002, June 5, 2015, paras 33, 75 and 77-78; *AT v Globe24h.com*, 2017 FC 114, para 16.

[38] PIPEDA Report of Findings #2015-002, June 5, 2015, para 88 (aff'd *AT v Globe24h.com*, 2017 FC 114); PIPEDA Report of Finding #2019-002, April 25, 2019, paras 75-76; 54-57 and 78; and 103-104:

> ... As a consequence, Canadians were not informed that their personal information was at similar risk of being used for political micro-targeting. ... in the case of the TYDL App, there does not appear to be any social aspect to the sharing of friends' information with the App. On this basis alone, the language in the DP was not sufficient to obtain consent to disclosures to the TYDL App."

PIPEDA Report of Findings #2016-003, April 21, 2016, paras 92, 127-132, 136-137 and 139-140 (an organization cannot imply consent when sending unsolicited emails to public business email accounts where those emails are unrelated to the email recipient's business); and

Tamir Israel, "Digital Privacy in Emerging Contexts: Lessons from the SCC's Evolving Section 8 Jurisprudence", February 11, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3335518.

[39] Clearview AI, "Our Mission", last accessed August 30, 2020, https://clearview.ai/.

[40] PIPEDA Report of Findings #2015-002, June 5, 2015, paras 83-89; *AT v Globe24h.com*, 2017 FC 114, paras 75-76.

[41] Office of the Privacy Commissioner of Canada, "Policy Position on Online Behavioural Advertising", December 2015; PIPEDA Report of Findings #2014-011, January 14, 2014.

[42] Tamir Israel & Christopher Parsons, "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada", *The Citizen Lab & Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)*, August 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2901522, Box 2, p 88; *X (Re)*, 2017 FC 1047, paras 145-146, 178 and 181; *R v Spencer*, 2014 SCC 43.

[43] Office of the Information & Privacy Commissioner for British Columbia, In Re Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia, [2012] BCIPCD No 5, Investigation Report F12-01, paras 106-112.

[44] J Michael MacDonald & Jennifer Taylor, Independent Legal Opinion on Street Checks, *Nova Scotia Human Rights Commission*, October 15, 2019; *R v Spencer*, 2014 SCC 43.

[45] *AT v Globe24h.com*, 2017 FC 114, para 74; *R v Spencer*, 2014 SCC 43; *Alberta v Hutterian Bretheren of Wilson County*, 2009 SCC 37, para 40.

[46] United Nations, Office of the High Commissioner for Human Rights, "The Principle of Non-Refoulement Under International Human Rights Law", https://www.ohchr.org/Documents/Issues/Migration/GlobalCompactMigration/ThePrincipleNon-RefoulementUnderInternationalHumanRightsLaw.pdf;

European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, Chapter 4;

Singh v Minister of Employment and Immigration, [1985] 1 SCR 177; and *Atawnah v Canada (Public Safety and Emergency Preparedness)*, 2016 FCA 144, para 31.

[47] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, p 80:

> If the texture of the skin makes it impossible to enrol fingerprints, or results in low fingerprint quality, there is a tendency to assume that the applicant is attempting to avoid fingerprinting and does not want to co-operate with authorities. This may impact the overall sense of trustworthiness and credibility of the applicant in question – according to findings of the FRA field research. Similarly, inaccurate data in databases results in the suspicion that the applicant has intentionally used false documents or given incorrect data.

[48] Stewart Bell and Andrew Russell, "Facial Recognition 'Confirmed' Ajaz Developer Was Wanted Crime Boss, but CBSA Couldn't Prove It", *Global News*, December 19, 2019, https://globalnews.ca/news/6301100/confirmed-facial-recognition-but-did-not-proceed-documents/.

[49] See, for example, Petra Molnar and Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System", *The Citizen Lab & International Human Rights Program*, September 2018, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf, pp 52-53:

> ... 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 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. 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.

[50] For a critique of the European Union approach to fingerprint evidence in immigration contexts, see Section 1.6 of the primary report.

In the Australian context, facial recognition proposals have been criticized for failing to encode a policy prohibiting use of facial recognition as evidence of identity in court proceedings: PJCIS Report, paras 2.68 – 2.69; IGA, para 2.1(f): "Non-evidentiary system: the results of the Identity Matching Services are not designed to be used as the sole basis for ascertaining an individual's identity for evidentiary purposes."

[51] Jeremy C Fox, "Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect", *The Boston Globe*, April 28, 2019, https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html; and

Stewart Bell and Andrew Russell, "Facial Recognition 'Confirmed' Ajaz Developer Was Wanted Crime Boss, but CBSA Couldn't Prove It", *Global News*, December 19, 2019, https://globalnews.ca/news/6301100/confirmed-facial-recognition-but-did-not-proceed-documents/.

[52] Office of the Privacy Commissioner of Canada, "Crossing the Line? The CBSA's Examination of Digital Devices at the Border", *Complaint under the Privacy Act*, October 21, 2019, para 29:

> A BSO will rely on one of three basic types of referrals when referring a traveller for a secondary examination: A 'random referral' is conducted on a random basis to ensure individuals are complying with all CBSA-administered laws and regulations; A 'selective referral' is made by a BSO if the officer believes that an examination is warranted, based on indicators to identify high-risk individuals and goods.; A 'mandatory referral' requires further documentation or examination by the CBSA, or on behalf of other government departments or agencies. Examples may include form completion, duty payment, or if a lookout exists.

[53] *Dhillon v Canada (Attorney General)*, 2016 FC 456, paras 6-8:

> CBSA maintains and monitors enforcement information within the Integrated Customs Enforcement System [ICES]. ... When a traveller enters the country identity documents are scanned and the traveller's name is queried against the ICES records. ... Where a contravention is recorded and a penalty imposed within the ICES a point value is automatically generated. The point value has been determined for each category of offence and is dependent upon a combination of the type of offence, the value of the commodities involved and the type of commodity. The points value becomes the percentage frequency that a computer generated referral to a secondary examination will occur on subsequent entries into Canada.

[54] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, pp 76-77;

Itiel Dror & Kasey Wertheim, "Quantified Assessment of AFIS Contextual Information on Accuracy and Reliability of Subsequent Examiner Conclusions", *National Institute of Justice*, July 2011; and

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

[55] Evan Dyer, "Bias at the Border? CBSA Study Finds Travellers from Some Countries Face More Delays", *CBC News*, April 24, 2019, https://www.cbc.ca/news/politics/cbsa-screening-discrimination-passports-1.5104385. It is not clear what role facial recognition errors might play in this referral process, as the CBSA considers that releasing information of this kind is contrary to national security.

[56] *R v Spence*, 2005 SCC 7, para 5; *R v Le*, 2019 SCC 34 in general and in particular para 83-84 and 97; *Ewert v Canada*, 2018 SCC 30, para 57; *Campbell v Vancouver Police Board (No 4)*, 2019 BCHRT 275, para 112.

[57] See, generally: Petra Molnar and Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System", *The Citizen Lab & International Human Rights Program*, September 2018, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf;

Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada", *The Citizen Lab & International Human Rights Program*, (September 2020);

Kate Crawford, "The Hidden Biases in Big Data", April 1, 2013, *Harvard Business Review*, https://hbr.org/2013/04/the-hidden-biases-in-big-data;

Safiya Umoja Noble, "Algorithms of Oppression", (NY: New York University Press, 2018); and

Sarah Myers West, Meredith Whitaker & Kate Crawford, "Discriminating Systems: Gender, Race, and Power in AI", April 2019, *AI Now Institute*.

Fin.