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

Full Report & Analysis

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 report can be obtained at:
https://cippic.ca/uploads/FR_Transforming_Borders.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 report includes some graphics taken from external sources, which are explicitly identified alongside each graphic.

This report also includes some graphics that were specifically generated to illustrate elements of the report itself. These graphics were created by Tina Salameh, and are specifically identified in the text of the report.

An accompanying overview of this report excerpts key segments from it, and can be found at: https://cippic.ca/uploads/FR_Transforming_Borders-OVERVIEW.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*

TABLE OF CONTENTS

TABLE OF BOXES

Overview & Report Summary

Facial recognition is a rapidly evolving technology with significant intrusive potential that threatens anonymity, substantive equality, privacy and human rights more broadly.

As a technology, facial recognition has become sufficiently accurate to instill confidence in its results by those who rely on it. Yet accuracy challenges persist, especially when employed at scale, and overconfidence in the technology can lead to serious consequences for individuals. More problematically, many recognition algorithms remain plagued by deep racial biases, resulting in a situation where the benefits and harms of facial recognition technology errors are often unevenly distributed while their discriminatory impact compounds historical prejudices and stereotypes. In some border control contexts, errors and racial biases in facial recognition systems can have a devastating impact on individuals.

Facial recognition can surreptitiously identify individuals from a distance, and based on any live or historical image, posing a serious threat to real-world and online anonymity. It can be used to locate enrolled individuals, or to track individual movements through live CCTV camera feeds, identify individuals participating in sensitive activities such as political protests, or to find online social media and other pseudonymous profiles of known individuals, all without the knowledge or participation of those being surveilled. Facial recognition can also provide a convenient mechanism for mapping digital functionality to the physical world, eroding privacy.

> **“ 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**

By enabling digital interfaces—which could include random cameras, ‘augmented reality’ headsets, or fully automated access control gates—to recognize individuals, deep digital profiles can be linked to any individual’s physical presence. The same linking capability can be used to apply sophisticated automated decision-making tools to individuals, impacting their ability to navigate the physical world. Credit ratings can be accessed from in-store cameras, compatibility metrics can be viewed through

emerging augmented reality headsets, and risk assessment scores of often dubious accuracy can be used to determine whether an individual may or may not access an area controlled by an automated gate. Finally, facial recognition can become a powerful national identification, creating a persistent and robust identification for individual interactions with companies and the state.

In a number of examples, the generally intrusive nature of border crossings has been leveraged to create facial recognition capabilities which are then repurposed to achieve a range of public policy and private sector objectives. Border control facial recognition systems can be transformed into crime investigation tools, administrative and corporate identity assurance mechanisms, customer service enhancements, and the backstop to a comprehensive digital identity management capability. Even at the border itself, where the state is generally granted significant latitude to achieve its objectives, the harms of facial recognition systems are frequently underestimated while their effectiveness is inflated.

Despite these challenges, the technology is experiencing a wave of adoption in border control settings around the world. Once adopted, facial recognition capabilities are frequently repurposed to achieve public policy and private objectives unrelated to those that animated their adoption. In light of these developments, this report catalogues evolving border control facial recognition systems and highlights some of the legal and policy challenges raised by their adoption. Its ultimate conclusion is that new border control facial recognition systems should not be adopted at this time, while the proportionality and biases of existing systems should be re-examined. In addition, the report provides some recommendations and best practices that might mitigate some of the harms of facial recognition systems should these be adopted.

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. [1]

[1] Whether this perceived public acceptance is accurate or not remains to be seen. A 2018 survey conducted by the Brookings Institute, for example, found that 44% of respondents viewed the adoption of facial recognition at airports unfavourably while only 31% indicated adoption was favourable. See: https://www.brookings.edu/blog/techtank/2018/10/08/brookings-survey-finds-50-percent-of-people-are-unfavorable-to-facial-recognition-software-in-retail-stores-to-prevent-theft/.

> **“ 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**

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.

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.

> **“ 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, tracking and identifying travellers at numerous points throughout their border control journey and 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.

> “ **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.

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.

> **"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 biometric 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.

> **“ 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 coercive 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 in nature, 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 general purpose national identity. As it remains unclear whether legal and constitutional impediments to this form of repurposing are adequate, the risk of this form of repurposing must be considered when systems of this nature are justified on the basis of border control objectives.

> **“ 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.**
>
> **Australia, Identity-Matching Services, Bill 2018, Explanatory Memo**

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.

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.

> **"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.

Report Roadmap & Summary

This report seeks to document how facial recognition systems are being adopted in border control contexts around the world and to provide an overview of considerations that should govern assessment of their impact should they be adopted.

Structurally, this report opens by describing key features of a facial recognition system. Section 2 of the report then itemizes different ways in which facial recognition is transforming the border control process, drawing on indicative examples from Canada and other jurisdictions. Section 3 provides some general legal and human rights considerations that animate the adoption of facial recognition systems, drawing on case studies as contextual elaboration of these more general principles. Section 3 also provides examples of different statutory regimes that have been used to authorized facial recognition in some jurisdictions around the world. While the first three sections are often descriptive in nature, key policy implications are identified and emphasized throughout. These policy implications are drawn together, summarized and distilled into a list of key findings and recommendations in the concluding section of the report.

Section 1 identifies some important operational features of facial recognition systems while defining relevant terms and technical concepts. Section 1.1 describes various datasets required for the creation and operation of a facial recognition system. For any facial recognition system to operate, a reference dataset must be created. Historical facial images and associated identification and other profile data of travellers will be enrolled in this reference dataset, and will form the underlying basis for facial recognition of travellers in border control interactions. Live facial images of travellers captured in border control interactions will be compared against the historical and pre-vetted facial image profiles in the reference dataset. Several design choices inherent in the creation of the reference dataset can affect the overall impact and effectiveness of a facial recognition system, and these are explored in Section 1.1.1. Training and testing datasets are also required before a comparison algorithm can learn to recognize faces. Section 1.1.2 describes how shortcomings in the constitution of these training and testing datasets can impact the overall accuracy and effectiveness of a facial recognition system.

Section 1.2 describes the mechanics of facial comparison and outlines the implications of some operational design choices. Capturing images at a distance while travellers are in motion, for example, can be faster and more efficient but might undermine accuracy. Section 1.2 also describes different types of facial comparison tasks—namely one to one comparison (1:1), where a live image is compared against a single reference image) and one to many (1:N) comparison, where a live image is compared to all in a gallery of reference images in order to determine which, if any, are similar. These modes of comparison entail different operational considerations and can accomplish a different array of tasks.

Section 1.3 describes the different considerations that must be accounted for when the effectiveness of a facial recognition system is assessed. There are, essentially, two types of error rates that must be accounted for. False positive rates measure how frequently a facial recognition algorithm mistakenly matches a traveller to a historical facial reference image that belongs to someone else. False negative rates, by contrast, measure the frequency at which a facial recognition system fails to confirm that a traveller matches a pre-vetted facial image associated with their identity profile. False positives and false negatives will harm affected travellers and impact system effectiveness in different ways depending on the objective of the facial recognition system, and some of these differences are discussed in section 1.3.1.

Section 1.3.2 describes racial biases in facial recognition algorithms and underscores the importance of assessing demographic-specific error rates when assessing the effectiveness and potential impact of a facial recognition system. Many recognition algorithms exhibit substantially more pronounced error rates when applied to specific demographic groups, and these significant biases are often obscured if the overall error rate of an algorithm is examined on its own. Racial disparities in error rates tend to be more pronounced for false positives than they are for false negatives, yet even for false negatives errors can be substantial when applied systematically to large volumes of travellers. Generally speaking these demographic disparities fall most heavily on members of marginalized groups, and particularly on women in marginalized groups. Notably, the majority of tested algorithms display racial bias, and these disparities become more pronounced when lower quality images (intended to emulate those used at border crossings) are used to assess error rates in lieu of high quality mugshots. Sections 1.3.3 and 1.3.4 describes how many factors can compound racial bias in a facial recognition system. Inferior camera lenses and poor lighting undermine a facial recognition system's general accuracy while travellers with darker skin tones are more heavily impacted. Older (over 70) and younger (under 29) age groups also experience greater error general rates and, in some instances, greater racial disparities.

Measuring the true efficiency and detrimental impact of a facial recognition system must take into account its real-world operation. Section 1.3.6 details how real-world effectiveness and detrimental impact can be impacted by a number of pragmatic factors, some of which are extraneous to the facial recognition system itself but nonetheless impact its capacity to process travellers as intended. These factors must nonetheless be considered when assessing the proportionality of a facial recognition system. Notably, real-world volumes must be taken into account, and even small error rates will yield hundreds of error rates on a daily basis if applied across all travellers.

Section 1.4 outlines different ways in which some facial recognition systems attempt to incorporate consent and individual choice at various stages. Consent can be a factor when travellers are enrolled

into a facial recognition system or program, when facial images are gathered to train an algorithm to recognize facial images, and when an existing system is used to facially recognize a traveller. Many facial recognition systems fail to obtain meaningful consent in each or all of these constituent elements. Opt-out mechanisms have been a particularly inappropriate basis for navigating individual choice. Many of these mechanisms are ineffective, whereas individuals are rarely even aware an option exists or that they or their images are even being subjected to a facial recognition process.

Section 1.6 itemizes ways in which facial recognition systems offer many opportunities for covert application and surreptitious operation, and the impacts that can result from this lack of transparency. Facial recognition is inherently more surreptitious than other core biometrics—individuals can be enlisted into the operation of a facial recognition system from a distance or even on the basis of a historical image. As a result, travellers will be unaware that they are being engaged in a facial recognition process unless substantial steps are taken to notify them. Lack of awareness is furthered by the nature of facial recognition itself, which provides many opportunities for covert application and surreptitious operation. Second, government agencies sometimes shroud the operation of facial recognition systems in additional secrecy, obfuscating key details relating to the accuracy and racial biases of systems being deployed. This in turn undermines public trust in the agencies that operate these systems, especially among members of the marginalized communities most deeply impacted by racially biased facial recognition. Finally, the opaque nature of facial recognition matching determinations makes it difficult for any human decision-maker to question the veracity of those outcomes and correct inevitable errors. Despite the known fallibility of biometric recognition, human decision-makers develop overconfidence and trust in the outcomes of these systems and this undermines the ameliorative effect of including humans in the decision-making loop.

Section 2 describes the different ways in which facial recognition systems are transforming border crossings for travellers, identifying different border control tasks that are incorporating facial recognition systems. Section 2.1 describes the comparative implications of using competing facial recognition capabilities to accomplish various border control tasks. Use of any facial recognition capability can inject inaccuracy and racial bias at a systemic level when used in lieu of manual recognition. However, systems capable of ‘identification’ are generally more intrusive than those limited to ‘verification’. The latter are able to compare a traveller’s live image to one encoded on their passport, verifying that the document is theirs. Systems configured for ‘identification’ can similarly verify travel documents, but are also capable of identifying unknown travellers, screening travellers against biometrically enabled watch-lists, and operating from a distance without any direct traveller interaction. Identification-capable systems are therefore more intrusive.

Section 2.2 documents the various ways in which facial recognition is facilitating the automation of border control functionality. Before automated infrastructure such as electronic gates or customs kiosks can process travellers, it requires a reliable identification mechanism that operates with minimal human intervention. Facial recognition is rapidly becoming the identification method of choice for automated infrastructure, due to its speed of operation and its surreptitious and non-disruptive nature. The ultimate objective is to displace travel documents with facial recognition—your face will be your passport. Automation of border control infrastructure encourages greater reliance on algorithmic decision-making tools to determine traveller's customs, immigration and security status as minimizing human intervention is necessary to fully realize promised efficiency gains. Automated decision-making tools are frequently characterized by racial bias, and these biases can compound biases already inherent in facial recognition. The overall trajectory of automation at the border envisions a sophisticated traveller sorting mechanism with minimal human intervention.

While travellers are frequently called upon to identify themselves at various parts of the border crossing process, section 2.3 explores the ways in which facial recognition is extending the frequency and objectives animating identification requirements. Some border crossings are being transformed with hundreds of touchpoints throughout a given port of entry, and even on travellers' mobile devices. Travellers' interactions with these various touchpoints are also being recorded, linked and aggregated, allowing for a detailed profile of the travellers' border crossing journey.

Section 2.4 briefly describes trusted or known traveller programs that rely on facial recognition to reliably identify travellers who qualify for expedited security screening at border crossings. Such programs leverage the coercive nature of the border control context in order to incentivize voluntary traveller enrollment—travellers consent to enhanced pre-screening and biometric recognition at the border, and in return are granted access to expedited border crossing. Some of these programs are encouraged with the express objective of creating biometric capabilities that extend well beyond the border.

As section 2.5 documents, many facial recognition systems adopted at the border are repurposed for a variety of purposes. Border control systems have been repurposed for general law enforcement investigatory objectives, as a general purpose identity service for private and public sector bodies, as a general surveillance tool and as a digital identity management mechanism. The private sector is frequently enlisted to achieve facial recognition objectives in various border control contexts. Section 2.6 outlines some of these cooperative agreements, and the manner in which the resulting paradigm can legitimize and normalize private sector use of facial recognition for other, unrelated objectives.

While a full legal analysis of all the different legal implications of facial recognition systems is beyond the scope of this report, Section 3 conveys a general impression of how facial recognition systems adopted at the border might interact with the law. Section 3.1 summarizes these legal considerations as they apply to some facial recognition systems. The summary in section 3.1 draws upon more detailed descriptions of legal principles and regimes provided in sections 3.2 and 3.3.

Section 3.2 provides a description of legal principles as they apply generally apply to the border. These principles are contextualized through a series of case studies applying these principles to various border control facial recognition implementations. Section 3.2.1 introduced the primary agencies and legislative instruments that govern border control interactions, and the general objectives that animate them. Notably, the creation and use of biometric facial recognition systems is increasingly seen as more intrusive.

Section 3.2.2 details key factors that trigger protections against arbitrary detention and interference with privacy. The border control context imposes a generally permissive framework for *Charter* protection in light of the recognized need for the state to control who and what enters and departs its borders. Routine interferences with liberty are expected when crossing borders and, as a result, are less stigmatizing when they occur. As a result, border crossings are inherently coercive and intrusive compared to most other contexts governing interactions between individuals and the state. Despite the general latitude granted to border control objectives, the *Charter* places limits on border agencies' ability to interfere with privacy and arbitrarily detain travellers. Routine search and detention is permitted, but more intrusive interferences require some level of individualized justification. The *Privacy Act* imposes additional safeguards that apply in the border context, requiring consent where personal information will be used for purposes that are inconsistent with those for which it was collected. The *Privacy Act* and related guidelines impose additional transparency and accuracy obligations. The intrusiveness, accuracy and transparency of facial recognition when applied systematically to all travellers will be dependent on a number of criteria. Where the private sector is enlisted or private vendor tools are employed, PIPEDA can also impact what is appropriate and constitutionally permissible.

Section 3.2.3 examines procedural and administrative safeguards that might be implicated in the border control context. Particularly where facial recognition is used in asylum or immigration determinations, additional safeguards might be triggered. Section 3.2.4 outlines constitutional and statutory equality rights protections as they apply at the border. Differential treatment of marginalized groups at border crossings can be severely stigmatizing while compounding historical collective distrust of state agencies. Applying facial recognition to all travellers can systematize any racial biases

inherent in the technology, subjecting marginalized groups to differential treatment and perpetuating negative stereotypes. This form of racial bias is not routine, and the damage it imposes on members of marginalized communities can be long-lasting.

Section 3.3 provides examples of different legislative regimes that have been used to authorize and limit facial recognition systems in border control contexts. The use of dedicated legislative regimes can add critical safeguards including accuracy thresholds, limits on racial bias and transparency requirements.

Section 4 closes with an overview that draws together key insights and conclusions found throughout the report. These are summarized in a set of key findings and drawn upon to provide a set of recommendations, reproduced here for convenience.

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 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.[2]

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.

[2] 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.

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."[3] 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.[4]

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

[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:

> 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.

[4] 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.

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.[5]

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.

[5] 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.

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.[6] 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.

[6] 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.

1.1 Testing, Training & Reference Datasets

Before a facial recognition system can be deployed for border control purposes, a reliable reference set of identified facial samples must be compiled. Additionally, a testing and training dataset of facial images is required to teach an algorithm how to recognize facial images.

The **reference dataset** constitutes a collection of biometric facial **samples** [facial images that are stored and, at times, optimized for facial recognition purposes] or **templates** [a numerical representation of key facial features extracted from a facial sample] and associated enrollment data. In border control contexts, the **enrollment data** associated with a stored reference sample will typically include identification information such as the name, address, nationality or passport number of the individual from whom the biometric sample was initially extracted. It can also include additional information, such as data collected during the processing of a visa application, security vetting information, risk assessment outcomes, and more.

This reference dataset typically forms the basis against which border control facial recognition tasks are carried out. That is, when travellers present themselves in person to various border control entities, their faces will be photographed and compared against those stored in this reference dataset.

Before an automated system can carry out this comparison task, it must first **learn** how to recognize faces. It is, of course, impossible for a facial recognition algorithm to memorize every face in every real-world setting in which it might need to be recognized. The learning process therefore optimizes the algorithm on a relatively small '**training dataset**' of matching facial images, until it is able to generalize the matching process to facial images it has not yet encountered. Achieving this inductive matching capability with sufficient real-world accuracy rates requires a large training dataset of millions if not tens of millions of facial images.

Facial recognition in border control contexts typically relies on the pre-existence of these two elements of the facial recognition system: a trained facial recognition algorithm and an enrolled reference dataset. That is, most direct uses of facial recognition in border control contexts will not be able to change the general constitution or operation of the matching algorithm or the reference dataset when attempting to recognize a given traveller. Nonetheless, various design and implementation choices at this initial stage can have serious implications for the overall impact of the facial recognition system. The manner in which these two components of the facial recognition systems are generated can also raise privacy and related ethical concerns.

1.1.1 Reference Datasets: A Biometric Database

A number of choices regarding the architecture, composition and generation of the reference dataset used in a border control facial recognition system can have privacy implications.

System architecture: centralized or decentralized

The reference dataset can be stored in a centralized or a decentralized manner, and the choice of architecture could have implications for the facial recognition system and its privacy impact.

Biometric passports are an example of a decentralized border control reference dataset, where the reference facial images are stored on individual's passports. Since around 2008, the International Civil Aviation Organization (ICAO), which is the primary international entity for standardizing passports, has specified the inclusion of a facial-recognition ready image on compliant passports.[7] The ICAO also requires all passports to contain machine-readable components and to include a passive, contact-less Radio Frequency Identification (RFID) memory chip.[8] ICAO-compliant biometric passports will encode a digital facial image that meets ICAO's quality and size standards onto the passport's RFID chip at the time of its issuance.[9]

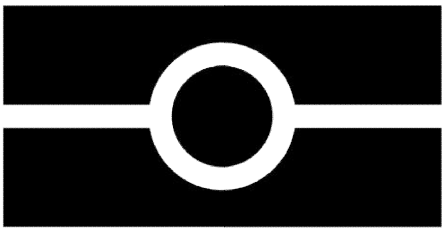

Figure 1: The 'Chip-Inside' Symbol

This symbol adorns most e-passports that contain ICAO compliant biometric-enabled passive RFID chips, typically on the front cover[10]

When a traveller presents an ICAO compliant biometric passport to a border control entity, the facial reference image can be retrieved from the physical passport's RFID chip and compared to a live-captured photograph of the traveller's face. If the traveller is interacting with an automated border control entity, the entire facial recognition process can be automated and machine-readable information can also be accessed from the physical passport, providing the traveller's

[7] The ICAO now requires the inclusion of a facial biometric on compliant passports, while allowing for the optional inclusion of other biometric features (fingerprints, iris features): ICAO Doc 9303, "Machine Readable Travel Documents", Part 9, 7th Edition, 2015, https://www.icao.int/publications/documents/9303_p9_cons_en.pdf, p 4. For a history of Canada's adoption and development of the e-passport, see: Brenda, McPhail, Christopher Parsons, Karen Louise Smith, Joseph Ferenbok & Andrew Clement, "Identifying Canadians at the Border: ePassport and the 9/11 Legacy", (2012) 27(3) *Can J of L and Society* 341.

[8] ICAO Doc 9303, "Machine Readable Travel Documents", 7th Edition, 2015, Part 3, https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf. Doc 9303 requires two images, one of which is specifically designated for the purpose of facilitating biometric recognition processes.

[9] The ICAO standard for facial images is set out in ICAO Doc 9303, "Machine Readable Travel Documents", 7th Edition, 2015, Parts 3 and 9.

[10] The image depicts a contact-less chip (the central circle) contained between two layers of material. It may only be used on ePassports that meet some minimum ICAO specifications: ICAO, "The History of the Chip-Inside Symbol", in (2015) 10(2) *MRTD Report: Balancing Security and Facilitation*, https://www.icao.int/publications/journalsreports/2015/MRTD_Report_Vol10_No2.pdf, pp 18-19.

Image Source: https://upload.wikimedia.org/wikipedia/commons/thumb/f/fb/EPassport_logo.svg/1280px-EPassport_logo.svg.png.

name, passport number, nationality, and place of birth, as well as the travel document's issuing state, issuance and expiry date, and other details.[11] The ICAO is currently exploring whether its standard should be expanded so that more detailed data (such as visas and travel stamps) could be stored on compliant passport RFID chips.[12]

Many states (and non-state entities) have adopted this requirement for officially issued travel documentation, including Canada, which began issuing electronic passports with ICAO compliant facial images in 2013.[13]

Another example of a decentralized border control reference dataset would be the World Economic Forum's Known Traveller Digital Identity (KTDI) proposal, which proposes to store the reference dataset of facial images and enrollment data on a distributed ledger accessible through travellers' individual mobile devices.[14] The digital identity proposal would encode all passport information (including an ICAO compliant facial reference images) on travellers' mobile devices, which would then operate as the primary travel document. Border officials will photograph travellers wishing to rely on their KTDI profile to navigate a border crossing, access the ICAO compliant facial image stored on the traveller's phone, and compare the two using a facial recognition system as a means of confirming that the passport and other information stored on the mobile device's KTDI profile is associated with the traveller in question.[15]

Australia has implemented a similar capability using a centralized reference dataset. The Australian Department of Foreign Affairs and Trade (DFAT) operates a centralized database it generates as part of the Australian passport application process. The database includes

---

[11] ICAO Doc 9303, "Machine Readable Travel Documents", 7th Edition, 2015, Part 3, https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf.

[12] An overview of the ongoing process to expand storage capacity on ICAO compliant on e-passports can be found in: Jasper Mutsaers (Netherlands) & Justin Ikura (Canada), "The Evolution of the ePassport: An Overview of Next Generation ePassport Technology", (2017) 12(2) *ICAO TRIP Magazine* 30, https://www.icao.int/publications/journalsreports/2017/TRIP_Vol12_No2.pdf, pp 30-33.

[13] Passport Canada, "International Comparison of Passport-Issuing Authorities", March 2012, https://www.canada.ca/content/dam/ircc/migration/ircc/english/department/consultations/passport/pdf/2012-03-compare-eng.pdf, p 14:

> All of the Five Nations countries except Canada fully implemented the ePassport between 2005 and 2007. One major incentive for this change was a new requirement adopted in 2006 by the United States, requiring Visa-Waiver Program countries to adopt the ePassport if they wished to continue enjoying visa-free access to the United States. Canada is in a privileged position, as it is currently exempt from this program. This means that Canadians may visit the United States for tourism without a visa, even without holding an ePassport. Canada has been issuing diplomatic and special passports as ePassports since 2009, as a pilot project. The full national implementation of the Canadian ePassport is scheduled to be complete in 2013.

See also: Government of Canada, "History of Passports", last modified April 10, 2014, https://www.canada.ca/en/immigration-refugees-citizenship/services/canadians/celebrate-being-canadian/teachers-corner/history-passports.html: "On July 1, 2013, Passport Canada started issuing a new, even more secure electronic passport, known as the ePassport. This new-generation passport has an electronic chip embedded in the book to provide greater protection against fraud and tampering, and contribute to domestic and international travel security."

[14] 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.

[15] 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.

biometric-ready facial images and associated passport information.[16] An Australian border control entity can photograph a traveller and submit this photograph along with the traveller's passport number to DFAT's facial recognition engine. DFAT's system can query its centralized database until it finds the profile associated with the passport number, and retrieve the facial sample stored in that profile.[17]

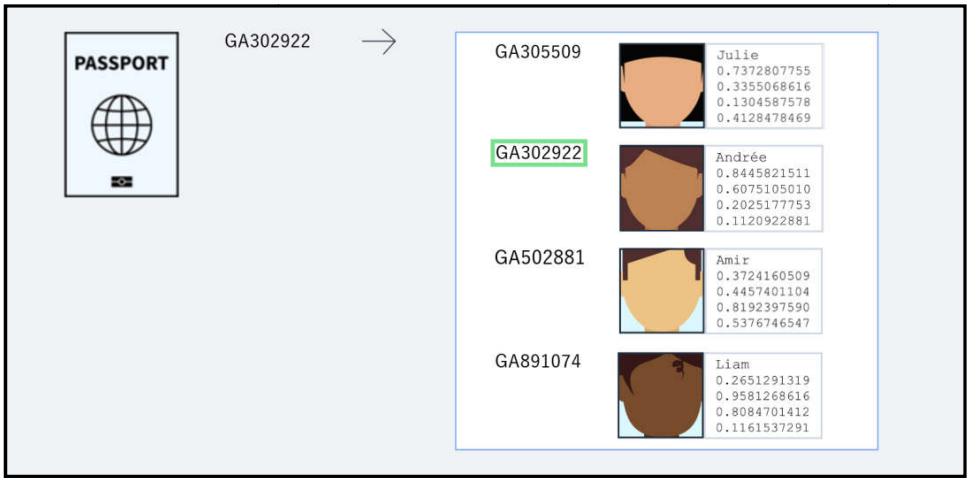

Figure 2: Querying centralized dataset in 1:1 comparison

DFAT's system will then compare the two faces to see if they match.[18]

Driver's license databases represent another example of a centralized reference dataset that has been used for border control functions. Many states in the United States operate centralized databases that include information such as an individual's drivers' license number, name, address and a facial image of that individual. Many of these databases are biometrically-enabled, and include functioning facial recognition systems.[19] The United States Immigration Customs & Enforcement (ICE) has been repurposing these various databases in its attempts to locate undocumented residents.[20] ICE would send a photograph of an undocumented resident to

[16] *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum, "The Australian Passport Office database which holds images collected as part of the Australian passport identity verification process. The Department has arrangements in place for access to this database which is currently used for border clearance. Access to images of Australian citizens supports Contactless Automated Immigration Clearance."

[17] Stephen Gee, Assistant Secretary, Department of Foreign Affairs and Trade, Australia, "Biometric Systems: Can They Be Cheap and Simple?", (2018) 13(1) *ICAO TRIP Magazine* 12, cross-posted to: *Uniting Aviation*, January 9, 2019, https://www.unitingaviation.com/strategic-objective/security-facilitation/cheap-and-simple-biometric-systems/.

[18] Note that this describes DFAT's 1:1 querying capability, whereas the system is also capable of operating in a 1:N manner, meaning that photograph submitted by the border control entity will be compared directly to all facial images in DFAT's database and return all sufficiently similar matches. See Section 1.2.2, below for a description of 1:1 and 1:N comparison.

[19] United States, Government Accountability Office, "Face Recognition Technology", *Testimony Before House of Representatives, Committee on Oversight and Reform*, GAO-19-579T, June 4, 2019, https://www.gao.gov/assets/700/699489.pdf. This report notes that in 2012 41 states and the District of Columbia were reported to have facial recognition capabilities, primarily developed for the purpose of reducing driver's license fraud.

[20] This was uncovered through research by the Georgetown Center on Privacy & Technology: Center on Privacy & Technology, "Making News, Impacting Policy on Facial Recognition Technology", *Georgetown Law*, July 11, 2019, https://www.law.georgetown.edu/news/center-on-privacy-technology-making-news-impacting-policy-with-research-on-police-facial-recognition/; Harrison Rudolph, "ICE Searches of State Driver's License Databases", *Center on Privacy & Technology*, July 8, 2019, https://medium.com/center-on-privacy-technology/ice-searches-of-state-drivers-license-databases-4891a97d3e19.

licensing bodies in several states, who would then compare these photographs to all those contained in their licensing database. If the undocumented resident's photograph is recognized, ICE would become aware of the resident's corresponding name and address.[21]

A centralized biometric capability can provide a powerful tool for connecting data across datasets that are otherwise distinct. The European Union, for example, is in the process of creating a centralized search portal that will interoperate across a number of distinct EU border control databases.[22] The search portal will include a 'biometric matching service', which will centralize storage of biometric templates (including facial images) taken from the disparate databases it seeks to interoperate. EU officials will then be able to biometrically query across any linked databases, substantially increasing the nature and volume of information that can be accessed through a single facial recognition query and the purposes for which it can be queried.[23] The addition of biometric querying also results in new functionality, such as the ability to combine profiles across disparate databases that did not previously share a common identifier.[24]

Centralized architectures can also present challenges in terms of the data transmission necessary for querying the reference dataset. This is particularly problematic where space constraints will not permit for robust and consistent network access. For example, United States Customs and Border Protection found during a pilot project that departure gates at major international airports lacked the network connectivity necessary to provide consistent facial recognition querying of CBP's centralized reference dataset, undermining the viability of the program.[25]

While both centralized and decentralized architectures are susceptible to security breaches, data inaccuracies and repurposing, centralized reference datasets are more readily compromised at a systemic level.

---

[21] Drew Harwell, "FBI, ICE Find State Driver's License Photos Are A Gold Mine for Facial Recognition Searches", July 7, 2019, *Washington Post*, https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[22] European Union, Regulation 2019/818, establishing a framework for interoperability, May 20, 2019; European Union, Regulation 2019/817, establishing a framework for interoperability, May 20, 2019; European Commission, High-Level Expert Group on Information Systems and Interoperability, May 2017; European Commission, Communication on Stronger and Smarter Information Systems for Borders and Security, COM(2016)205, April 6, 2016; European Commission, Twentieth Progress Report Towards an Effective and Genuine Security Union, COM(2019)552, October 20, 2019, pp 4-5.

[23] European Data Protection Supervisor, Opinion 9/2017, proposal for a Regulation on the eu-LISA, October 9, 2017; European Data Protection Supervisor, Statement on the Concept of Interoperability in the Field of Migration, Asylum and Security, May 15, 2017.

[24] European Union, Fundamental Rights Agency, "Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security", May 2017; European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018.

[25] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, pp 16-17.

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.[26] 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.[27] 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.[28] 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.[29] 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.[30]
- **Secondary Purposes:** Both decentralized and centralized systems can be repurposed for administrative, crime control, and digital identification purposes, with systemic implications.[31] Centralized systems, however, can be repurposed for mass querying without the involvement, or even knowledge, of impacted individual.[32] Centralized reference datasets are also susceptible to mass aggregation with other biometrically enabled reference datasets on the basis of the biometric identifier alone.[33] In some jurisdictions, centralization is legally precluded without independent lawful justification.[34]
- 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.

---

[26] 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.

[27] 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.

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

[29] 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."

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

[31] For an example of a decentralized biometric border control system that is designed to be repurposed, see: Box 12 at p 95, below, 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 at p 98, below, which describes Australia's Identity Matching Services initiative.

[32] See footnotes 19 -21 and accompanying texts, above.

[33] 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."

[34] *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."; European Data Protection Supervisor, Opinion 9/2017, proposal for a Regulation on the eu-LISA, October 9, 2017,para 14; European Commission, Twentieth Progress Report Towards an Effective and Genuine Security Union, COM(2019)552, October 20, 2019, p 4.

The enrollment process: Generating a quality reference dataset

The reference dataset will form the basis of future comparisons, and the quality of the images included in this dataset as well as their general fitness for biometric comparison continues to impact the overall accuracy of a facial recognition system despite significant improvements in overall recognition capabilities.[35] Poor quality facial images can also impact disproportionately on particular demographics and individuals from some countries of origin.[36]

Some facial recognition systems include image quality control specifications that are designed to be optimal for facial recognition. In the border control context, the ICAO has established standards that specify factors including facial image size, pose (i.e. the image must be front-facing) and image pixel density so as to assist in the facial recognition process.[37] However, one pilot study in the EU found uneven enforcement of ICAO image standards across different countries.[38] This can be particularly problematic if poor passport images are disproportionately represented in countries of origin in ways that exacerbate existing racial biases in facial recognition accuracy.

However, this level of specification is not always possible to impose, particularly where conditions for generating the reference dataset are not as controlled as the passport issuance process. United States Customs and Border Protection (CBP), for example, populates its facial recognition reference datasets with photographs taken under less controlled conditions, such as those captured during entry inspection as well photographs obtained by the Department of Homeland Security during encounters with travellers where higher quality images are not available.[39] This secondary input method will often

---

[35] For 1:1 facial verification, see: Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, p 2: "For visa images, the column for FNMR at FMR = 0.0001 has been removed. The visa images are so highly controlled that the error rates for the most accurate algorithms are dominated by false rejection of very young children and by the presence of a few noisy greyscale images. For now, two visa columns remain: FNMR at FMR= 10^{-6} and, for matched covariates, FNMR at FMR= 10^{-4}. We have inserted a new column labelled "BORDER" giving accuracy for comparison of moderately poor webcam border-crossing photos that exhibit pose variations, poor compression, and low contrast due to strong background illumination. The accuracies are the worst from all cooperative image datasets used in FRVT."

For 1:N facial identification, see: Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, p 3: "Quality: The low error rates here are attained using mostly excellent cooperative live-capture mugshot images collected with an attendant present. Recognition in other circumstances, particularly those without a dedicated photographic environment and human or automated quality control checks, will lead to declines in accuracy. This is documented here for poorer quality webcam images and unconstrained "wild" images."

For the difference between 1:1 and 1:N facial recognition, see Section 1.2.2, at p 26, and Section 2.1, at p 65, below.

[36] 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, p 7, demonstrates that with high quality images false negative rates can be low, but with lower quality images false negatives impact disproportionately on individuals born in Africa and the Caribbean and, to a lesser extent, on women.

[37] ICAO Doc 9303, "Machine Readable Travel Documents", Part 9, 7th Edition, 2015, https://www.icao.int/publications/documents/9303_p9_cons_en.pdf, p 10.

[38] eu-LISA, "Smart Borders Pilot Project: Report on the Technical Conclusions of the Pilot", Volume 1, (2015), pp 43 and 162: "5 out of 12 issuing countries (42%) typically included photos in their issued documents that had an average eye distance below the threshold. ... Capture of ICAO-compliant live facial images was not strictly necessary for facial image verification but may be required if facial images were to be enrolled for storage in a central database for future use in automated processes. For this purpose the image from the chip on e-passports could be used, although data obtained in the pilot suggested that facial images on documents were sometimes not ICAO-compliant themselves."

[39] United States, Department of Homeland Security, Customs and Border Protection, "Privacy Impact Assessment: Traveler Verification Service (TVS): CBP-TTSA Technical Demonstration Phase II", August 14, 2018, DHS/CBP/PIA-030(e), p 1; United States, Department of Homeland Security, Customs and Border Protection, "Privacy Impact Assessment Update: Traveler Verification Service (TVS): CBP-TSA Technical Demonstration", September 25, 2017, DHS/CBP/PIA-030(d).

be used for foreign travellers, as the state in question will have more ready access to passport quality images of citizens, which are often obtained through the application process and repurposed for border-related facial recognition systems.[40] In pilot testing of CBP's facial recognition system, attempts to match live images of travellers who were solely enrolled through this secondary input method were frequently unsuccessful.[41] While even lower quality images, such as those captured from social media or from live surveillance footage, are sometimes used as inputs for a facial recognition search, some agencies will take steps to prevent the inclusion of these as the underlying reference images.[42] Yet other reference datasets are developed to include an image quality assessment process that evaluates the quality of a given stored reference image, making it possible to determine whether any given image is of sufficient quality to meet the particular objectives sought to be achieved by the facial recognition attempt in question.[43]

Storing templates or storing faces

A reference dataset can consist of facial images or facial templates extracted from those images. Facial templates are a numerical representation of key facial features, and form the basis of automated facial comparison.[44] Facial recognition systems operate on the basis of facial templates, not facial images. That is, a facial recognition system will compare two templates to determine if the two facial images from which they were extracted are a match. In a closed facial recognition system, the underlying facial images are not required and can be discarded, as it is sufficient to retain the facial templates. However, as there is no universal standard for the creation of facial templates, each facial recognition system creates its own templates that are not interoperable with other facial recognition systems.

[40] This is the case with CBP, which will only need to rely on images obtained upon entry or through DHS encounters where passport images cannot be obtained from the United States Department of State: United States, Department of Homeland Security, Customs and Border Protection, "Privacy Impact Assessment: Traveler Verification Service (TVS): CBP-TTSA Technical Demonstration Phase II", August 14, 2018, DHS/CBP/PIA-030(e); United States, Department of Homeland Security, Customs and Border Protection, "Privacy Impact Assessment Update: Traveler Verification Service (TVS): CBP-TSA Technical Demonstration", September 25, 2017, DHS/CBP/PIA-030(d).

[41] United States, Department of Homeland Security, Office of Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-80, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, pp 19-20.

[42] United States, Government Accountability Office, "Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy", May 2016, GAO-16-267, footnotes 26 and 38; United States, Government Accountability Office, "Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, but Additional Work Remains", Testimony before Congressional Committee on Oversight and Reform, June 4, 2019, GAO-19-579T, footnote 7.

[43] The European Union regime monitors the quality o fingerprints enrolled into its centralize EU border control biometric databases using an automated assessment tool designed to check for quality standards, and which rejects any fingerprint that fails to meet its basic standards: European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, p 88. The European Union frameworks for facial recognition also requires that facial image quality standards be established, including for images extracted from passports that purport to meet ICAO standards (that is, including facial images obtained from eMRTD passports): European Union, Regulation 2017/2226, Entry/Exit System (EES), November 30, 2017, Articles 66(1)(a) and 36(b). A pilot test conducted by eu-LISA concluded that while ICAO-compliant facial images were not strictly necessary for a facial recognition system, quality assurance might be required prior to enrollment into a centralized reference dataset: eu-LISA, "Smart Borders Pilot Project: Report on the Technical Conclusions of the Pilot", Volume 1, (2015), p 162.

Australia's facial recognition interface provides a Quality Assurance interface, which permits agencies to submit facial images and returns a list of quality attributes, so that the submitting agency can determine whether the facial image quality is sufficient for its automated recognition purpose: Stephen Gee, Assistant Secretary, Department of Foreign Affairs and Trade, Australia, "Biometric Systems: Can They Be Cheap and Simple?", (2018) 13(1) *ICAO TRIP Magazine* 12, cross-posted to: *Uniting Aviation*, January 9, 2019, https://www.unitingaviation.com/strategic-objective/security-facilitation/cheap-and-simple-biometric-systems/.

[44] See Section 1.2.1 for more details on the comparison process.

A reference dataset that consists of facial templates alone is more secure. If it is compromised, the templates themselves cannot be readily repurposed for facial recognition purposes unless the compromising agent can access the same recognition algorithm. As facial recognitions systems enjoy wider use as access controls, replacing passwords and fingerprints, a compromised facial image repository can also be used as a means of unlocking devices or accounts without authorization.[45]

The use of templates can also limit a facial recognition reference dataset's capacity for being repurposed, as new purposes and objectives will often rely on customized or vendor-specific recognition algorithms that are incompatible with the specific templates that were retained.[46] The majority of border-related facial recognition systems encountered in preparation of this report store the original facial images, rather than the template, in order to facilitate interoperability between different facial recognition algorithms.[47] For example, the United States Transportation Security Administration's (TSA) Biometric Roadmap emphasizes interoperability so that private airlines, who are encouraged to partner in TSA's facial recognition border control system, will not be limited in their choice of vendor.[48] However, United States Customs and Border Protection has currently been piloting

[45] Glyn Moody, "A Major Security Breach Raises a Key Question: What Happens You're your Biometric Data is Exfiltrated from a System?", August 28, 2019, *Privacy News Online*, https://www.privateinternetaccess.com/blog/2019/08/a-major-data-breach-in-the-access-platform-biostar-2-raises-the-question-what-happens-when-your-biometric-data-is-exfiltrated-from-a-system/; Andrew Peterson, "OPM Says 5.6 Million Fingerprints Stolen in Cyberattack", September 23, 2015, *Washington Post*, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.2de9556b3ec4; See also:

> Keeping of biometric data in its original format may pose greater privacy risk than in their template form17 because the templates usually contain less details and offer little secondary use when compared with the original image18. Data users should therefore, as soon as possible, derive biometric data templates from the original biometric samples/images for storage and subsequent use, and discard the original samples/images safely afterwards. The templates derived from biometric samples/images should be stored in such a form from which it is technically infeasible or difficult to convert back to the original graphical image.

Hong Kong, Office of the Privacy Commissioner for Personal Data, Guidance on Collection and Use of Biometric Data, *Guidance Note*, August 2020, https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf, footnote 9 and p 2.

[46] ICAO Doc 9303, "Machine Readable Travel Documents", Part 9, 7th Edition, 2015, https://www.icao.int/publications/documents/9303_p9_cons_en.pdf; NIST IR 8238 pt 2, 2018. See also: Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology", February 2018, *Electronic Frontier Foundation*, p 11.

[47] ICAO Doc 9303, "Machine Readable Travel Documents", Part 9, 7th Edition, 2015, https://www.icao.int/publications/documents/9303_p9_cons_en.pdf, p 8:

> Facial recognition vendors all use proprietary algorithms to generate their biometric templates. These algorithms are kept secret by the vendors as their intellectual property and cannot be reverse-engineered to create a recognizable facial image. Therefore facial recognition templates are not interoperable between vendors — the only way to achieve interoperability with facial images is for the "original" captured photograph to be passed to the receiving State. The receiving State then uses its own vendor algorithm (which may or may not be the same vendor/version as the issuing State used) to compare a facial image captured in real time of the eMRTD holder with the facial image read from the data storage technology in his eMRTD.

See also: , Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, pp 8-9:

> Template diversity*:* The FRVT is designed to evaluate black-box technologies with the consequence that the templates that hold features extracted from face images are entirely proprietary opaque binary data that embed considerable intellectual property of the developer. Despite migration to CNN-based technologies there is no consensus on the optimal feature vector dimension. This is evidenced by template sizes ranging from below 100 bytes to more than four kilobytes. This diversity of approaches, suggests there is no prospect of a standard template something that would require a common feature set to be extracted from faces. Interoperability in automated face recognition remains solidly based on images and documentary standards for those, in particular the ICAO portrait [26] specification deriving from the ISO/IEC 19794-5 Token frontal [23] standard, which are similar to certain ANSI/NIST Type 10 [25] formats.

[48] United States, Transportation Security Administration, "TSA Biometric Roadmap: For Aviation Security & The Passenger Experience", September 2018, p 19:

> Interoperability
>
> TSA biometric solutions must be compatible with current TSA systems and processes, interoperable with mission partner systems (e.g., CBP, OBIM), and maximize the use of secure and accessible interfaces to facilitate the exchange of biometric data across stakeholders. Support for various data types, versions, and structures should not favor any particular vendor or solution set. Some airlines and airports are willing to collect images, transmit data, and receive matching results on passenger biometrics but may be reluctant to store them due to cost or risk. TSA shall support cyber-secure solutions that enable the use of passenger biometrics across airlines and airports rather than proprietary solutions that may require passengers to enroll multiple times.

a number of facial recognition border control implementations, and these have been designed to retain facial templates alone, while actual images are discarded once the template is extracted.[49]

Permanence, currency & size of the reference dataset

Reference datasets can be developed with varying ability to update or change images, with potential implications for the accuracy of the overall facial recognition system. Ageing can undermine recognition quality and as a result the use of current reference images is important.[50]

For example, ICAO-compliant facial images are encoded onto physical passports at the time of issuance and can only be replaced upon the issuance of a new travel document.[51] As a result, the currency of the image being used as a basis for facial recognition remains linked to the passport renewal period.[52] Other reference datasets are more flexible in constitution, but lack formal mechanisms for ensuring historical images are periodically replaced with more current images, impacting both the currency of images and overall volume of images contained in the reference dataset at any given point of time.[53] The lack of recent images can undermine the accuracy of a facial recognition system, as ageing, plastic surgery or other cosmetic changes.[54] Similarly, for some modes of facial recognition the overall size of the reference dataset being searched can undermine the accuracy of the algorithm.[55]

---

[49] United States, Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 6: "TVS will then generate biometric templates for each gallery photograph and store the template, but not the actual photograph, in the TVS virtual private cloud (VPC) for matching when the traveler arrives or departs."

[50] For a description of the impact ageing can have on facial recognition accuracy, see Section 1.3 and specifically page 42, below.

[51] ICAO Doc 9303, "Machine Readable Travel Documents", Part 9, 7th Edition, 2015, https://www.icao.int/publications/documents/9303_p9_cons_en.pdf, p 12: "This edition of Doc 9303 is based on the assumption that eMRTDs will not be written to after personalization. Therefore the personalization process SHOULD lock the contactless IC as a final step. Once the contactless IC has been locked (after personalization and before issuance) no further data can be written to, modified or deleted from the contactless IC. After issuance a locked contactless IC cannot be unlocked."

[52] In Canada, ePassports are issued for either 5 or 10 years: Government of Canada, "The Canadian ePassport", last modified September 5, 2014, https://www.canada.ca/en/immigration-refugees-citizenship/news/video/canadian-epassport.html: "With the Canadian ePassport, you have the option of a 5- or 10-year validity period, you receive a higher-security document and you can continue to travel freely." However, children under the age of 16 may only obtain passports with a 5-year validity period: Government of Canada, "History of Passports", last modified April 10, 2014, https://www.canada.ca/en/immigration-refugees-citizenship/services/canadians/celebrate-being-canadian/teachers-corner/history-passports.html: "Can children's ePassports also be valid for 10 years? No. All children under the age of 16 receive ePassports that are valid for a maximum of five years."

[53] Australia, for example, only recently adopted a mechanism for retiring historical images in its reference dataset: Stephen Gee, Assistant Secretary, Department of Foreign Affairs and Trade, Australia, "Biometric Systems: Can They Be Cheap and Simple?", (2018) 13(1) *ICAO TRIP Magazine* 12, cross-posted to: *Uniting Aviation*, January 9, 2019, https://www.unitingaviation.com/strategic-objective/security-facilitation/cheap-and-simple-biometric-systems/.

[54] Studies suggesting meaningful deterioration in the ability to recognize individuals accurately based on reference images that were enrolled 8-9 years earlier on average, and within 5-6 years for some. See: Lacey Best-Rowden & Anil K Jain, "Longitudinal Study of Automatic Face Recognition", 2018 40(1) *IEEE Transactions on Pattern Analysis and Machine Intelligence* 148.

[55] This is more a factor where 1:N modes of recognition are employed (see a description of 1:1 and 1:N recognition in Section 1.2.2 at page 26, below): Stephen Gee, Assistant Secretary, Department of Foreign Affairs and Trade, Australia, "Biometric Systems: Can They Be Cheap and Simple?", (2018) 13(1) *ICAO TRIP Magazine* 12, cross-posted to: *Uniting Aviation*, January 9, 2019, https://www.unitingaviation.com/strategic-objective/security-facilitation/cheap-and-simple-biometric-systems/. However, recent improvements suggest that 1:N some algorithms are yielding increasingly accurate results when applied to reference datasets of 12 million images: 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, pp 2-3: "With good quality portrait photos, the most accurate algorithms will find matching entries, when present, in galleries containing 12 million individuals, with rank one miss rates of approaching 0.1%. ... As the number of enrolled subjects grows, some mates are displaced from rank one, decreasing accuracy. As tabulated later for N up to 12 million, false negative rates generally rise slowly with population size."

Enrollment data accompanying reference facial images

A range of data can be included directly in the reference dataset. At minimum, this is likely to include pre-vetted biographical information.[56] In other instances, more detailed and voluminous information can be associated with a given facial image. The ICAO's biometric passport specification, for example, currently requires certain core passport information (passport number, name, nationality, etc) to be encoded alongside the ICAO-compliant facial image on RFID chips contained in biometric passports.[57] The ICAO is currently exploring an expansion of its specification to allow for the inclusion of digitally encoded travel stamps and visas.[58] Additional details can be enrolled into a reference dataset. The WEF's KTDI proposal, for example, envisions the inclusion of credit ratings, education accreditations, and vaccination details obtained from a traveller's bank, University or health institution, respectively.[59]

Enrollment data can expand as a result of indirect measures, often difficult to envision at the time of the facial recognition system's creation. For example, a consequence of the European Commission's proposal to merge several European Union-wide information technology systems into one central searchable repository will be an expansion in the amount and type of personal information that will become available on the basis of a biometric search.[60]

Finally, the ability to update and correct enrollment data is relevant. In any facial recognition system, it must be presumed that enrollment errors will occur, and these have been documented with respect to at least some border control systems. One small-scale survey of EU-wide biometric systems that are largely generated in border control contexts found that between 50-60% of questioned border control officials had encountered incorrect enrollment data on at least a few occasions.[61] These enrollment data errors were attributed to a wide range of factors including spelling errors, interpretation errors,

[56] The broader vetting mechanisms that various states undertake when issuing travel-related documents are mostly outside the scope of this report, but are outlined in: ICAO TRIP, "Guide on Evidence of Identity", Ver 5.3, May 2018, https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20Guidance%20on%20Evidence%20of%20Identity.pdf.

[57] ICAO Doc 9303, "Machine Readable Travel Documents", Part 9, 7th Edition, 2015, https://www.icao.int/publications/documents/9303_p9_cons_en.pdf, p 12.

[58] Jasper Mutsaers (Netherlands) & Justin Ikura (Canada), "The Evolution of the ePassport: An Overview of Next Generation ePassport Technology", (2017) 12(2) *ICAO TRIP Magazine* 30, https://www.icao.int/publications/journalsreports/2017/TRIP_Vol12_No2.pdf, pp 30-32.

[59] See Box 12 at p 95, below for more details.

[60] The initiative will merge six large-scale European Union-wide information systems addressing matters such as visa information, entry/exit, travel information and criminal records: European Commission, "Communication from the Commission to the European Parliament, Eighteenth Progress Report towards an effective and genuine Security Union", March 20, 2019, COM(2019)145 Final. While only some of these systems were independently facial recognition enabled, their merger will allow for facial recognition capabilities to apply across all included information systems through a Common Identity Repository (CIR) and Multiple Identity Detector (MID) functionality designed to link profiles cross-system: European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, p 9 and Table 2, p 25.

[61] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, p 82, figure 12. Another 2016 small-scale survey conducted by EU FRA at various EU border crossing points found that between 40-50% of border control officers had encountered inaccurate or outdated information or a mismatch between information and identity when using two key EU border control databases (see Figure 11).

See also: European Union, Fundamental Rights Agency, "Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security", May 2017, p 32: "According to public servants interviewed as part of FRA's project on biometrics, a more frequent problem is that the data profile of another person has been attached to the fingerprints, both in relation to Eurodac and VIS. Such a wrong link can result from administrative mistakes."

technical difficulties, and, notably, to workload strain arising from high volumes of travellers.[62] Erroneous enrollment data can lead to serious consequences for individuals, in part due to its association with a biometric matching system. For example, Eurodac is an EU-wide border control automated biometric system which records a traveller's fingerprints as well as the time and place in which these were recorded. Eurodac matches have been held on multiple occasions to invalidate asylum claims on the basis of this enrollment data.[63]

To the extent that enrollment remains under the control of the country that generates the facial recognition apparatus in question, mechanisms must be in place to ensure enrollment data remains accurate. These correction mechanisms must also extend to facial recognition systems that are shared with other jurisdictions, where updates and corrections to enrollment data become more challenging to implement. Additionally, some facial recognition proposals envision the use of a blockchain ledger as a means of encoding some types of data.[64] As blockchain technologies are inherently resistant to the retroactive correction or deletion,[65] erroneous or outdated information might be indelibly linked to an individual by means of their facial biometric.

1.1.2 Training & Testing Datasets: Data Quality & Racial Bias

Before a facial recognition system can be deployed, it must learn how to recognize faces. This involves training an algorithmic learner on a set of facial images.[66] The training dataset of facial images used in the learning process can have implications for the facial recognition system.

It is impossible for an algorithm to memorize every facial image that it might need to associate with a given individual in real-world scenarios. The algorithm must therefore learn a generalized skillset—the

[62] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, p 83:

> Many factors affect the reliability of the alphanumerical data in a system, such as: spelling errors; wrong sex or nationality registered; lack of documents provided by a person; incorrect or incomplete information provided by the data subject; lack of interpretation in case of language difficulties leading to data entry errors; technical deficiencies; incorrect transcription of names into the Latin alphabet; cultural norms determining the usage of first and second names; recording of birth dates when the precise date is unknown; lack of skills and training; the common format for data transmissions is not followed; increased workload and strain on the staff recording and dealing with data. The last point was particularly evident following the large number of arrivals in 2015.

[63] See a more detailed discussion of Eurodac in Section 1.6 Covert Operation & Opaque , below.

[64] 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. The KTDI proposal, which is described in greater detail in Box 12 at p 95, below, seeks to encode identity attestations from various border control and private sector entities around the world on a blockchain ledger.

[65] 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 24.

[66] Note that terminology used to describe the mathematical models that form the basis for facial recognition and other related types of algorithmic decision-making systems vary, with many terms used interchangeably. These differing and often overlapping terms are discussed in: 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*. Technically, the learning algorithm is a mathematical formula whose final parameters are unknown at the outset, but that is capable of learning from data in order to complete a 'task' (in this instance, the task is to recognize faces). A more detailed description of the general operation of the machine learning process and its various challenges is beyond the scope of this report, but can be found in: Ian Goodfellow, Yoshua Bengio & Aaron Courville, "Deep Learning" (Boston: MIT Press, 2016), https://www.deeplearningbook.org/, Chapter 5; Pedro Domingos, "A Few Useful Things to Know About Machine Learning", (2012) 55(10) *Communications of the ACM* 78, doi:10.1145/2347736.2347755; and Mei Wang & Weihong Deng, "Deep Face Recognition: A Survey", *version 8*, February 12, 2019, https://arxiv.org/pdf/1804.06655.pdf.

ability to recognize faces it has not seen or experienced before. To achieve this generalized capability, the learning algorithm will need to experience face matching exercises. A training dataset of facial images is required for this learning process. The size, composition and method of acquisition of the training dataset can be relevant to an overall assessment of the facial recognition system and its privacy implications.

Public availability of sufficiently large training datasets remains limited

While improvement in algorithmic learning continue to develop at a rapid pace, the volume of data in the training dataset continues to play a pivotal role in the overall accuracy of the facial recognition system.[67] Most learning processes still require a training dataset with millions of images belonging to thousands or tens of thousands individuals in order to achieve meaningful real-world accuracy rates.[68] There are a number of publicly available datasets that have been curated for the specific purpose of facilitating the facial recognition learning process,[69] whereas some training datasets are collected from public-facing photo sites such as Flickr.[70] The overall size of these publicly available training datasets remains limited, and online platforms such as Google and Facebook reportedly train their facial recognition algorithms on training datasets comprising privately held facial images relating to millions of their individual users.[71] The provenance of these private and public training datasets has become controversial (see section 1.4.2, below).

Training datasets are racially biased & fail to represent facial image features

The composition of the training dataset remains an important factor in the overall accuracy of the facial recognition system. A training dataset that contains only racially biased, highly standardized, front-facing facial images will not provide sufficient diversity of factors for a facial recognition system to achieve real-world results. Despite ongoing advancements, facial recognition systems continue to struggle with consistent accuracy across racial and gender demographics.[72] Racially biased testing datasets which lack demographic diversity can therefore severely undermine the overall accuracy of the resulting facial recognition system.[73] In addition, facial image features such as pose, illumination

[67] Pedro Domingos, "A Few Useful Things to Know About Machine Learning", (2012) 55(10) *Communications of the ACM* 78, doi:10.1145/2347736.2347755, pp 84-85.

[68] Rajeev Ranjan, Swami Sankaranarayanan, Ankan Bansal, Navaneeth Bodla, Jun-Cheng Chen, Vishal M Patel, Carlos D Castillo & Rama Chellappa, "Deep Learning for Understanding Faces", (2018) *IEEE Signal Processing Magazine* 66, p 74, table 2; Mei Wang & Weihong Deng, "Deep Face Recognition: A Survey", version 8, February 12, 2019, https://arxiv.org/pdf/1804.06655.pdf, p 12: "The prerequisite of effective deep FR is a sufficiently large training dataset. Zhou et al. suggested that large amounts of data with deep learning improve the performance of FR. The results of Megaface Challenge also revealed that premier deep FR methods were typically trained on data larger than 0.5M images and 20K people."

[69] Rajeev Ranjan, Swami Sankaranarayanan, Ankan Bansal, Navaneeth Bodla, Jun-Cheng Chen, Vishal M Patel, Carlos D Castillo & Rama Chellappa, "Deep Learning for Understanding Faces", (2018) *IEEE Signal Processing Magazine* 66, p 73, table 1.

[70] Olivia Solon, "Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent", March 12, 2019, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.

[71] Mei Wang & Weihong Deng, "Deep Face Recognition: A Survey", version 8, February 12, 2019, https://arxiv.org/pdf/1804.06655.pdf, p 5.

[72] Patrick Grother, "Bias in Face Recognition: What Does That Even Mean? And Is It Serious?", *Biometrics Congress*, November 2, 2017, slide 14.

[73] 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 (note that this study did not test for root causes in facial recognition demographic bias, and was agnostic as

and expression, level of facial occlusion and image blurring/motion continue to undermine accurate facial recognition.[74] A training dataset that fails to reflect this variety of facial images will undermine a facial recognition system's real-life ability to recognize individuals.

Variations in skin tone and bone structure continue to present a challenge for facial recognition systems, leading to discriminatory systems with uneven recognition on the basis of geographic origin, gender and race.[75] Some evidence suggests that training datasets comprised exclusively of specific ethnicities or datasets that are labelled for racial differences can mitigate racial discrimination in the algorithmic learning process.[76] However, many of the largest publicly available training datasets continue to reflect images of celebrities at public events, which are widely available online but represent a relatively homogenous demography.[77] The mistaken presumption that large online

to the training process for the recognition algorithms it assessed (p 9: "We did not train algorithms. ... We did not attempt, or invite developers to attempt, mitigation of demographic differentials by retraining the algorithms on image sets maintained at NIST. We simply ran the tests using algorithms as submitted."), however, it found that some (but not all) algorithms developed in China exhibited lower false positive rates with respect to East Asian faces, and indicates that this suggests reference dataset diversity can mitigate bias (pp 7 and 39: ")). See also: Brendan F Klare, Mark J Burge, Joshua C Klontz, Richard W Vorder Bruegge & Anil K Jain, "Face Recognition Performance: Role of Demographic Information", (2012) 7(6) *IEEE Transactions on Information Forensics & Security* 1789, https://doi.org/10.1109/TIFS.2012.2214212, an early study suggesting that training recognition algorithms on demographically balanced datasets is not sufficient to improve bias while training recognition algorithms exclusively on a specific ethnicity does improve its accuracy with respect to that specific demographic.

[74] The ability to navigate three key variables—Pose, Illumination and Expression (PIE)—remains integral to the accuracy of face detection and facial recognition systems. Pose indicates facial orientation or angle with respect to the image-capturing device. Illumination indicates differences in the amount of light reflected from the skin of the targeted face, leading to variations in shadows and shading on the facial sample based on differences in background lighting and camera sensitivity. Expression refers to variation in the appearance of the face itself, affecting the apparent geometric shape and position of key facial features in the target facial sample. Facial occlusion also remains a factor. Occlusion refers to natural or artificial hindrances that block facial features, either purposefully or unintentionally, in a digital image. Occluding objects can include accessories such as scarves or eye glasses, or natural features such as a raised hand, or newly grown facial hair. Blurry images similarly present a challenge to recognition accuracy.

Note that significant progress has been made in terms of accurate facial recognition along each of these variables, yet challenges persist. See: Mei Wang & Weihong Deng, "Deep Face Recognition: A Survey", version 8, February 12, 2019, https://arxiv.org/pdf/1804.06655.pdf, p 3: "Although deep-learning-based approaches have been widely used due to their powerful representation, Ghazi et al. proved that various conditions, such as poses, illuminations, expressions and occlusions, still affect the performance of deep FR and that face processing is beneficial, particularly for poses."; Rajeev Ranjan, Swami Sankaranarayanan, Ankan Bansal, Navaneeth Bodla, Jun-Cheng Chen, Vishal M Patel, Carlos D Castillo & Rama Chellappa, "Deep Learning for Understanding Faces", (2018) *IEEE Signal Processing Magazine* 66, p 79 (with respect to the ability of face analytic algorithms to detect key facial features: "Most data sets contain only a few thousand images. A large-scale annotated and unconstrained data set will make the face alignment system more robust to the challenges, including extreme pose, low illumination, and small, blurry face images.").

[75] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", NIST Interagency Report XXXX DRAFT, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, p 220; Patrick Grother, "Bias in Face Recognition: What Does That Even Mean? And Is It Serious?", *Biometrics Congress*, November 2, 2017, slide 14 ("Face recognition algorithms are sensitive to demographics: Race > Age > Sex"); 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; 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, p 2:

> Contemporary face recognition algorithms exhibit demographic differentials of various magnitudes. Our main result is that false positive differentials are much larger than those related to false negatives and exist broadly, across many, but not all, algorithms tested. Across demographics, false positives rates often vary by factors of 10 to beyond 100 times. False negatives tend to be more algorithm-specific, and vary often by factors below 3.

See also: Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, pp 168 and 220. With respect to face detection algorithms, see: Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", (2018) 81 *Proceedings of Machine Learning Research* 1, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[76] Brendan F Klare, Mark J Burge, Joshua C Klontz, Richard W Border Bruegge & Anil K Jain, "Face Recognition Performance: Role of Demographic Information", (2012) 7(6) *IEEE Transactions on Information Forensics & Security* 1789, https://doi.org/10.1109/TIFS.2012.2214212, p 10; See also: 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, p 7:

> A number of algorithms developed in China give low false positive rates on East Asian faces, and sometimes these are lower than those with Caucasian faces. This observation - that the location of the developer as a proxy for the race demographics of the data they used in training - matters was noted in 2011, and is potentially important to the reduction of demographic differentials due to race and national origin.

[77] Mei Wang & Weihong Deng, "Deep Face Recognition: A Survey", version 8, February 12, 2019, https://arxiv.org/pdf/1804.06655.pdf, Table VII and p 12:

datasets will be representative of the population is a recognized source of bias in machine learning processes more generally, and is not limited to facial recognition.[78]

Testing datasets raise similar implications

Similar considerations relate to any testing datasets or benchmarks used to assess facial recognition systems. These datasets must be distinct from the training dataset, as the system must be tested on its generalized ability to recognize faces it has not yet seen. However, despite this caveat, the training dataset must nonetheless reflect a sufficient diversity of facial features and demographic constitution to ensure that the facial recognition system is tested under conditions that emulate the real-world situations in which the system will operate. The lack of racial and gender diversity in testing datasets has been criticized. For example, one of the most widely used testing benchmarks, the 'LFW – Labelled Faces in the Wild',[79] is estimated to consist of 77.5% male and 83.5% white subjects.[80]

Some benchmark datasets with more racial diversity have emerged, but these remain smaller in terms of the number of facial images they contain or their variety along other factors such as pose, illumination, and other factors.[81] The United States Department of Commerce's National Institute of Standards and Technology (NIST) has been operating an ongoing test of various commercial recognition algorithms, and has in recent years tracked demographic impact on the basis of country of origin and other factors.[82] NIST has been criticized, however, for including facial images in its testing dataset without the consent or participation of the individuals pictured in the images.[83]

Data bias usually exists in most databases with the reason that only partial distribution of face data is covered by each database. Most datasets (VGGface2 and MS-celeb- 1M) are collected from Websites and consist of celebrities on formal occasions: smiling, make-up, young, and beautiful. They are largely different from databases captured in the daily life (Megaface). Such significant discrepancies cause a poor performance in applications when directly adopting the pre-trained models. Another universal but serious data bias is uneven distributions of demographic cohorts (e.g., race/ethnicity, gender, age). According to [109], [64], [17], the female, Black, and younger cohorts are usually more difficult to recognize for non-deep FR algorithms due to this data bias.

[78] See, for example, 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.

[79] Brendan F Klare, Ben Klein, Emma Taborsky, Austin Blanton, Jordan Cheney, Kristen Allen, Patrick Grother, Alan Mah, & Alin K Jain, "Pushing the Frontiers of Unconstrained Face Detection and Recognition: IARPA Janus Benchmark A", (2015) *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* 1931, p 1: "A key step towards advancing unconstrained face recognition was the release of the "Labeled Faces in the Wild (LFW) dataset in 2007."

[80] Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", (2018) 81 *Proceedings of Machine Learning Research* 1, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, p 3.

[81] Brendan F Klare, Ben Klein, Emma Taborsky, Austin Blanton, Jordan Cheney, Kristen Allen, Patrick Grother, Alan Mah, & Alin K Jain, "Pushing the Frontiers of Unconstrained Face Detection and Recognition: IARPA Janus Benchmark A", (2015) IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 1931, this only includes 500 subjects.

[82] While some degree of racial bias was assessed by NIST in its 1:1 facial verification test since 2017, NIST released an analysis focused explicitly on demographic bias in 1:1 and 1:N recognition in 2019: 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.

[83] Os Keyes, Nikki Stevens & Jacqueline Wernimont, "The Government is Using the Most Vulnerable People to Test Facial Recognition Software", March 17, 2019, *Slate: Future Tense*, https://slate.com/technology/2019/03/facial-recognition-nist-verification-testing-data-sets-children-immigrants-consent.html.

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.

1.2 The Mechanics of Facial Comparison

Once a facial algorithm has been trained and a reference dataset has been generated, the facial capture and comparison process can raise additional considerations.

1.2.1 Facial recognition in operation

The mechanics of the facial recognition process can be examined as three discrete steps. First, a traveller's face needs to be captured, often from a live video feed or a digital photograph taken in a customs kiosk. Second, a biometric representation or template is extracted from the captured facial image. Finally, the captured facial template is compared against one or more stored reference facial templates.

Capturing & detecting a traveller's facial image (creating the facial probe).

This initial operational step involves detecting and isolating an individual's face by automated means and **capturing** it as a source for input (a biometric or facial '**probe**') into a biometric recognition system. The face can be detected in a digital image or physical photograph, or it can be recorded and detected directly from the individual through the use of a video or static digital camera or similar **capture apparatus**. The **face detection** algorithm must be able to find and isolate the face of an individual from amongst numerous objects and other background elements including landscape, trees, or a torso, and, in some instances, must be able to account for multiple individuals of varying heights and head shapes at the same time.[84]

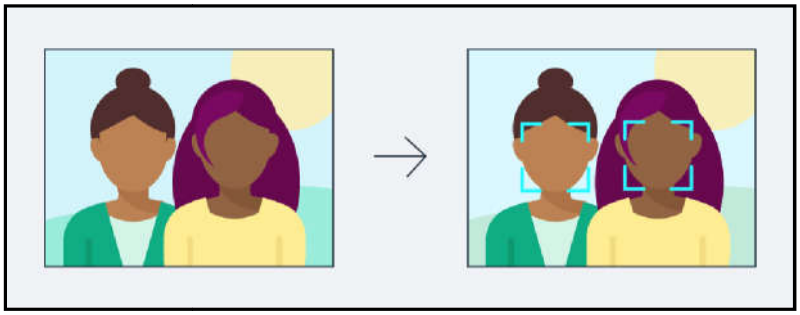

Figure 3: Detecting & Capturing facial images from travelers

Once detected and captured, many facial recognition systems will manipulate or process the facial image in a number of ways designed to render it a suitable facial probe for extraction of biometric information (extraction is described in the next sub-section). For example, a facial image captured at an angle might be realigned into normalized orientations, rendering all

[84] A good summary of recent face detection techniques is provide in: Rajeev Ranjan, Swami Sankaranarayanan, Ankan Bansal, Navaneeth Bodla, Jun-Cheng Chen, Vishal M Patel, Carlos D Castillo & Rama Chellappa, "Deep Learning for Understanding Faces", (2018) *IEEE Signal Processing Magazine* 66.

captured facial images 'front facing'.[85] The processed digital facial image becomes a facial probe, ready for input into facial recognition processes.

Biometric probes can be detected and captured from a variety of sources. Digital or physical photographs taken by an individual and sent to a border control agency can form one input. Some states, for example, require individuals to submit print or digital photographs in passport application or renewal processes, and will impose strict image specification restrictions. Before these can be automatically compared to a reference dataset for recognition purposes, the 'face' in these photographs must be detected and captured.[86] For example, a web-based passport photo checking service launched by the United Kingdom's Home Office deployed a face detection algorithm to ensure passport photos submitted through an online portal met image specifications.[87]

A facial recognition system might also record digital images directly from the traveller through a static camera. Canada, for example, has adopted Primary Inspection Kiosks that automate passport and customs control at border control checkpoints. The Kiosks obtain identity information encoded on a traveller's machine-readable biometric passport.[88] Travellers are then prompted to pose for a static digital photograph. Before this digital photograph can be submitted to automated facial recognition, the traveller's face must be detected and captured by a kiosk digital camera.

---

[85] European Union, FRONTEX, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", September 2015, https://doi.org/10.2819/86138, p 41:

> It is RECOMMENDED to provide pre-processed and quality-assessed images to the verification unit. Pre-processing SHOULD cover at least the following.
>
> - Detecting the face in a frame.
> - Cropping the face from the frame.
> - De-rotating the face to ensure that the centres of the eyes are nearly on a horizontal line.
>
> It is RECOMMENDED to perform a quality assessment on the images. The quality assessment SHOULD cover at least face- and eye-finding; it MAY contain a quality estimation based on criteria specified in ISO 19794-5. If a quality assessment is performed within the capture unit, the best image according to the applied criteria SHOULD be provided to the verification unit. This speeds up the whole process because template generation and verification on clearly inadequate images is avoided.

Rajeev Ranjan, Swami Sankaranarayanan, Ankan Bansal, Navaneeth Bodla, Jun-Cheng Chen, Vishal M Patel, Carlos D Castillo & Rama Chellappa, "Deep Learning for Understanding Faces", (2018) *IEEE Signal Processing Magazine* 66, p 68. Normalization processing might include realigning the image, shearing it, or manipulating it in similar ways so it most closely emulates a front-facing, centered image of a face.

[86] Since 2004, for example, Canada's 'Facial Recognition Project' (operated by Passport Canada, at the time) has recorded digital images of photographs submitted in passport applications, captured facial samples from the resulting digital images, and input these captured facial samples into a facial recognition system for the purpose of preventing passport application fraud: Office of the Privacy Commissioner of Canada, "Automated Facial Recognition In the Public and Private Sectors", March 2013, https://www.priv.gc.ca/media/1765/fr_201303_e.pdf, p 6. Canada has empowered its passport control agency to "convert an applicant's photograph into a biometric template for the purpose of verifying the applicant's identity, including nationality, and entitlement to obtain or remain in possession of a passport." At the same time, Canada was also empowered to "convert any information submitted by an applicant into a digital biometric format for the purpose of inserting that information into a passport" (Canadian Passport Order, SI/81-86, PC 1981-1472, section 8.1, adopted in Order Amending the Canadian Passport Order, SI/2004-113, September 1, 2004: http://www.gazette.gc.ca/rp-pr/p2/2004/2004-09-22/pdf/g2-13819.pdf).

[87] Adam Vaughan, "UK Launched Passport Photo Checker it Knew Would Fail with Dark Skin", October 9, 2019, *NewScientist*, https://www.newscientist.com/article/2219284-uk-launched-passport-photo-checker-it-knew-would-fail-with-dark-skin/.

[88] These Primary Inspection Kiosks are described in more detail in Section 2.1.1, below.

Facial images/probes can also be captured at a distance from live video footage of moving travellers. Some border crossings have now implemented systems that direct video cameras at lineups of travellers. These systems detect & capture each traveller's face, as they walk past.

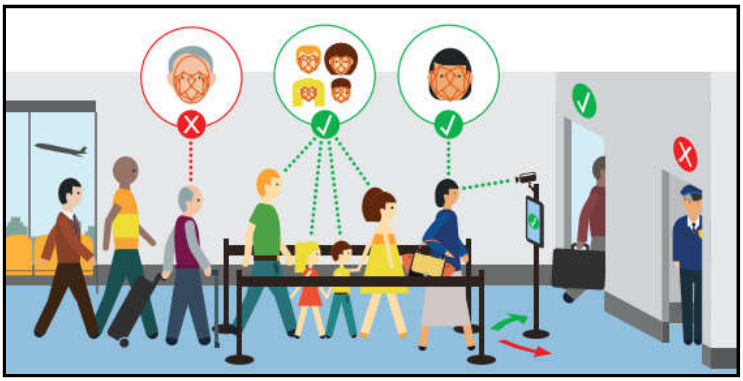

Figure 4: Gemalto Cogent Live Face Identification System
IMAGE SOURCE: Gemalto[89]

Capture in motion systems are faster and more efficient at processing travellers than fixed kiosk systems. United States border control agencies, for example, have indicated a preference for 'capture at a distance' facial recognition mechanisms on the basis that a 'stop and look' approach is not practical in light of the high volume of travellers that need to be processed.[90] However, there is a direct trade off between efficiency and accuracy, as 'capture at a distance' approaches will generate inferior facial images/probes.

United States border control agencies are also examining the use of facial recognition systems in Customs and Border Protection agent body worn cameras, posing similar obstacles for image quality.[91]

Image recording systems of this nature must be capable of identifying and isolating faces from live camera feeds at a rate that accommodates anticipated throughput.[92] These capture systems must also be able to account for a greater variation in images as they seek to isolate faces in motion and

[89] Gemalto, "Gemalto Exceeds Expectations at 2018 Biometric Technology Rally", https://www.gemalto.com/brochures-site/download-site/Documents/gov-cogent-biometric-technology-rally.pdf.

[90] United States, Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 11:

> Due to the large volume of travelers and border crossers, it would not be practical for CBP to use formally-generated frontal head-on facial images, such as are taken for a driver's license or passport. Rather, CBP is increasingly employing technologies that do not require subjects to present their face directly to the camera. Given this new focus, technology providers are continuing to refine their solutions to collect face images with minimal participation from the subject. While a more streamlined capture of facial images (rather than a "stop and look" approach) poses operational benefits to CBP, it also poses increased privacy risks since the individual may be unaware that their photo is being captured.

[91] United States, Customs and Border Protection, Request for Information: Body-Worn Cameras in Support of Incident-Driven Video Recording System, October 2019, https://assets.documentcloud.org/documents/6488270/CBP-BWC-and-FR-RFI-10-16-2019.pdf, p 19.

[92] Jacob A Hasselgren, John J Howard, Yevgeniy B Sirotin, Andrew J Blanchard & Arun S Vemury, "Operational Tradeoffs in the 2018 Department of Homeland Security Science and Technology Directorate Biometric Technology Rally", (2018) *IEEE International Symposium on Technologies for Homeland Security* 1, https://doi.org/10.1109/THS.2018.8574183, p 1: "At these volumes, even error rates that would typically be considered acceptable for a biometric system (one to three percent) could cause hundreds to thousands of non-identification exceptions, meaning high-throughput systems must be extremely accurate. ... a system designed to focus on fast transaction times may sacrifice image quality and thus matching capability."

from a wider variety of facial poses, illumination and expression, as well as with greater levels of facial occlusion or blurring in image capture than is the case in a static image recording scenario. All of these factors continue to render accurate facial recognition more difficult, even as greater accuracy is demanded by the higher anticipated individual traffic rate.[93]

Live video isolation of faces as sources of input for facial recognition systems has been proposed in even less controlled environments. The isolation process would be similar to that described above, but the individuals targeted for isolation will be moving more randomly through open spaces, such as duty free areas, the pre-check-in area, or even outside the passenger drop-off area outside an airport.[94] Detecting and capturing facial images in these open environments poses additional challenges for image quality.

Extracting a biometric description from the captured facial image/probe.

Once an individual's facial probe is detected, isolated and captured, the facial recognition system will extract a biometric or facial **template** from it. An algorithm that has already learned how to recognize faces will analyse the probe image, identify key features of the face and encode these as a collection of numbers or labels that, collectively, describe the face.[95]

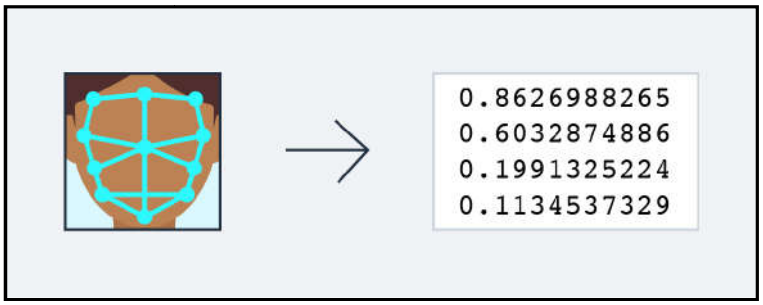

Figure 5: Extracting & encoding key facial features into a biometric template

The objective of this extraction process is not to create a universal numerical description of the traveller's face, but rather one that is repeatable and distinctive. The biometric description should therefore be one that is similar to others which would be extracted from the same traveller, while being different from those extracted from other travellers.

---

[93] Jacob A Hasselgren, John J Howard, Yevgeniy B Sirotin, Andrew J Blanchard & Arun S Vemury, "Operational Tradeoffs in the 2018 Department of Homeland Security Science and Technology Directorate Biometric Technology Rally", (2018) *IEEE International Symposium on Technologies for Homeland Security* 1, https://doi.org/10.1109/THS.2018.8574183, p 1: "At these volumes, even error rates that would typically be considered acceptable for a biometric system (one to three percent) could cause hundreds to thousands of non-identification exceptions, meaning high-throughput systems must be extremely accurate. ... a system designed to focus on fast transaction times may sacrifice image quality and thus matching capability."

[94] United States, Transportation Security Administration, "TSA Biometrics Roadmap: For Aviation Security & Passenger Experience", September 2018, https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf, Figure 4.

[95] For example, one facial recognition model encodes a facial image sample into 128 numbers measuring various features of the face. It may not always be clear what precisely is being measured by each of these numbers: Adam Geitgey, "Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning", July 24, 2016, *Medium*, https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78.

Once the biometric description is extracted from the captured facial image, that image and any underlying recordings from which it was captured are no longer necessary for the facial recognition process. Some facial recognition systems are designed to retain these images, while others will discard them once the template is extracted. Biometric facial templates are not universal – they are each unique to the facial recognition system that generated them, and they will not typically be recognizable by other facial recognition systems. Some commercial facial recognition systems will treat the process of generating and interpreting the specific facial template they use as a trade secret.[96]

Comparing the biometric representation to reference facial images.

As a final step, the captured facial template is compared to one or more stored facial reference images.

The immediate objective of this process is to determine the likelihood that the facial probe (recently captured from a traveller) and a given facial image reference (stored in the reference dataset) are both from the same individual.

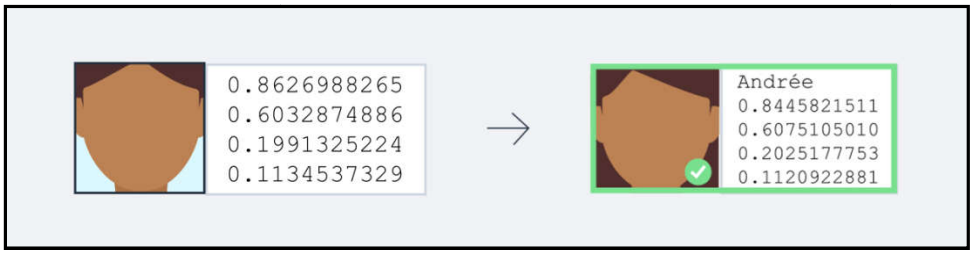

Figure 6: Facial Comparison determining a match

The immediate comparison process generates a **comparison score**, which estimates the similarity or dissimilarity between the traveller's template and each stored reference image with which it is compared.

At this stage, different facial recognition systems can produce different outputs. The simplest output of a comparison would be a **match**/**non-match** decision: a determination that the two samples being compared are or are not from the same individual. This determination will be based on whether the comparison score falls within a previously established '**confidence threshold**'.[97] Other systems will be configured to output a list of potential matches, either producing all potential reference images that meet the confidence threshold or providing the top X most similar reference images. Manual vetting is relied upon to decide which of the listed images, if any, is an actual match to the probe image.

[96] ICAO Doc 9303, "Machine Readable Travel Documents", Part 9, 7th Edition, 2015, https://www.icao.int/publications/documents/9303_p9_cons_en.pdf; National Institute of Standards and Technology, "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification", November 2018, *NISTIR 8238 pt 2*, https://doi.org/10.6028/NIST.IR.8238.

[97] Confidence thresholds are described in more detail in Section 1.3, below.

1.2.2 Type of Recognition Task: One-to-One/One-to-Many Comparison

The facial comparison process can operate in a 'one-to-one' or 'one-to-many' manner. These two modes of operation can differ substantially in terms of their capabilities, accuracy and other relevant factors. These two modes of comparison are described here, whereas additional examples of their comparative use in border control contexts can be found in Section 2.1 at p 65, below.

A **one-to-one** [1:1] comparison compares two facial images presumed to be from the same traveller and indicates whether they match or not. More specifically, 1:1 recognition compares a traveller's captured facial image to a single reference image previously associated with a travel document or identity profile. Most typically, 1:1 comparison is conducted for the purpose of **verifying** a travel document or other identity claim by confirming that the traveller and the source of a facial image associated with the claimed identity in the reference dataset are the same person. The immediate question 1:1 comparison typically seeks to answer is "Were both these facial images taken from the same person?"[98]

In a common example of 1:1 comparison, a traveller is photographed at an airport kiosk and the photograph is compared to the stored reference image on the contact-less chip on the traveller's passport (see description of contact-less chips at pp 6-11, above). If the comparison falls within the confidence threshold, the system indicates a 'match', and the passport is verified as belonging to the traveller.

The reference image can also be stored centrally instead of on a traveller's passport. Before centralized 1:1 comparison can occur, an identifier must be obtained from the traveller so that the reference image can be queried from the centralized dataset.

Figure 7: Querying centralized dataset in 1:1 comparison

[98] 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, p 4.

The centralized reference dataset is queried using this identifier and the image which was linked to it when the traveller was first enrolled is retrieved. In border control contexts, this identifier will most often be the traveller's passport number, which is encoded in machine-readable formats on most passports.[99] The facial recognition system will then compare the two images, verifying whether the passport belongs to the traveller or not.

By contrast a **one-to-many** [1:N] comparison compares a traveller's facial image to many reference images.

Figure 8: 1:N comparison seeking to identify an unknown traveller

A 1:N comparison can be exhaustive, comparing the traveller's facial image to all those in the reference dataset, while others are selective, and only compare the traveller's facial image to subsets of the reference dataset that are deemed most likely to yield a match.[100] While 1:N comparison can be used to verify an identity claim, it also has the capacity to **identify** unknown individuals, or **screen** individuals against pre-populated biometric lists.

A 1:N recognition system will sometimes be calibrated to provide a gallery of the most similar images in a reference dataset rather than simply providing the top match.[101] The size of the image gallery will often be calibrated based on the volume of anticipated queries, the scope of anticipated human intervention, and on the availability of time and resources for manual assessment, with larger image galleries requiring more intensive human resources per query.[102] In an investigative context, where

[99] For more details on the ways in which ICAO compliant passports to communicate details such as passport numbers to automated border control systems, see Section 1.1.1, above.

[100] 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, p 66: Some one-to-many search algorithms implement a 1:N search of a probe image as N 1:1 comparisons of the probe with the N enrolled items. This is followed by a sort operation which yields N candidates sorted in decreasing order of similarity. The result of that is returned in either of two ways: The system will return an operator-specified number of candidates, or it will return however many candidates are above an operator-specified threshold. In the case where a threshold is used, the number of candidates returned will be a random-variable that is dependent on the image data itself. Other algorithms do not implement 1:N search as N 1:1 comparisons. Instead they might employ a set of fast-search algorithms aimed at expediting search. These include various techniques to partition the enrollment data so that far fewer than N comparisons are actually executed. However, this does not mean that false positive occurrences will be reduced because the algorithms are still tasked with finding the most similar enrollments.

[101] See: 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, Figure 23.

[102] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft*

facial recognition might play one part of a broader, largely human-driven investigation into identity, an image gallery might be used.[103] By contrast, where automated border control gates are intended to rely on facial recognition to process the majority of travellers at high throughput and without human intervention, there is minimal latitude for human vetting of multiple images.[104]

Where few queries are anticipated to occur as part of a broader, human-driven investigation into identity, larger image galleries are often used.[105] Where the effectiveness of a facial recognition system is contingent on the majority of travellers being processed by automated means, image galleries may not be appropriate or feasible at all. Facial recognition is implemented in automated border control infrastructure, for example, to achieve more efficient processing of travellers.[106] Achieving these efficiency goals requires minimal human intervention for the majority of travellers, rendering a manual image gallery model impractical. In other border control contexts that are not time-dependent, such as in de-duplication (fraud) checks upon passport application or renewal, image galleries can be effective if the size of these galleries is calibrated to account for available human resources.[107] For example, Canada's Facial Recognition Project (initially piloted by Passport Canada in 2004 and now operated by IRCC), uses facial recognition to detect fraudulent duplication attempts in passport applications.[108] In its initial operation, a 1:N comparison mode generating a 10 image gallery was employed, with human operators relied upon to make the final determination as to whether any of the 10 images were a match to the passport applicant or not.[109]

Supplement, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Figure 9 outlines some considerations.

[103] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Figure 9.

[104] A description of various Automated Border Controls can be found in 2.2 at p 76, below.

[105] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Figure 9 provides the example of

[106] For a description of different Automated Border Control systems, see Section 2.2, below.

[107] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Figure 9 ("For example a passport office with 10000 applications per day, and reviewer labor sufficient to review 10 cases per hour might set threshold to target FPIR=0.024); Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification", NIST Interagency Report 8238, November 2018, https://doi.org/10.6028/NIST.IR.8238, p 4.

[108] Office of the Privacy Commissioner of Canada, "Automated Facial Recognition In the Public and Private Sectors", March 2013, https://www.priv.gc.ca/media/1765/fr_201303_e.pdf, p 6. See also: Immigration, Refugees and Citizenship Canada, Personal Information Bank PPU 081, Regular and Official Passports, *InfoSource: Personal Information Banks*, last modified June 26, 2019, https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/access-information-privacy/info-source/personal-information-banks.html#passports: "IRCC uses facial recognition technology to convert an applicant's photo into a biometric template and to compare it with information contained in the Passport facial recognition database."

Canada has empowered its passport control agency to "convert an applicant's photograph into a biometric template for the purpose of verifying the applicant's identity, including nationality, and entitlement to obtain or remain in possession of a passport." At the same time, Canada was also empowered to "convert any information submitted by an applicant into a digital biometric format for the purpose of inserting that information into a passport" (Canadian Passport Order, SI/81-86, PC 1981-1472, section 8.1, adopted in Order Amending the Canadian Passport Order, SI/2004-113, September 1, 2004: http://www.gazette.gc.ca/rp-pr/p2/2004/2004-09-22/pdf/g2-13819.pdf).

[109] Passport Canada, "Facial Recognition Application Project – Privacy Impact Assessment: Executive Summary", June 28, 2016, https://www.international.gc.ca/gac-amc/publications/atip-aiprp/assessments-evaluation/facial-faciale.aspx:

In 1:1 comparison, the reference biometric must be known in advance, meaning that the traveller must provide some form of identifier – either a name, a passport number, or some form of identity document. By contrast, 1:N comparison biometrically discovers the traveller's identity – all a traveller must do is present their face to a camera, no non-biometric data is required. This allows 1:N configurations to identify unknown travellers whereas 1:1 systems are limited to verifying traveller-presented identification numbers or biometric documents. In 1:N systems, travel documents can become secondary. For example, Australia is in the process of implementing a 'contactless' border control system, which relies on facial recognition as the primary means of identification – your face is your passport.[110] Additionally, 1:N comparison can be used to screen travellers by comparing their facial images to all those contained in a biometrically-enabled watch list.[111]

Most 1:N algorithms will need to systematically search the entirety of a given reference dataset in order to determine which, if any, of the images stored within it are a match. When a 1:N algorithm provides a result (a matching image or an indication that no matching images are present) after searching a reference dataset of 12 million individuals, that result is in essence the product of 12 million 1:1 comparisons.[112] This leads to higher error rates, as errors are compounded over the entire reference dataset.[113]

> In the proposed Passport Office application of FR technology, an operator in the Security Division would confirm a suggested computer match of the photographs using FR software. Confirmation by the operator requires a judgment call that the individual in the two photographs appear to be the same individual. … The correct match is proposed within the top 10 positions by the technology over 90% of the time. These figures apply for the images of the best quality. For images of a lower quality such as RCMP–provided photographs, the percent in the top then choices drops to 75%. For more complete results, please refer to the document prepared by the Passport Office.

[110] *Migration Amendment (Seamless Traveller) Regulations 2018*, https://www.legislation.gov.au/Details/F2018L01538, p 9: "This supports the digital transformation agenda by allowing reliance on electronic information already collected and removing the need to present a physical document, where possible. This is colloquially referred to as 'contactless processing' as little contact is made with clearance authorities other than presenting to a SmartGate for the purpose of having a facial image taken and compared with existing data."; *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text, Attachment B, p 2: "This is colloquially referred to as 'Contactless Processing' as little contact is made with clearance authorities other than presenting to a SmartGate for the purpose of having a facial image taken and compared with existing data."

[111] For example, the UK is piloting the use of facial recognition to screen travellers at borders against biometrically-enabled criminal watch lists: United Kingdom, Home Office, "Biometrics Strategy: Better Public Services Maintaining Public Trust", June 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf, para 35.

[112] Some 1:N comparison systems will use heuristics and other shortcuts to identify image features that need not be searched when attempting to identify a given image probe: 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, p 66:

> Some one-to-many search algorithms implement a 1:N search of a probe image as N 1:1 comparisons of the probe with the N enrolled items. This is followed by a sort operation which yields N candidates sorted in decreasing order of similarity. The result of that is returned in either of two ways: The system will return an operator-specified number of candidates, or it will return however many candidates are above an operator specified threshold. In the case where a threshold is used, the number of candidates returned will be a random-variable that is dependent on the image data itself.
>
> Other algorithms do not implement 1:N search as N 1:1 comparisons. Instead they might employ a set of fastsearch algorithms aimed at expediting search. These include various techniques to partition the enrollment data so that far fewer than N comparisons are actually executed. However, this does not mean that false positive occurrences will be reduced because the algorithms are still tasked with finding the most similar enrollments.

[113] See discussion at Section 1.3.1 at p 36, below. See also: Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Tables 9 – 17; Stephen Gee, Assistant Secretary, Department of Foreign Affairs and Trade, Australia, "Biometric Systems: Can They Be Cheap and Simple?", (2018) 13(1)

The lower accuracy of 1:N matching algorithms can be mitigated to some degree by decreasing the size of the reference dataset. United States border control officials operate a 1:N Traveler Verification Service (TVS), for example, that compiles a biometrically-enabled manifest of travellers scheduled for pending outbound international flights based on US advanced passenger flight information (APIS).[114] By reducing the reference dataset to travellers on a given flight rather than all travellers, the effectiveness of the system is increased. The Australian facial border control system, by contrast, compares travellers' faces against a reference dataset comprising all Australian passport holders as well as any non-Australians who have enrolled in the system.[115] The European Union concluded in 2015 that 1:N facial recognition lacks sufficient accuracy for fully automated border control purposes, and instead indicated a preference for 1:1 verification.[116] The United States National Institute of Standards and Technology (NIST) similarly concluded in 2019 that "Low FPIR is not attainable" without the use of active human intervention when 1:N recognition algorithms are applied to large datasets.[117]

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.

ICAO TRIP Magazine 12, cross-posted to: *Uniting Aviation*, January 9, 2019, https://www.unitingaviation.com/strategic-objective/security-facilitation/cheap-and-simple-biometric-systems/.

[114] Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf, pp 5-6.

[115] *Migration Amendment (Visa Revalidation and Other Measures) Bill 2016, Schedule 3 – Immigration Clearance,* https://www.legislation.gov.au/Details/C2016B00172; "The Australian Passport Office database which holds images collected as part of the Australian passport identity verification process. The Department has arrangements in place for access to this database which is currently used for border clearance. Access to images of Australian citizens supports Contactless Automated Immigration Clearance."

[116] eu-LISA, "Smart Borders Pilot Project: Report on the Technical Conclusions of the Pilot", Volume 1, (2015), pp 162-163:

> While the tests proved that the verifying (1:1) a traveller's identity using the facial-image biometric modality – based on a facial image captured live and checking it against the picture on the traveller's eMRTD chip – is feasible, the facial image is considered to be insufficient as sole identifier for identification purposes within a large scale database (1:n).

Note that 1:N identification witnessed substantial improvement between 2013-2018. However, the best 1:N identification systems continue to exhibit false negative rates of about 4% at false positive rates of 0.1% with good quality photos in their top ranked match, human intervention through the use of image galleries is required to achieve higher accuracy rates. See Figure 2 and discussion at Section 1.3.1, pp 34-36, below.

[117] 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, p 63: "Low FPIR is not attainable: The error tradeoff characteristics show a rapid increase FNIR as the threshold is increased to reduce FPIR. For example, in FNIR Figure 24, FNIR reaches 50% when FPIR is reduced to 0.0001."

1.3 Gauging True Effectiveness, Racial Bias & Accuracy

Assessing the impact of a facial recognition system requires a robust assessment of its accuracy, as facial recognition systems remain inherently fallible and the rate at which they erroneously identify or fail to identify individuals will determine their detrimental impact on travellers as well as their effectiveness in achieving their objectives.

Too often, assessment of facial recognition system accuracy fails to take into account racial bias, allowing population-wide error rates to obscure the far more significant impact on marginalized groups, who frequently experience the impact of these biases most directly. This deficiency occurs despite well documented racial biases across most facial recognition algorithms.

Assessment of facial recognition systems must occur prior to their adoption, and must take into account the settings in which they will be implemented, including the anticipated volume of travellers that will be processed and quality of the images that will be compared. These factors will impact the overall accuracy of an algorithm as well as its specific propensity for racial bias and are critical considerations when deciding whether to adopt facial recognition in a border context. If implemented, assessment of the facial recognition system must continue to occur on an ongoing basis, so that the real-world impact of the system can be monitored.

1.3.1 False Negative / Positive Match Rates & Confidence Thresholds

Border control facial recognition systems will typically rely on pre-trained commercial facial recognition algorithms. These algorithms must be carefully tested for accuracy, taking into account the context in which they will ultimately be applied. Prior to implementation, a facial recognition algorithms' accuracy can be assessed on a theoretical basis, through the use of a testing dataset, or on a predictive basis, by creating physical testing installations that simulate anticipated real-world implementation environments.

Algorithmic accuracy is measured in rates of false acceptance and false rejection. For any given facial recognition algorithm, there is a trade-off between false acceptance and rejection. This trade-off is navigated by a facial recognition system's confidence threshold. The overall rating of a facial recognition algorithm's accuracy is typically measured by its ability to accurately recognize faces with equal levels of false positives and negatives.[118]

[118] D.O. Gorodnichy, S.N. Yanushkevich & V.P. Shmerko, "Automated Border Control: Problem Formalization", *CBSA Science & Engineering Directorate*, Division Report 2014-41, September 2014, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc203/p801324_A1b.pdf,

False acceptance, measured as the **False Positive Identification Rate** ("**FPIR**"), or the **False Match Rate** ("**FMR**"), occurs where a positive facial recognition claim that should have been rejected is accepted (false positive).[119] That is, a facial recognition system inaccurately claims that an individual matches a facial sample enrolled in its reference dataset. False rejection, often measured as the **False Non-Match Rate** ("**FNMR**"), or the **False Negative Identification Rate** ("**FNIR**"), occurs where a negative facial recognition claim should have been accepted (false negative).[120] That is, a facial recognition system fails to recognize that an individual is the source of a sample in its reference dataset.

Confidence thresholds are a critical component in navigating the trade-offs between false positives and false negatives. Confidence thresholds are configurable benchmark scores that determine what level of estimated similarity must be achieved before recognition will occur. Any comparison that results in a score that falls below the benchmark is treated as a non-match.

All other factors being equal, a low confidence threshold allows a facial recognition system to recognize a higher proportion of travellers, but more of those travellers will be inaccurately recognized (more false positives leading to a higher FMR). By contrast a high confidence threshold will fail to recognize some travelers, but is less likely to incorrectly recognize the wrong traveler (more false negatives leading to a higher FNMR). Thresholds are typically set in a manner that will achieve an acceptable level of false positives, with a high threshold correlating to low FMR.

Threshold (FPIR)	Total tested travellers	Enrolled & tested travellers	Total recognized	Unrecognized enrolled & tested	Incorrectly recognized
High (.001)	100	85	83	2	0
Low (.1)	100	85	94	1	10

Table 1: Confidence Thresholds in Hypothetical Operation

In this purely illustrative example, a facial recognition system is calibrated with a high confidence threshold, so that only 1 in one thousand travellers will be falsely recognized (FPIR=0.1%). Of 100 travellers, 15 were not enrolled and none of these were identified by the facial recognition system,

[119] False Match Rate or FMR is defined as the rate at which a facial recognition algorithm falsely indicates that two biometric samples are from the same individual when it is known they are not. See: ISO/IEC, Information Technology – Vocabulary – Part37: Biometrics, ISO/IEC 2382-37:2017(E), 3.9.8 and 3.9.9. When assessing 1:N algorithms, 'False Positive Identification Rate' (FPIR) is used as a metric instead of 'False Match Rate'. Whereas FMR reflects the rate at which an algorithm erroneously matches two images that are not taken from the same individual, FPIR reflects the rate at which an algorithm incorrectly indicates that a reference image is a 'match' after comparing a probe image to those in a reference dataset.

[120] False Non-Match Rate or FNMR is defined as the rate at which a facial recognition algorithm falsely indicates that two biometric samples are NOT from the same individual when it is known they ARE. See: ISO/IEC, Information Technology – Vocabulary – Part37: Biometrics, ISO/IEC 2382-37:2017(E), 3.9.10 and 3.9.11. When assessing 1:N algorithms, 'False Negative Identification Rate' (FNIR) is used as a metric instead of 'False Non-Match Rate'. Whereas FNMR reflects the rate at which an algorithm fails to match two images that are taken from the same individual, FNIR reflects the rate at which an algorithm fails to identify a reference image known as a 'match' after comparing a probe image to those in a reference dataset.

FNMR excludes situations where a biometric system fails to acquire a facial image from a traveller and no attempt to compare facial images occurs (see section 1.3.6, below). The False Rejection Rate (FRR) is more inclusive measure of rejection, in that it includes images that the facial recognition system failed to acquire due to capture or other related issues.

while 2 were enrolled but were incorrectly missed by the facial recognition system (an FNIR of 1.7%). In total, 83 travellers were automatically processed. By contrast, employing a low confidence threshold (FPIR=10%), 94 of the same travellers were automatically processed by the facial recognition system. Of these, 8 travellers were un-enrolled and mistakenly matched to enrolled profiles, an additional 2 enrolled travellers were mistakenly matched to incorrect enrolled profiles, and the system failed to recognize 1 traveller who was properly enrolled (an FNIR of 1.1%).[121]

In border control contexts, confidence thresholds are often driven by the need to achieve acceptably low false positive levels (FMR), as the security consequences of erroneously admitting a traveller are prioritized over the impact on travellers who must submit to manual processing due to higher false negatives (FNMR). Achieving an acceptably low FMR can entail substantial tradeoffs.

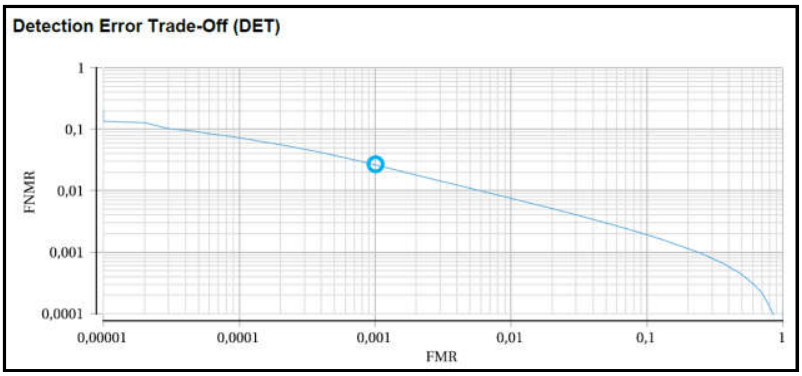

Figure 9: 2018 FNMR/FMR Trade-offs for Cognitec's 1:1 FaceVACS, used by e-Gates in German airports
IMAGE SOURCE: Nuppeney, "Automated Border Control (EasyPASS)", 2018[122]

The magnitude of this trade-off between FMR and FNMR will vary by facial recognition algorithm.[123]

Confidence thresholds can be adjusted to account for the needs of various border control implementations. An algorithm's theoretical FNMR can be tested at varying FMR thresholds,[124] and both are assessed, as each has distinct implications for the overall accuracy and impact of a system.[125]

---

[121] This reflects the theoretical capabilities of the second best performing algorithm in NIST's ongoing assessment of 1:N facial recognition algorithms: Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Table 23, Algorithm 127 (FNIR for a rank 1 result is .0017 @ threshold established to generate FPIR of .001, and FNIR is .011 at a threshold established to generate FPIR of 0.1). The algorithm was tested to reflect 1:N matching capabilities with a reference dataset of 1.6 million high quality mugshot images, using low quality webcam facial images as probes.

[122] Markus Nuppeney, "Automated Border Control (EasyPASS): Monitoring the System Performance", *NIST: IFPC 2018*, November 27, 2018, https://nigos.nist.gov/ifpc2018/presentations/05_nuppeney_20181127_IFPC2018_EasyPASS_Nuppeney.pdf.

[123] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Figure 1.

[124] The False Match Rate (FMR) of an algorithm can be tested by establishing a confidence threshold necessary to achieve a pre-determined False Non-Match Rate (FNMR). The FNMR of an algorithm can be similarly tested by establishing a confidence threshold it requires to achieve a pre-determined FMR. For an example of how this testing is conducted in a comparative context, see Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, Tables 6-10, which tests FNMR for a number of algorithms when each operates at a threshold necessary to achieve a pre-determined FMR for a given reference dataset.

[125] United States, Government Accountability Office, "Face Recognition Technology", *Testimony Before House of Representatives, Committee on Oversight and Reform*, GAO-19-579T, June 4, 2019, https://www.gao.gov/assets/700/699489.pdf, p 15:

Assessing false positives & negatives in 1:N Comparison

Assessment of 1:N comparison algorithms will, at times, include additional accuracy metrics to account for more rigorous levels of human intervention. Specifically, where a 1:N recognition algorithm will be used as an investigative tool rather than as an identification tool, less stringent accuracy is sometimes employed.

Where a 1:N facial recognition system is configured to return multiple matches for human evaluation,[126] FNIR is sometimes assessed based on whether an algorithm succeeded in identifying a traveller in its top 50 ranked matches rather than in its top ranked match alone.[127] For example, the FBI indicates that one of its facial recognition systems is able to correctly identify candidates in its database 86% of the time within its top 50 responses.[128] In these scenarios, no confidence threshold is established at all. FNIR is dramatically improved, while the algorithm will effectively output at least 49 false positives for each query. The operating presumption is that a human being will need to investigate each or many of the 50 images before ultimate identification occurs.[129]

It is insufficient to assess a 1:N algorithm solely on its propensity for false negatives in its top 50 matches. When choosing whether to procure a facial recognition system, algorithms should be selected on their capacity to identify individuals with the least possible number of matches in

---

> In comments on our May 2016 report, DOJ officials also stated that searches of NGI-IPS produce a gallery of likely candidates to be used as investigative leads, not for positive identification. As a result, according to DOJ officials, NGI-IPS cannot produce false positives and there is no false positive rate for the system. We disagree with DOJ. According to the National Institute of Standards and Technology, the detection rate and the false positive rate are both necessary to assess the accuracy of a face recognition system. Generally, face recognition systems can be configured to allow for a greater or lesser number of matches. A greater number of matches would generally increase the detection rate, but would also increase the false positive rate. Similarly, a lesser number of matches would decrease the false positive rate, but would also decrease the detection rate. Reporting a detection rate of 86 percent without reporting the accompanying false positive rate presents an incomplete view of the system's accuracy.

See also: 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, p 6:

> We report false positive and false negative rates separately because the consequences of each type of error are of importance to different communities. For example, in a one-to-one access control, false negatives inconvenience legitimate users; false positives undermine a system owner's security goals. On the other hand, in a one-to-many deportee detection application, a false negative would present a security problem, and a false positive would flag legitimate visitors. The prior probability of imposters in each case is important. For example, in some access control cases, imposters almost never attempt access and the only germane error rate is the false negative rate.

[126] See Section 1.2.2, p 26, above for a more detailed description.

[127] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification", *NIST Interagency Report 8238*, November 2018, https://doi.org/10.6028/NIST.IR.8238, p 4. Note that with respect to 1:N comparison, FNIR is used to indicate false negative rates in lieu of FNMR whereas FPIR is used to indicate false positive rates in lieu of FMR. FNIR/FPIR focus on the ultimate output of a 1:N facial recognition algorithm rather than on its capacity to carry out individual matches carried out throughout a large reference dataset. That is, if a reference image gallery comprises 6 million images and an algorithm operating with a FMR of 0.000001% and attempts to match a traveller's facial probe image against each of the 6 million images, the output of this comparison process will yield a false positive outcome 60% of the time (6 million 1:1 comparisons at a False-Match Rate of 0.000001% = 60% False Positive Identification Rate). See: 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, p 66.

[128] United States, Government Accountability Office, "Face Recognition Technology", *Testimony Before House of Representatives, Committee on Oversight and Reform*, GAO-19-579T, June 4, 2019, https://www.gao.gov/assets/700/699489.pdf, p 14.

[129] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

order to minimize privacy impact and make more efficient use of resources.[130] It is therefore critical to assess FNIR deterioration as image galleries are progressively reduced in size when selecting and implementing an algorithm.[131] Selectivity—an algorithm's capacity for ranking the correct image higher within the top 50 matches—should also be considered when assessing the accuracy and impact of a 1:N comparison algorithm.[132] Once in operation, accuracy should be assessed on an ongoing basis to determine whether smaller image galleries can be employed so as to minimize privacy impact and efficiency.[133]

Moreover, it is critical to continue to assess the real-world impact of this algorithm. Specifically, when 1:N identification is used in an 'image gallery' configuration, it is important to document and assess false positives at the human investigator level: How frequently did human investigators identify the *wrong* individual from the gallery of 50 provided images. Photo lineups have played a problematic role in some investigative contexts, where it can cause investigators to 'fixate' on a suspect on the presumption that this individual is present in the gallery, particularly if they are already familiar with one of the individuals in the 50 image gallery. For these and related reasons, courts have acknowledged that the evidentiary value of photo lineups as identification tools is minimal at best, and unless strict safeguards are in place, can be prejudicial.[134] Policing agencies in the United States have also been criticized for relying solely on photo lineup image galleries generated by facial recognition systems as a means of identifying individuals for more intensive scrutiny and even arrest without seeking additional corroboration.[135]

As a result, in the border control context, use of large image galleries is not possible where practical or operational constraints require minimal human intervention.

---

[130] United States, Government Accountability Office, "Face Recognition Technology", *Testimony Before House of Representatives, Committee on Oversight and Reform*, GAO-19-579T, June 4, 2019, https://www.gao.gov/assets/700/699489.pdf, pp 14-15:

> If false positives are returned at a higher than acceptable rate, law enforcement users may waste time and resources pursuing unnecessary investigative leads. In addition, we concluded that by conducting this assessment the FBI would help ensure that it is sufficiently protecting the privacy and civil liberties of U.S. citizens enrolled in the database. Therefore, we recommended that the FBI conduct tests of NGI-IPS to verify that the system is sufficiently accurate for all allowable candidate list sizes and ensure that both the detection rate and the false positive rate are identified for such tests. … According to the National Institute of Standards and Technology, the detection rate and the false positive rate are both necessary to assess the accuracy of a face recognition system. Generally, face recognition systems can be configured to allow for a greater or lesser number of matches. A greater number of matches would generally increase the detection rate, but would also increase the false positive rate. Similarly, a lesser number of matches would decrease the false positive rate, but would also decrease the detection rate. Reporting a detection rate of 86 percent without reporting the accompanying false positive rate presents an incomplete view of the system's accuracy."

[131] 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, p 61 and Figures 18-21.

[132] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, pp 18 and 30.

[133] United States, Government Accountability Office, "Face Recognition Technology", *Testimony Before House of Representatives, Committee on Oversight and Reform*, GAO-19-579T, June 4, 2019, https://www.gao.gov/assets/700/699489.pdf, pp 14-15.

[134] *R v Hibbert*, 2002 SCC 39, paras 51-12; *R v* Phillips, 2018 ONCA 651, paras 44-48; R *v Faleh*, 2019 ABCA 441, paras 32-33 (trial judge was alive to the frailties of … eyewitness and photo lineup evidence); *R v Brown*, 2007 ONCA 71, paras 11-12 and 17; *R v Le (TD)*, 2011 MBCA 83, para 140; *R v Jones*, [2004] 193 OAC 56, para 11.

[135] Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data", *Georgetown Law: Center on Privacy & Technology*, May 16, 2019, https://www.flawedfacedata.com/; 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.

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.[1]

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.[2]

[1] 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.

[2] 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/.

Accounting for Size of Reference Dataset

The accuracy of a search is impacted by the number of reference images involved in the comparison.

One-to-one comparison is categorically more accurate than 1:N comparison, as the former need only compare two images presumed to be from the same person whereas the latter must search a large reference dataset to identify a match or the absence thereof. Table 2 compares accuracy rates for the leading 1:1 and 1:N algorithms in NIST's ongoing facial recognition testing.

Mode of comparison	Total tested travellers	Enrolled & tested travellers	Total recognized	Unrecognized enrolled & tested	Incorrectly recognized
1:1[136]	10,000	9,950	9,885	42	0
1:N[137]	10,000	9,950	9,499	451	10

Table 2: Accuracy Differences in 1:1 vs 1:N Comparison

Particularly where a large reference dataset (12 million images) is used, the 1:N algorithm is substantially inferior in terms of false positives and false negatives.

One-to-many algorithm performance substantially deteriorates as the size of a reference dataset increases.[138] Figure 10 shows false match rates for five of the top algorithms in NIST's ongoing 1:N facial recognition testing, presenting comparative FNIR for reference datasets of increasing size.

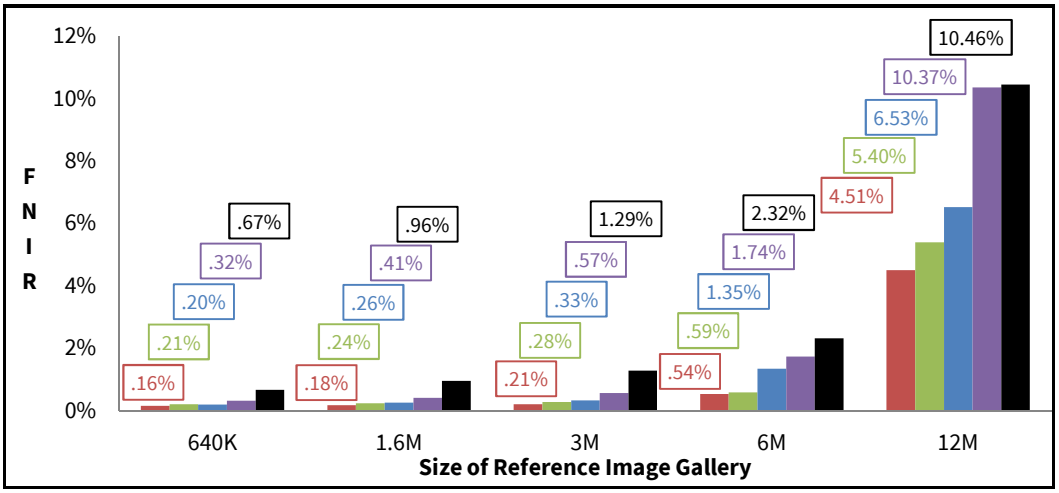

Figure 10: Impact of Reference Gallery Size on 1:N Comparison Accuracy at High Threshold (FPIR=0.1%)[139]

The leading vendor registers a 28 fold increase in false negatives when applied to a reference dataset comprising 12 million images as opposed to one comprising 640 thousand images.

Border control contexts will often require the ability to recognize large volumes of travellers. In 2017-2018, for example, Immigration, Refugees and Citizenship Canada issued 4.97 million travel

[136] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, Table 8, Algorithm 130, achieving a 0.42% FNMR when using a confidence threshold calibrated to achieve 0.0001% FMR in comparisons between Visa images and images taken at borders (ie at kiosks).

[137] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Table 10, Algorithm 117, achieving a 4.51% FNIR in its top ranking result when using a confidence threshold calibrated to achieve 0.1% FMR using a reference dataset comprised of 12 million images.

[138] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Figures 37-48.

[139] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf. Data reflects FNMR for 5 of the top performing (numbers 76, 77, 96, 117 and 148) in Tables 9-11, using a high threshold (FPIR = 0.1%).

documents in 2017-18, and reports 23.79 million travel documents in circulation.[140] Toronto Pearson International Airport reported 20 million international travellers in 2019.[141] Over 33 million air travellers entered Canada from abroad in 2019, an average of about 92,000 per day.[142] Facial recognition systems using 1:N comparison in order to detect passport fraud (de-duplication) or to process international travellers will need to contend with reference datasets of larger magnitudes than the 12 million image dataset tested above.[143]

1.3.2 Racial, gender & demographic bias remain deeply problematic

Racial bias remains a pervasively frequent feature of facial recognition, and as a result many of the detrimental consequences of the adoption of such systems fall on marginalized groups.

The overall accuracy rates of facial recognition systems frequently obscures the disproportionate impact these systems will have on often marginalized demographic groups due to persistent racial and gender biases. As such variations remain common, false positive and negative rates will be different for members of some demographic groups and for women.[144] As a result, a true measure of the anticipated utility as well as detrimental social impact of a border control facial recognition system will not turn on its overall accuracy alone, but will be contingent on its racial bias as well.

Several studies have shown that facial analytic algorithms in general exhibit racial bias.[145] For

---

[140] Immigration, Refugees and Citizenship Canada, "Passport Program: Annual Report for 2017 to 2018)", (2019), https://www.canada.ca/content/dam/ircc/migration/ircc/english/resources/publications/passport-ar/documents/pdf/ar_18_eng.pdf.

[141] Toronto Pearson International Airport, "Traffic Summary", April 2020, https://tpprodcdnep.azureedge.net/-/media/project/pearson/content/corporate/partnering/pdfs/traffic-summary-april-2020.pdf.

[142] Statistics Canada, "International Travellers Entering or Returning to Canada", Table 24-10-0005-01 (formerly CANSIM 427-0005), https://doi.org/10.25318/2410000501-eng, (Summing results for January – December, 2019, for "United States Residents Entering by Plane", "Travellers from Countries Other than United States Entering by Plane", "Canadian Travellers Returning from the United States by Plane" and "Canadian Travellers Returning from Countries other than United States by Plane". The annual total is 33,874,557.

[143] Note that Immigration, Refugee and Citizenship Canada uses a 1:N recognition algorithm with a 10 image gallery when assessing passport applications to avoid fraud and duplication. IRCC anticipates he algorithm to provide the correct match in the 10 image gallery 90% of the time if higher quality images are used and 75% of the time if relying on lower quality images: Passport Canada, "Facial Recognition Application Project – Privacy Impact Assessment: Executive Summary", June 28, 2016, https://www.international.gc.ca/gac-amc/publications/atip-aiprp/assessments-evaluation/facial-faciale.aspx.

To date, facial recognition used by airports and the Canada Border Services Agency to process international travellers at airports uses 1:1 recognition. See Section 2.1.1, below, for more details.

[144] 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, p 40 (with respect to false positives in 1:1 matching algorithms:

> The East African FMR values are often two orders of magnitude higher than the nominal value and those recorded within Eastern Europe. That is, the log10 FMR values are +2 higher corresponding to FMR that is of order 100 times larger than the de-facto baseline. From a security perspective this is analogous to using a two-digit PIN instead of the common four digits. For West Africa, the FMR values are between one and two orders of magnitude above baseline. A shift of 1.4 on the logarithmic scale corresponds to a factor of 25 increase, for example. …
>
> In the scatter plot for African women Figure 9 there is a cluster of algorithms located near $x = 0{:}00012$ and $y = 0{:}003$. Compared to the target FMR value of 0:00003 (the vertical line) there is a near four-fold increase in FMR of women over men. Much more significantly there is a more than 100-fold vertical excursion from white men to African women.

[145] Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", (2018) 81 *Proceedings of Machine Learning Research* 1, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Joy Buolamwini, Testimony before United States House Committee on Oversight and Government Reform, May 22, 2019, *In Re Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*; Cynthia M Cook, John J Howard, Yevgeniy B Sirotin, Jerry L Tipton & Arun S Vemury, "Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems", (2019) 1(1) *IEEE T-BIOM* 32, https://ieeexplore.ieee.org/document/8636231.

example, one survey of automated face-based gender classifiers found that error rates can be over 34% higher for dark skinned female faces than for light male faces.[146] Country of origin is also a documented basis on which algorithmic accuracy will vary, to the extent that country of origin represents phenotype variations.[147]

These early studies prompted the United States Department of Commerce's National Institute for Standards and Technology (NIST) to test numerous recognition algorithms in an attempt to assess racial and demographic bias, and its findings were released in a 2019 study. The study uses a number of image galleries including mugshots, Visa application photos, and images intended to emulate photos taken at border crossings (such as through kiosks). NIST applied gender, racial and country of origin labels to these images. Note that researchers have criticized the use of gender, race and country of origin labels as a means of assessing bias in facial analytic algorithms.[148] In particular, the use of binary gender labels is problematic as it does not account for transgender identities while race-based labels do not reflect the diversity of phenotypic features that might impact facial recognition accuracy.[149]

Most facial recognition algorithms will exhibit some bias with respect to particular demographics, and the degree of this bias will change from algorithm to algorithm. Bias does not always correlate with the overall accuracy of an algorithm, meaning that algorithms will have greater or lesser degrees of racial bias and algorithms that are more accurate overall may not necessarily produce lower degrees of bias.[150] Configuration of facial recognition algorithms can also lead to trade-offs between general accuracy and racial bias. This suggests that border control agency procurement and configuration decisions implicitly include a choice between minimizing general traveller impact and minimizing impact on travellers from specific demographic communities.

Generally speaking, identification algorithms (1:N) tend to produce higher false positives and negatives for Black women. Black women are also less likely to be in the top results following 1:N identification comparison, indicating higher false negative rates (FNIR).[151] False positive rates in

[146] Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", (2018) 81 *Proceedings of Machine Learning Research* 1, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, p 8.

[147] National Institute of Standards and Technology, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", April 4, 2019, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing; Patrick Grother, "Bias in Face Recognition: What Does That Even Mean? And Is It Serious?", *Biometrics Congress*, November 2, 2017, https://www.nist.gov/sites/default/files/documents/2017/11/20/grother_11_02_bias.pdf.

[148] Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", (2018) 81 *Proceedings of Machine Learning Research* 1, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, pp 3-4 and 6.

[149] Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", (2018) 81 *Proceedings of Machine Learning Research* 1, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, pp 3-4 and 6.

[150] Although general improvements in overall accuracy are generally correlated to improvements in accuracy for some demographic groups: Cynthia M Cook, John J Howard, Yevgeniy B Sirotin, Jerry L Tipton & Arun S Vemury, "Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems", (2019) 1(1) *IEEE T-BIOM* 32, https://ieeexplore.ieee.org/document/8636231.

[151] 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, p 63: "searches of white women are more likely to produce the correct result in the top ranks than

1:N identification comparisons are also higher for Black women, with FPIR frequently an order of magnitude higher than for white men.[152] A small number of 1:N algorithms operated with relatively minimal racial disparities in false positive rates when tested with high quality mugshot images.[153] However, these algorithms were not tested with border control quality images, which are lower quality and produce far greater racial disparities.[154]

Verification algorithms tend to exhibit higher false positive rates (FMR) within specific demographic groups than when assessed generally, because comparisons are being made between individuals who exhibit similar facial features to those within the examined population.[155] These higher false positive rates are substantially more pronounced for some marginalized groups, as demonstrated by NIST's demographic study.[156] Specifically, comparisons between individuals from within each of 5 regions (Central America, Africa, the Caribbean, South Asia and East Asia) exhibit higher false positive rates than comparisons between individuals from Eastern European countries.[157] Especially when using lower quality border control images, such as those taken by automated kiosks or e-gates, false positives and negatives will generally be higher for individuals from African and Caribbean countries, with false positive rates frequently one or two orders of magnitude higher than baseline rates.[158] Finally, women tend to generate higher FMR and FNMR across most algorithms and most countries of origin.[159]

---

are search of men. This is less true for [B]lack women. A possible mechanism for this is available from section 4 verification results, namely that [B]lack women tend to produce high one-to-one false match rates. High non-mate scores may be displacing the correct [B]lack women from rank 1 position."

[152] 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, p 63.

[153] 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, p 68, figure 27.

[154] 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, p 54:

> In domestic mugshots, the lowest FNMR in images of subjects whose race is listed as [B]lack. However, when comparing high-quality appliction photos with border-crossing images, FNMR is often highest in African born subjects. We don't formally measure contrast or brightness in order to determine why this occurs, but inspection of the border quality images shows underexposure of dark skinned individuals often due to bright background lighting in the border crossing environment. In mugshots this does not occur. In neither case is the camera at fault.

The greater racial disparities resulting from use of passport and border control images, which are categorically lower in quality than mugshot images, is evident in 1:1 comparison and is likely to be multiplied by the use of 1:N comparison: *Ibid*, p 63: "[B]lack women tend to produce high one-to-one false match rates. High non-mate scores may be displacing the correct [B]lack women from rank 1 position." and p 47: "As with application photos, most algorithms give systematically higher false match rates in women than in men. The magnitude of this difference is lower with mugshots than with application photos."

[155] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, Figure 116: "For the visa images, the false match calibration curves show FMR vs. threshold, T. The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate T. As shown later (sec. 3.6), FMR is higher for demographic-matched impostors."

[156] 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, Figure 13.

[157] 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, p 28, Figures 5-6 and Annex 7, Figures 275-276.

[158] 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, p 54, p 40 and Figure 13 and p 3:

> However, with lower-quality border crossing images, false negatives are generally higher in people born in Africa and the Caribbean, the effect being stronger in older individuals. These differing results relate to image quality: The mugshots were collected with a photographic setup specifically standardized to produce high-quality images across races; the border crossing images deviate from face image quality standards."

[159] 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, pp 47 and 56.

Even the best performing 1:1 verification algorithms in NIST's demographic analysis are problematic. For example, one top rated algorithm is configured to produce low false positives for images labelled 'White men'.[160] Operating at that threshold, it will falsely recognize high quality images labelled as 'Black women' almost 20 times more frequently.[161] The same algorithm will falsely recognize images labelled 'American Indian men' 50 times more often and 120 times more frequently for images labelled 'American Indian women'.[162] Operating at the same confidence threshold, the same algorithm will fail to recognize images labelled 'American Indian' close to 1.5 times more frequently than it will miss images labelled 'White men'.[163] Using lower quality images aimed at emulating the border control context, this algorithm will fail to match individuals from African and Caribbean countries 1.3 times more frequently than individuals from Eastern European countries.[164] Most algorithms tested by NIST perform worse, and older algorithms historically procured by border control agencies can be expected to perform substantially worse.

As noted above, some of these demographic variations might result from a lack of diversity in training datasets. However, some studies suggest that racial and gender variance cannot be fully addressed through more diverse or better labelled training datasets alone. For example, some studies suggest that the more common usage of cosmetics amongst women creates an inherently greater degree of variation that is gender specific and cannot be fully mitigated simply by using a more diverse training dataset.[165] Similarly, some studies have indicated that the use of more

[160] FMR=0.001%, for images labeled 'white men'. 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, Annex 12, Figure 118 (showing comparative FMR and FNMR for various demographic groups when a threshold is set to achieve FMR=0.001% for images NIST labels white male conducting 1:1 comparisons using high quality mugshot images).

The algorithm, visionlabs_007, was chosen because it is the top performing algorithm in terms of sex, country of birth and age group when comparing visa application images to border control images and is generally referred to as an algorithm with relatively low discriminatory differential (see 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, Figures 18 and 22, and p 58) and because it is the top performing 1:1 algorithm in NIST's *general* comparison of border control and visa application images that is also included in its demographics study (Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, Table 10, algorithm 197).

[161] The algorithm yields FMR=0.019% for images NIST labels as 'Black women' when configured with a confidence threshold that produces FMR=0.001% for images labeled 'white men'. See 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, Annex 12, Figure 118.

[162] The algorithm yields FMR=0.05% for images NIST labels as 'American Indian men' and FMR=0.12% for images NIST labeled 'American Indian women' when configured with a confidence threshold that produces FMR=0.001% for images labeled 'white men'. See 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, Annex 12, Figure 118.

[163] The algorithm yields FNMR=0.64% for images NIST labels as 'American Indian men', FNMR=0.6% for images NIST labeled 'American Indian women', and FNMR=0.44% for images labeled 'White men' when configured with a confidence threshold that produces FMR=0.001% for images labeled 'white men'. 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, Annex 12, Figure 118.

[164] The average false negative rate for individuals from East Africa, West Africa and the Caribbean countries in 1:1 comparisons between high quality visa applications and images designed to emulate border control photos taken at kiosks and other automate infrastructure is FNMR=0.5138%, whereas the average false negative rate for individuals from Eastern European countries is FNMR=0.3981%. 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, Figure 22.

[165] Mei Wang & Weihong Deng, "Deep Face Recognition: A Survey", *version 8*, February 12, 2019, https://arxiv.org/pdf/1804.06655.pdf; Brendan F Klare, Mark J Burge, Joshua C Klontz, Richard W Border Bruegge & Anil K Jain, "Face Recognition Performance: Role of Demographic Information", (2012) 7(6) IEEE Transactions on Information Forensics & Security 1789, https://doi.org/10.1109/TIFS.2012.2214212, p 6: "Together, these results strongly suggest that the

diverse training datasets will not, in and of itself, remove all variance in algorithmic recognition across some racial and ethnic groups.[166]

In light of this, the impact of an algorithm cannot be assessed solely on the basis of aggregate false positive/negative rates, as this general assessment will obscure the algorithm's racial bias and, by extension, its impact on specific demographic groups.

Despite these challenges, racial and demographic bias is often ignored when border control systems are adopted and operated. A Canadian facial recognition system used to assess whether images submitted in passport applications have been previously used in association with other identities, for example, only reported the system's overall ability to generate accurate results and did not assess whether this accuracy applied consistently across different racial and demographic groups.[167] Another system adopted to facilitate automated customs and immigration processing of incoming travellers does not appear to have contemplated racial bias either, and border control officials operating the system appear to have been surprised that racial bias was a factor that needs to be considered.[168] Similarly, despite an administrative obligation to rigorously test general accuracy in border control biometric systems, racial bias is only now being assessed in central facial recognition systems by United States Customs and Border Protection.[169]

1.3.3 Invariance to ageing, age groups must be assessed

Despite gains in overall accuracy, some personal characteristics continue to pose a challenge for facial recognition systems.

Ageing continues to impact algorithmic recognition accuracy, with studies suggesting meaningful deterioration in the ability to recognize individuals accurately based on reference images that were enrolled 8-9 years earlier on average, and within 5-6 years for some.[170] There is also some indication

female cohort is inherently more difficult to recognize. … One explanation may be the use of cosmetics by females (i.e., makeup), which results in a higher within-class variance for females than males."

[166] Cynthia M Cook, John J Howard, Yevgeniy B Sirotin, Jerry L Tipton & Arun S Vemury, "Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems", (2019) 1(1) *IEEE T-BIOM* 32, https://ieeexplore.ieee.org/document/8636231.

[167] Passport Canada, "Facial Recognition Application Project – Privacy Impact Assessment: Executive Summary", June 28, 2016, https://www.international.gc.ca/gac-amc/publications/atip-aiprp/assessments-evaluation/facial-faciale.aspx:

> In the proposed Passport Office application of FR technology, an operator in the Security Division would confirm a suggested computer match of the photographs using FR software. Confirmation by the operator requires a judgment call that the individual in the two photographs appear to be the same individual. … The correct match is proposed within the top 10 positions by the technology over 90% of the time. These figures apply for the images of the best quality. For images of a lower quality such as RCMP–provided photographs, the percent in the top then choices drops to 75%. For more complete results, please refer to the document prepared by the Passport Office.

[168] 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.

[169] United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, p 52.

[170] Lacey Best-Rowden & Anil K Jain, "Longitudinal Study of Automatic Face Recognition", 2018 40(1) *IEEE Transactions on Pattern Analysis and Machine Intelligence* 148.

that deterioration in accuracy can be up to 2 years faster for women than for men.[171] Younger age groups continue to pose particular challenges for facial recognition algorithms, with substantially higher false negative rates for those below 16 and even 20 years of age.[172] Individuals over 65 also produce high false positive rates, particularly for women.[173] Algorithmic accuracy should therefore be gauged with these potential variations in mind, as their impact on travellers will depend on whether they are used across all age groups, and whether there are mechanisms in place to control for ageing.

Some border control initiatives therefore exclude older and younger travellers from facial recognition programs, with travellers under 14 years of age and over 79 years of age frequently excluded categorically.[174] Even with this exclusion, however, age-related bias persists. For example, a pilot program operated by United States Customs and Border Protection found that travellers aged 14-29 and 70-79 were substantially over-represented among false-non-matches (FNMR).[175]

A real-world imposter is likely to attempt to impersonate an individual with comparable age, gender and demographic background and so an accurate estimation of real world false positive rates should account for those variables. In addition, false positives are higher when tested *within* an age group then when tested across all age groups (e.g. where an imposter seeks to impersonate a traveller of comparable age).[176] Finally, age-related recognition errors can exacerbate racial and gender-driven recognition challenges, further elevating error rates. Ultimately, ongoing challenges with racial bias may render the technology inappropriate for wide-spread adoption.

---

[171] Lacey Best-Rowden & Anil K Jain, "Longitudinal Study of Automatic Face Recognition", 2018 40(1) *IEEE Transactions on Pattern Analysis and Machine Intelligence* 148.

[172] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020 https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, page 108 and Figures 166-183 (with respect to visa images: "Younger subjects give considerably higher FNMR. This is likely due to rapid growth and change in facial appearance"). Note that this represents FNMR variation on the basis of current age group, not on the basis of ageing (This is accomplished by assigning subjects to age bracket based on the average between their current age and the their visa image age, and as such the actual number of years elapsed between the two images being matched is not a factor); 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, p 51.

Initially set out in: Patrick Grother & Mei Ngan, "Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms", *NIST Interagency Report 8009*, May 26, 2014, https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf, p 36.

[173] 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, p 51: "For women from all most countries, comparison of images of individuals in the 65-and-over age group produce the highest false match rates. For men this is often true also."

[174] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, footnote 13 and p 12 ("To calculate these results, CBP only counted passengers between the ages of 14 and 79 who were included in the biometric pilot."); *Immigration and Refugee Protection Act*, SC 2011, c 27, sections 10.01 and 10.02 ("10.01 A person who makes a claim, application or request under this Act must follow the procedures set out in the regulations for the collection and verification of biometric information..."). *Immigration and Refugee Protection Regulations*, SOR/2002-227, *as amended*, paragraphs 12.2(1)(a)-(b):) 12.2 (1) Section 10.01 of the Act does not apply to (a) a person who is under the age of 14; (b) a person who is over the age of 79, unless that person makes a claim in Canada for refugee protection").

[175] Travellers under the age of 29 comprised about 18% of all travellers tested in the pilot, but generated 36% of all failures to match against their reference images, whereas travellers over the age of 70 represented 4% of tested travellers but comprised 10% of travellers who failed to match against their reference images. United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, p 19. See also footnote 13 and p 12 ("To calculate these results, CBP only counted passengers between the ages of 14 and 79 who were included in the biometric pilot.").

[176] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", NIST Interagency Report XXXX DRAFT, May 21, 2020 https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, p 243.

1.3.4 Bias in Capture Apparatus, Image Quality Assurance & Face Detection

The use of inferior image capture apparatus and poor lighting contributes to higher errors in the recognition process by producing low-quality probe images or failing to acquire traveller's facial image altogether. Members of marginalized groups can be disproportionately excluded as result.

A facial recognition system's real-world accuracy should take into account its **Failure to Acquire** ("**FtAR**") rate. Failure to acquire occurs where facial recognition of a traveller fails because the system was unable to detect the traveller's face or if the quality of a captured facial image is too low to create a biometric template.[177] In addition, images that are successfully 'captured' but are of lower quality can produce higher error rates in the comparison process.[178] Note that FtAR is a subset of the False Negative Identification Rate and the False Non-Match Rate described in Section 1.3.1, above. That is, where a 'Failure to Acquire' prevents an enrolled traveller from being recognized, it will be counted as a 'false negative'.[179] However, it is important to track FtAR because its impact on overall false negative rates can be distinct while there may be limits on ameliorating image capture related deficiencies that cannot be resolved through improvement of algorithms alone. In other contexts, where facial detection or image quality assurance algorithms are used as stand-alone requirements of a border control function, failure of such techniques can directly impact service availability.

If a given facial image is too blurry, for example, the image might be discarded without any attempt being made to extract its biometric description. The amount of time a camera is given to record a facial image can impact a given facial recognition system's failure to acquire rate. In

[177] Where a facial recognition system fails to detect a face in an image at all, this is more precisely referred to as a 'Failure to Capture'.The Failure to Acquire rate is inclusive of Failure to Capture: ISO/IEC, Information Technology – Vocabulary – Part37: Biometrics, ISO/IEC 2382-37:2017(E), 3.9.3, 3.9.4 and 3.9.5.

[178] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", *NIST Interagency Report 8271: Draft Supplement*, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, Figures 22-25 (across most algorithms, FNIR is consistently better (lower) for high quality mugshot images than for lower quality webcam probes) and p 2 ("Quality: The low error rates here are attained using mostly excellent cooperative live-capture mugshot images collected with an attendant present. Recognition in other circumstances, particularly those without a dedicated photographic environment and human or automated quality control checks, will lead to declines in accuracy. This is documented here for poorer quality webcam images and unconstrained "wild" images.").

Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, p 4: "This report includes results for a new dataset - see the column labelled "visa-border" in Table 5. It compares a new set of high quality visa-like portraits with a set webcam border-crossing photos that exhibit moderately poor pose variations and background illumination. The two new sets are described in sections 2.3 and 2.4. The comparisons are "cross domain" in that the algorithm must compare "visa" and "wild" images."; and Tables 6-10, where comparisons that involve lower quality border control images (columns 5 and 6) and 'Wild' images (column 7) generate worse (higher) FNMR).

[179] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, Section 3.3 Failure to Enroll ("[Failure to Enroll] is the proportion of failed template generation attempts. Failures can occur because the software throws an exception, or because the software electively refuses to process the input image. This would typically occur if a face is not detected. FTE is measured as the number of function calls that give EITHER a non-zero error code OR that give a "small" template. This is defined as one whose size is less than 0.3 times the median template size for that algorithm. This second rule is needed because some algorithms incorrectly fail to return a non-zero error code when template generation fails. The effects of FTE are included in the accuracy results of this report by regarding any template comparison involving a failed template to produce a low similarity score. Thus higher FTE results in higher FNMR and lower FMR."

Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 2: Identification", NIST Interagency Report 8271: Draft Supplement, March 27, 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf, pp 18-19 ("we define a "miss rate" with the general name **false negative identification rate** (FNIR) ... This formulation is simple for evaluation in that it does not distinguish between causes of misses. Thus a mate that is not reported on a candidate list is treated the same as a miss arising from face finding failure, algorithm intolerance of poor quality, or software crashes. Thus if the algorithm fails to produce a candidate list, either because the search failed, or because a search template was not made, the result is regarded as a miss, adding to FNIR.")

particular, with current technologies, facial recognition systems that attempt per-traveler transactions times below 4-6 seconds might experience higher failure to acquire rates.[180] Creating conditions for higher transaction times at borders could involve asking travelers to stand in front of fixed cameras for a fixed period of time or ushering travellers through fixed pathways that grant sensors unobstructed views for more extended periods of time. It is similarly important that high quality cameras are used, capable of capturing high resolution images at high frame rates.[181] Lighting should similarly be controlled to the greatest degree possible.[182] In one field test at an airport, an FNIR of 25% (compared to an FNIR of 2% in other similar field tests) was attributed to poor lighting leading to inferior image quality.[183]

Different facial recognition implementations may also require wholly different capture apparatus. For example, facial recognition at land ports of entry/exit might require specific lenses capable of overcoming image capture challenges arising from the interjection of car windshields.[184]

Aspirationally, capture apparatus should be able to consistently generate images of the same quality as those used in ICAO-compliant machine-readable passports.[185] These can be mitigated to some degree, often by using sacrificing some efficiency in traveller processing, and border control agencies must carefully assess these tradeoffs.[186] Realistically, border control images will be of

[180] Jacob A Hasselgren, John J Howard, Yevgeniy B Sirotin, Andrew J Blanchard & Arun S Vemury, "Operational Tradeoffs in the 2018 Department of Homeland Security Science and Technology Directorate Biometric Technology Rally", (2018) *IEEE International Symposium on Technologies for Homeland Security* 1, https://doi.org/10.1109/THS.2018.8574183. This is one conclusion from DHS S&T Directorate's 2018 Biometric Technology Rally, which compared several different facial recognition mechanisms under somewhat controlled settings. The test found that facial recognition systems with per individual transaction times of approximately 4-9 seconds were exhibited lower failure to acquire rates. Algorithms with slower or faster transaction times tended to exhibit poorer ratings. However, it should be noted that specific facial recognition competitors were not tested at different transaction rates to measure the impact that such changes could have on the same system.

[181] European Union, FRONTEX, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", September 2015, https://doi.org/10.2819/86138, p 40.

[182] European Union, FRONTEX, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", September 2015, https://doi.org/10.2819/86138, p 40.

[183] United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, pp 51 and 53: "for one of the flights we observed, TVS was unable to match approximately 25 percent of travelers, even after repeated attempts. According to CBP officials who investigated the issue, the low match rate was caused by problems with the cameras and lighting at the gate—specifically, the photos taken were not of sufficient quality to match to the photos in the TVS gallery"

See also: 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, p 54:

> In domestic mugshots, the lowest FNMR in images of subjects whose race is listed as [B]lack. However, when comparing high-quality appliction photos with border-crossing images, FNMR is often highest in African born subjects. We don't formally measure contrast or brightness in order to determine why this occurs, but inspection of the border quality images shows underexposure of dark skinned individuals often due to bright background lighting in the border crossing environment. In mugshots this does not occur. In neither case is the camera at fault.

[184] Russell Brandon, "New Homeland Security System Will Bring Facial Recognition to Land Borders This Summer", June 5, 2018, *The Verge*, https://www.theverge.com/2018/6/5/17427150/facial-recognition-vehicle-face-system-homeland-security-immigration-customs.

[185] European Union, FRONTEX, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", September 2015, https://doi.org/10.2819/86138, p 40.

[186] United States, Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 11:

> Due to the large volume of travelers and border crossers, it would not be practical for CBP to use formally-generated frontal head-on facial images, such as are taken for a driver's license or passport. Rather, CBP is increasingly employing technologies that do not require subjects to present their face directly to the camera. Given this new focus, technology providers are continuing to refine their solutions to collect face images with minimal participation from the subject. While a more streamlined capture of facial images (rather than a "stop and look" approach) poses operational benefits to CBP, it also poses increased privacy risks since the individual may be unaware that their photo is being captured.

lower quality as they are taken without direction from a photographer and under time and lighting constraints.[187]

The impact of an inferior image capture system, face detection and image quality control algorithms will often fall more heavily on marginalized demographic groups. For example, the United Kingdom applied a face feature detection algorithm to images submitted through its online passport application portal.[188] While the face detection algorithm operated with sufficient accuracy in general, facial images with very light or dark skin tone were consistently rejected on the erroneous basis that they failed to meet image requirements such as having eyes open and mouths closed.[189] Some stand-alone image quality enhancement algorithms have also exhibited similar racial biases.[190]

Photographic lenses and other image capture equipment are often designed and calibrated in ways that reduce its ability to capture darker skin tones.[191] Background lighting that are calibrated for average skin tones render attempts to capture faces with very light or very dark skin tones difficult.[192] The lower skin reflectance of faces with darker skin tones will, in general, mean that higher quality image capture equipment and more time is required to capture facial images capable of producing comparable accuracy.[193] However, as border control conditions do not currently always permit for capture of high-quality images, it is likely that low probe image quality will contribute to racial bias in facial recognition systems for the foreseeable future.

---

[187] Patrick Grother, Mei Ngan & Kayee Hanaoka, "Ongoing Face Recognition Venter Test (FRVT), Part 1: Verification", *NIST Interagency Report XXXX DRAFT*, May 21, 2020, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf, p 26: NIST has generated a testing dataset designed to emulate border control live capture images. Images contained in the dataset generally emulate the varying conditions faced by fixed cameras at border control settings, such as those embedded in kiosks: "The images are taken with at camera oriented by an attendant toward a cooperating subject. This is done under time constraints so there are role, pitch and yaw angle variations. Also background illumination is sometimes strong, so the face is under-exposed. There is some perspective distortion due to close range images. Some faces are partially cropped."

[188] Adam Vaughan, "UK Launched Passport Photo Checker it Knew Would Fail with Dark Skin", October 9, 2019, *NewScientist*, https://www.newscientist.com/article/2219284-uk-launched-passport-photo-checker-it-knew-would-fail-with-dark-skin/.

[189] Adam Vaughan, "UK Launched Passport Photo Checker it Knew Would Fail with Dark Skin", October 9, 2019, *NewScientist*, https://www.newscientist.com/article/2219284-uk-launched-passport-photo-checker-it-knew-would-fail-with-dark-skin/:

> Now, documents released by the Home Office this week show it was aware of problems with its website's passport photo checking service, but decided to use it regardless. "User research was carried out with a wide range of ethnic groups and did identify that people with very light or very dark skin found it difficult to provide an acceptable passport photograph," the department wrote in a document released in response to a freedom of information (FOI) request. "However; the overall performance was judged sufficient to deploy."

See also: Alex Hern, "Twitter Apologises for 'Racist' Image-Cropping Algorithm", *The Guardian*, September 21, 2020, https://www.theguardian.com/technology/2020/sep/21/twitter-apologises-for-racist-image-cropping-algorithm.

[190] Katyanna Quach, "Once Again, Racial Biases Show up in AI Image Databases", *The Register*, June 24, 2020, https://www.theregister.com/2020/06/24/ai_image_tool/.

[191] Sarah Lewis, "The Racial Bias Built Into Photography", April 25, 2019, *New York Times*, https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html; Cynthia M Cook, John J Howard, Yevgeniy B Sirotin, Jerry L Tipton & Arun S Vemury, "Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems", (2019) 1(1) *IEEE T-BIOM* 32, https://ieeexplore.ieee.org/document/8636231.

[192] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, p 90; 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, p 54: "…when comparing high-quality application photos with border-crossing images, FNMR is often highest in African born subjects. We don't formally measure contrast or brightness in order to determine why this occurs, but inspection of the border quality images shows underexposure of dark skinned individuals often due to bright background lighting in the border crossing environment. In mugshots this does not occur. In neither case is the camera at fault."

[193] Cynthia M Cook, John J Howard, Yevgeniy B Sirotin, Jerry L Tipton & Arun S Vemury, "Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems", (2019) 1(1) *IEEE T-BIOM* 32, https://ieeexplore.ieee.org/document/8636231.

1.3.5 Relative efficiency must take into account level of intrusiveness

When assessing the anticipated efficiency gains of a given facial recognition system, it is important to account for the comparative intrusiveness of these gains. Efficiency gains should not be assessed solely against a backdrop of manual processing where a spectrum of solutions exist. For example, Vancouver Airport Authority's BorderXpress automated data-entry kiosk achieved substantial reduction in traveller processing times without incorporating any automated recognition process.[194] Other automation mechanisms could readily incorporate remote manual facial comparison without resorting to automated facial recognition and additional staffing.[195]

1.3.6 Measuring Accuracy & Impact: Periodic Real-World Testing

Facial recognition systems must be rigorously tested in settings that emulate real-world conditions prior to their adoption. Accuracy and impact must also be assessed on a periodic basis should a facial recognition system be implemented as even the most robust test settings cannot emulate all real-world conditions,[196] and to account for real-world.[197]

Theoretical algorithm quality does not necessarily correlate with real-world accuracy. For example, one top performing algorithm displayed unexpectedly higher False Match Rates when calibrated for high quality mugshot images, but used on equally high-quality Visa application images.[198] In another example, a pilot facial recognition program operated by the United States Customs and Border Protection found that the real-world false negative rate generated by an algorithm in an actual airport

---

[194] Airport Technology, "Vancouver Airport: Selling the BorderXpress System", February 9, 2016, https://www.airport-technology.com/features/featurevancouver-airport-selling-the-borderxpress-system-4800855/.

[195] United Kingdom, Home Affairs Committee, "Work of the UK Border Agency (August-December 2011)", 21st Report, March 27, 2012, https://publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1722/172202.htm, paras 59 and 62:

> One of the methods the UK Border "Agency" uses to reduce queuing times is e-Gates which read biometric chips in passports. Since 2006, a chip has been inserted into British passports, which carries biometric and biographical details about the holder and is presented into a "reader" at an airport. The information is verified by a facial recognition camera and if the information is correct the gates open. It is overseen by a UK Border "Agency" official but there are no physical checks of the passport itself. Currently, there are 63 e-Gates, at Heathrow, Gatwick, Stansted, Luton, Birmingham, East Midlands, Cardiff, Bristol and Manchester airports. At present, UK Border "Agency" staff are responsible for the operation and monitoring of all gates but once machines are fully introduced, staff will not be allocated to oversee the work of the machines. …
>
> IRIS—the iris recognition immigration system, a fore-runner of e-Gates, was launched in 2006. …IRIS had been criticised by travellers for taking longer than going through passport control. Between 2006 and April 2011, IRIS cost the Home Office £9.1 million. A June 2010 job advert for an immigration officer (staff who are based at ports of entry to examine documents and interview people to establish their eligibility for entry to the UK) puts the starting salary at £21,000-£22,000. This means that roughly 60 immigration officers could have been employed for the six years with the money that IRIS cost.

[196] United States, Government Accountability Office, "Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy", May 2016, GAO-16-267, p 36: "Moreover, as discussed above, accuracy rates of face recognition technologies may be different in a test setting than an operational setting, where other factors—such as the quality of the face photos in the database—can affect accuracy."; D.O. Gorodnichy, S.N. Yanushkevich & V.P. Shmerko, "Automated Border Control: Problem Formalization", *CBSA Science & Engineering Directorate*, Division Report 2014-41, September 2014, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc203/p801324_A1b.pdf.

[197] Jacob A Hasselgren, John J Howard, Yevgeniy B Sirotin, Andrew J Blanchard & Arun S Vemury, "Operational Tradeoffs in the 2018 Department of Homeland Security Science and Technology Directorate Biometric Technology Rally", (2018) *IEEE International Symposium on Technologies for Homeland Security* 1, https://doi.org/10.1109/THS.2018.8574183.

[198] 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, p 40: "Some algorithms, most notably those from Sensetime give FMR much different to the target value. The threshold was set using Annex 1 mugshots but the Figure reflects FMR measured over comparison of Annex 2 application photos. Both sets of photos are well illuminated portraits, so this instability across datasets would be unwelcome, especially if an algorithm were to be fielded on imagery qualitatively different."

setting was 7.5 times higher (FNIR=15%) than the theoretical false negative rate achieved by the same algorithm when only tested on facial images intended to emulate real world settings (FNIR=2%).[199] In other words, while the algorithm was able to theoretically process 98% of travellers based on image matching tests, in reality the facial recognition system was only able to process 85% of travellers. The discrepancy was attributed to technical issues regarding network connectivity, problems matching younger and older travellers (ages 14-29 and 70-79), and a lack of quality reference images for some types of travellers.[200] Note that travellers below the age of 14 and over the age of 79 were categorically excluded from the study, further reducing the volume of travellers that could be successfully processed by this facial recognition system.[201]

Calibration of recognition algorithms (setting confidence thresholds) must be done in real-world settings to account for these potential variations, and to ensure that the impact of inferior capture equipment, lighting differences, and other unforeseeable conditions is accounted for.[202] Assessing the true detrimental impact of an algorithm also requires assessment in real-world settings for the same reasons. Real world volumes must also be taken into account when assessing the true detrimental impact of a recognition algorithm, as even small error rates can have unacceptable impact when applied to millions of travellers.[203] This is particularly the case where recognition algorithms operate with racial biases that are applied systematically to large proportions of marginalized populations.[204]

---

[199] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, p 16:

> In 2017, the Sprint 8 pilot yielded a low biometric match rate. Although CBPintentionally did not target a specific match rate during the pilot, the end goal of the program is to biometrically confirm the departures of 97 to 100 percent of all foreign visitors processed through the major U.S. airports. During Sprint 8, from August to December 2017, TVS enabled CBP to technically match the photos of boarding passengers to photos in the digital gallery 98 percent of the time. However, TVS was unable to biometrically confirm 15 percent of all departing passengers included in the pilot. More specifically, the program's overall biometric confirmation rate only averaged 85 percent during our audit fieldwork, from August to December 2017.

[200] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, pp 18-19.

[201] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, p 12:

> To calculate these results, CBP only counted passengers between the ages of 14 and 79 who were included in the biometric pilot. CBP officials considered these results a success, although they had not previously established a metric for photo matching. We validated these results by using CBP data to calculate average match rates for December 2017.

[202] European Union, FRONTEX, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", September 2015, https://doi.org/10.2819/86138,p 42:

> The operating agency SHOULD NOT rely solely on the standard configuration of the algorithm provider. For live operation of the system, it is RECOMMENDED to determine a proper algorithm configuration based on image data and verification results (cross-comparisons between different travellers) from the actual operational environment and a representative catalogue of test users. It is RECOMMENDED to monitor the error rates (especially the FAR) continuously or at least periodically (e.g. once a year) and to adjust the configuration if needed.

[203] Jacob A Hasselgren, John J Howard, Yevgeniy B Sirotin, Andrew J Blanchard & Arun S Vemury, "Operational Tradeoffs in the 2018 Department of Homeland Security Science and Technology Directorate Biometric Technology Rally", (2018) *IEEE International Symposium on Technologies for Homeland Security* 1, https://doi.org/10.1109/THS.2018.8574183:

> At these volumes, even error rates that would typically be considered acceptable for a biometric system (one to three percent) could cause hundreds to thousands of non-identification exceptions, meaning high-throughput systems must be extremely accurate.

[204] See Box 19, at p 139, below, for more details.

Even systems meeting best practice operational accuracy in real-world settings will still detrimentally impact millions of travellers on a daily basis,[205] with greater and more significant impact on particular demographic groups resulting from biased application. As noted above, over 33 million travellers entered Canada in 2019 through air ports of entry, an average of 92,000 per day.[206] A false positive rate of %0.0092 and a false negative rate of 2% would yield about 8 false positives and 1,856 false negatives per day, which, on an annual basis, amounts to 3,116 false positives and 677,491 false negatives.[207] In this regard, while it is important that theoretical and prototype-based accuracy thresholds inform the assessment of facial recognition systems at the procurement stage, it is not appropriate to permit these theoretical or prototype-based accuracy rates to justify inferior operational inaccuracy rates,[208] as doing so would underestimate the detrimental impact experienced by travellers.

The **Operational Rejection Rate** ("**ORR**") assesses the rate at which an automated facial recognition system is compelled to refer travellers to manual processing, regardless of the reason.[209] ORR will include travellers who cannot be automatically processed due to facial comparison errors, a failure to acquire an image of sufficient quality to attempt a comparison, as well as traveller rejection that is unrelated to biometric recognition, such as where a traveller fails an automated watch list checks. ORR is an important measure, as it assesses the overall efficiency of an implemented facial recognition system. It is therefore an important metric for assessing the true effectiveness and impact of an implemented facial recognition system.

For example, Germany's EasyPASS e-Gates are unable to process about 5.6% of all travellers.[210] Approximately 2.6% of these rejections are attributed to the facial recognition component of EasyPASS, while 0.01% result from attempts to read information on the electronic travel documents being used, and 3% result from other reasons such as where a traveller fails a background check.[211]

---

[205] European Union, FRONTEX, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", September 2015, https://doi.org/10.2819/86138, p 42; Jacob A Hasselgren, John J Howard, Yevgeniy B Sirotin, Andrew J Blanchard & Arun S Vemury, "Operational Tradeoffs in the 2018 Department of Homeland Security Science and Technology Directorate Biometric Technology Rally", (2018) *IEEE International Symposium on Technologies for Homeland Security* 1, https://doi.org/10.1109/THS.2018.8574183: "At these volumes, even error rates that would typically be considered acceptable for a biometric system (one to three percent) could cause hundreds to thousands of non-identification exceptions, meaning high-throughput systems must be extremely accurate."

[206] Statistics Canada, "International Travellers Entering or Returning to Canada", Table 24-10-0005-01 (formerly CANSIM 427-0005), https://doi.org/10.25318/2410000501-eng, (Summing results for January – December, 2019, for "United States Residents Entering by Plane", "Travellers from Countries Other than United States Entering by Plane", "Canadian Travellers Returning from the United States by Plane" and "Canadian Travellers Returning from Countries other than United States by Plane". The annual total is 33,874,557, which amounts to 92,807 travellers per day, on average.

[207] United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, p 51, Table 2: United States Customs and Border Protection employs a facial recognition system with a 0.0092% false positive rate and a 98% false negative rate for travellers entering and leaving the United States.

[208] D.O. Gorodnichy, S.N. Yanushkevich & V.P. Shmerko, "Automated Border Control: Problem Formalization", *CBSA Science & Engineering Directorate*, Division Report 2014-41, September 2014, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc203/p801324_A1b.pdf.

[209] D.O. Gorodnichy, S.N. Yanushkevich & V.P. Shmerko, "Automated Border Control: Problem Formalization", *CBSA Science & Engineering Directorate*, Division Report 2014-41, September 2014, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc203/p801324_A1b.pdf, p 2.

[210] Markus Nuppeney, "Automated Border Control (EasyPASS): Monitoring the System Performance", *NIST: IFPC 2018*, November 27, 2018, https://nigos.nist.gov/ifpc2018/presentations/05_nuppeney_20181127_IFPC2018_EasyPASS_Nuppeney.pdf.

[211] Markus Nuppeney, "Automated Border Control (EasyPASS): Monitoring the System Performance", *NIST: IFPC 2018*, November 27, 2018, https://nigos.nist.gov/ifpc2018/presentations/05_nuppeney_20181127_IFPC2018_EasyPASS_Nuppeney.pdf.

However, the ultimate efficiency gains of adopting facial recognition in German airports in lieu of manual processing are nonetheless constrained by the need to account for these factors.

Similarly, a pilot operated by United States Customs and Border Protection at 9 major international airports compared travellers' live facial images to pre-populated image galleries of facial images generated for each departing flight on a 1:N basis.[212] While 99.4% of in-scope travellers were successfully matched (an FPIR of 0.03% and FNIR of 0.5%), the pilot excluded all travellers under the age of 14 and over the age of 79 as out of scope, and an additional 1% of all remaining travellers could not be processed as no reference image was available.[213] Additional practical challenges (staffing shortages, network interruption accessing CBP's cloud-based reference galleries, and demanding flight schedules) led to an inability to process 15% of all travellers.[214] More comprehensive CBP testing successfully matched 98% of successfully captured images (FPIR of 0.0092% and FNIR of 2%), but failed to capture 20% of in-scope travellers for a range of pragmatic considerations.[215] As travellers aged below 14 and above 79 are categorically excluded, the ORR of this system is well above 22%.

An internal 2017 CBSA assessment indicated that approximately 10% of all travellers were referred to secondary inspection, predominantly by Canada's automated Primary Inspection Kiosks.[216] While CBSA did not publicly disclose what proportion of these PIK referrals are attributable to facial recognition failures, 10% of travellers must be manually processed, impacting the overall efficiency of the automated system.[217] Also absent are statistics regarding the number of travellers who were forced to process manually due to facial recognition failures, but were *not* referred to secondary inspection.

In both these examples, the capacity to accurately forgo manual processing of travellers is substantially lower than is reflected by a facial recognition algorithm's optimized accuracy rating. Yet this overall metric remains a more accurate reflection of the benefits and detrimental impacts of the facial recognition system as implemented.

---

[212] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.

[213] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.

[214] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, pp 16-18.

[215] United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, pp 51-52.

[216] 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.

[217] 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.

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.

1.4 Consent & Individual Choice in Creation & Use

Individual involvement and awareness of participation in border control facial recognition systems can vary substantially, and is a distinct factor when algorithms are trained to recognize faces, when individuals are enrolled in reference datasets, and in the operation of a facial recognition system.

For a facial recognition border control system to be considered 'voluntary' the choice to participate in it must be meaningful. It is not sufficient to simply indicate that it is optional, choice must be easy to exercise.[218] Where a facial recognition system is a necessary condition of holding a passport, it is not considered to be 'voluntary', as passports are essential for any citizen wishing to travel abroad.[219] Similarly, where refusal to enroll in a biometric system can lead to adverse treatment, it might not be considered voluntary even if enrollment is not legally mandatory.[220]

1.4.1 Enrolling in a facial recognition system by choice

Enrollment in a reference dataset can occur with or without participation of the individual being enrolled. Canada, for example, has repurposed its passport image database into a passport fraud detection utility—images submitted with passport applications are compared to all historical passport images in order to determine if same individual is applying under multiple names.[221] Other states have repurposed passport image databases for facial recognition systems operated at ports of entry/exit.[222] Enrollment in these systems is not optional—anyone with a travel document is included. Passport holders may not even be aware that their historical and application images have been enrolled.

---

[218] Jason Kelley, "Skip the Surveillance By Opting Out of Face Recognition at Airports", April 24, 2019, *Electronic Frontier Foundation*, https://www.eff.org/deeplinks/2019/04/skip-surveillance-opting-out-face-recognition-airports; Allie Funk, "I Opted Out of Facial Recognition at the Airport—It Wasn't Easy", July 2, 2019, *WIRED*, https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/.

[219] *Schwarz v City of Bochum*, Case C-291/12, (2013, Court of Justice of the European Union Fourth Chamber), para 60.

[220] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, pp 33, 80:

> One asylum applicant from Afghanistan explained that he gave his fingerprints because the Hungarian authorities had stated that collecting his fingerprints was only for security purposes, and because any person who declined to give their fingerprints would be deprived of their liberty until they complied with this obligation. It was only after he arrived in Sweden and provided his fingerprints again that he discovered the implications on the asylum procedure. The interviewee felt deceived. …
>
> The high quality of fingerprints in Eurodac is of paramount importance to ensure the correct application of the Dublin Regulation. 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.

[221] Office of the Privacy Commissioner of Canada, "Automated Facial Recognition In the Public and Private Sectors", March 2013, https://www.priv.gc.ca/media/1765/fr_201303_e.pdf, p 6. Canada has empowered its passport control agency (Passport Canada, at the time) to "convert an applicant's photograph into a biometric template for the purpose of verifying the applicant's identity, including nationality, and entitlement to obtain or remain in possession of a passport." At the same time, Canada was also empowered to "convert any information submitted by an applicant into a digital biometric format for the purpose of inserting that information into a passport": Canadian Passport Order, SI/81-86, PC 1981-1472, section 8.1, adopted in Order Amending the Canadian Passport Order, SI/2004-113, September 1, 2004: http://www.gazette.gc.ca/rp-pr/p2/2004/2004-09-22/pdf/g2-13819.pdf.

[222] The United States and Australia have both made passport image databases available to their respective ports of entry/exit programs: *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum; *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement; United States, Department of Homeland Security, Customs and Border Protection, "Privacy Impact Assessment: Traveler Verification Service (TVS): CBP-TTSA Technical Demonstration Phase II", August 14, 2018, DHS/CBP/PIA-030(e); United States, Department of Homeland Security, Customs and Border Protection, "Privacy Impact Assessment Update: Traveler Verification Service (TVS): CBP-TSA Technical Demonstration", September 25, 2017, DHS/CBP/PIA-030(d).

Travellers are often given a choice as to whether they will be enrolled into a state's facial recognition system. For example, NEXUS is a 'secure' or 'trusted' traveller program designed to facilitate expedited processing at Canada-US border crossings for pre-vetted travellers deemed to be low risk. Whereas travellers are typically only subjected to border control scrutiny when attempting to cross an international border, NEXUS applicants voluntarily submit to enhanced risk and identity assessments at the application stage and on a periodic *ad hoc* basis to ensure the traveller's continued 'trusted' status.[223] NEXUS applicants are also enrolled into a biometric verification system, which is used for higher identity assurance at border crossings in order to reduce the risk that 'trusted' identities will be subverted.[224] Historically, iris scans and fingerprints were the dominant biometric used in NEXUS however the program is currently transitioning to facial recognition instead.[225] Similarly, the World Economic Forum's KTDI proposal, currently being piloted by Canada, also envisions a user-centric biometric model. Individual travellers self-enroll by creating a facial recognition-enabled profile on their mobile devices (see Box 12).

Often, facial recognition programs are nominally voluntary but do not require active traveller application prior to enrollment, relying on an 'opt out' mechanism instead. For example, foreign travellers are provided the option of enrolling into Australia's facial recognition program for future visits, but are not compelled to do so.[226] When travellers enter Australia, they may optionally use facial recognition-enabled 'SmartGates' for processing entry.[227] For foreign travellers who have never been enrolled in Australia's national facial recognition system, SmartGates will verify travellers' passports by comparing their facial image to an image encoded on their biometric passports. Upon verification, foreign travellers are also enrolled into Australia's broader facial recognition system, which will be used upon future visits.[228] While use of the SmartGates is optional, it is not clear if foreign travellers are able to use the SmartGates without being enrolled in the Australian system, or if travellers are made aware that they are being persistently enrolled.

---

[223] Canada Border Services Agency, "NEXUS Privacy Impact Assessment: Executive Summary", March 1, 2017, https://cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/nex-eng.html.

[224] Canada Border Services Agency, "NEXUS Privacy Impact Assessment: Executive Summary", March 1, 2017, https://cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/nex-eng.html.

[225] Canada Border Services Agency, "NEXUS Privacy Impact Assessment: Executive Summary", January 14, 2020, https://cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/nexus-eng.html.

[226] *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, p 3: "... travellers will also retain the option of choosing manual processing, with the physical identity document, by a clearance officer if preferred." See also: *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum.

[227] A more complete description of the operation of these SmartGates in Australia can be found in Section 2.1.2 at p 68,below.

[228] *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5751_ems_2fb75e14-e450-4d1c-9c16-e0c27f0913b0%22, p 57: "Images provided by the traveller (both citizens and non-citizens) to the SmartGate are stored in departmental systems. A document based identity verification process occurs at the time the traveller self-processes through the SmartGate. This verified image and others collected during subsequent travel, become the images used by the Department to confirm identity on future travel."

Additionally, commercial facial recognition tools are increasingly being used by border control agencies. Clearview AI, for example, offers a commercial facial recognition tool that permits licensed subscribers to upload a facial image into its interface and will return a gallery of similar facial images from its reference dataset.[229] The reference dataset is comprised of facial images scraped from various online platforms such as Facebook, Twitter, YouTube and others. It was created without consent from the individuals whose images are included in it, and often in violation of the terms of use of the web platforms being scraped.[230] Clearview AI has been used by various United States border control agencies, including Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP).[231] Following a joint investigation by the Privacy Commissioners of Canada, British Columbia, Alberta and Québec, Clearview AI has said it will stop serving Canadian customers,[232] however it is not clear if this is a permanent departure, if Canadian personal information continues to be used in non-Canadian searches, or if other comparable commercial services exist.

Online platforms have also repurposed images provided on their platforms and enrolled these into facial recognition databases. Facebook, for example, enrolled many of its United States-based users in its facial recognition capability. Both Facebook and Clearview AI have faced class actions under an Illinois biometric privacy law for creating facial templates without obtaining meaningful consent, and the Facebook lawsuit has been certified and settled.[233]

1.4.2 Individual Participation in Creation of Training & Testing Datasets

A number of the largest publicly available facial recognition training datasets are also populated with images of individuals who were not aware that their online photos had been included.[234] To the extent

[229] Kashmir Hill, "The Secretive Company that Might End Privacy as We Know It", *New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[230] Kashmir Hill, "Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos", *New York Times*, January 22, 2020, https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html; Jacob Kastrenakes, "YouTube Demands Clearview AI Stop Scraping its Video for Facial Recognition Database", *The* Verge, February 5, 2020, https://www.theverge.com/2020/2/5/21124172/youtube-clearview-ai-cease-and-desist; Jon Porter, "Facebook and LinkedIn are Latest to Demand Clearview Stop Scraping Images for Facial Recognition Tech", *The Verge*, February 6, 2020, https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube.

[231] 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.

[232] Office of the Privacy Commissioner of Canada, "Clearview AI Ceases Offering its Facial Recognition Technology in Canada", *Office of the Privacy Commissioner of Canada*, July 6, 2020, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/; Office of the Privacy Commissioner of Canada, "Commissioners Launch Joint Investigation into Clearview AI Amid Growing Concerns over Use of Facial Recognition Technology", February 21, 2020, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/.

[233] *Patel v Facebook Inc*, Case No 18-15982 (9th Circuit, 2019). Facebook ultimately settled the class action for $550 million USD: Tony Romm, "Facebook Agrees to Pay $550 Million to Settle Privacy Lawsuit, Days After Supreme Court Declined to Hear Case", January 29, 2020, *Washington Post*, https://www.washingtonpost.com/technology/2020/01/29/facebook-has-agreed-pay-550-million-settle-class-action-privacy-lawsuit-days-after-supreme-court-declined-take-case/; *Mutnick v Clearview AI*, Case No 1:20-cv-00512, (Dist Ct, Illinois, 2020); Catalin Cimpanu, "Class-Action Lawsuit Filed Against Controversial Clearview AI Startup", January 24, 2020, *ZDNet: Zero Day*, https://www.zdnet.com/article/class-action-lawsuit-filed-against-controversial-clearview-ai-startup/.

[234] Russell Brandon, "Microsoft Pulls Open Facial Recognition Dataset After Financial Times Investigation", July 7, 2019, *The Verge*, https://www.theverge.com/2019/6/7/18656800/microsoft-facial-recognition-dataset-removed-privacy; Olivia Solon, "Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent", March 12, 2019, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.

these training datasets allow individuals to 'opt out', such opt out mechanisms have to date proven ineffective.[235] Creative Commons, which manages a licensing system intended to facilitate open access to copyrighted works such as photographs, has also faced criticism after images shared with its licenses on a photo sharing site were included in public training datasets.[236] In other instances, companies have reportedly used deceptive practices, paying individuals to provide their facial images without notifying them that the images will be used in a facial recognition training dataset.[237]

Private reference datasets will often similarly repurpose images provided by platform users who have not consented and have minimal interest in contributing to the creation of a facial recognition system. EverAI, a cloud-based photo storage service, has been criticized for using its customer's photos and image tagging activities to train a facial recognition algorithm, which fuels a number of facial recognition products the company sells to state agencies.[238]

These practices have prompted a class action lawsuits against the creator of one major publicly available training dataset, as well as against companies that used this dataset to train their facial recognition algorithms.[239] Complaints from individuals included in some public training datasets without consent have also led some companies to remove these datasets from public accessibility.[240]

1.4.3 Opting out of Facial Recognition at the Border

Many facial recognition systems are nominally 'opt out' in operation, offering travellers manual document verification as an alternative at border crossings. It is not clear how many travellers are aware that alternative options exist, and preliminary reporting suggests that the opt-out mechanisms are difficult to exercise by those who are aware of them. Other programs operate on an 'opt-in' basis.

---

[235] Olivia Solon, "Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent", *NBC News*, March 12, 2019, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.

[236] Shannon Liao, "Creative Commons Says Copyright Can't Protect Your Photos From Ending Up in a Facial Recognition Database", March 14, 2019, *The Verge*, https://www.theverge.com/2019/3/14/18265826/creative-commons-photos-facial-recognition-database.

[237] Julie Carrie Wong, "Google Reportedly Targeted People with 'Dark Skin' to Improve Facial Recognition", *The Guardian*, October 3, 2019, https://www.theguardian.com/technology/2019/oct/03/google-data-harvesting-facial-recognition-people-of-color; Jack Nicas, "Atlanta Asks Google Whether It Targeted Black Homeless People", *New York Times*, October 4, 2019, https://www.nytimes.com/2019/10/04/technology/google-facial-recognition-atlanta-homeless.html.

[238] Olivia Solon & Cyrus Farivar, "Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools", May 9, 2019, *NBC News*, https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.

[239] *Janecyk v International Business Machines*, Case No 2020CH00833, (Circ Ct, Illinois, 2020); Daniel R Stoller, "IBM Hit With Lawsuit Claiming Image Use for Facial Recognition", January 23, 2020, *Bloomberg Law*, https://news.bloomberglaw.com/privacy-and-data-security/ibm-hit-with-lawsuit-claiming-image-use-for-facial-recognition; and Steven Musil, "Amazon, Google, Microsoft Sued Over Photos in Facial Recognition Database", July 14, 2020, *CNet*, https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/.

[240] Russell Brandon, "Microsoft Pulls Open Facial Recognition Dataset After Financial Times Investigation", July 7, 2019, *The Verge*, https://www.theverge.com/2019/6/7/18656800/microsoft-facial-recognition-dataset-removed-privacy; Olivia Solon, "Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent", March 12, 2019, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.

Some facial recognition programs operate on a relatively robust opt-in basis at border crossings. Travellers choose to use secure traveller programs that rely on facial recognition on a case-by-case basis, by choosing to use the designated expedited 'secure traveller' process when submitting to security screening at border control crossings.[241] The World Economic Forum's KTDI proposal is also envisioned to operate on a user-centric case-by-case basis, with travellers choosing to provide different border control entities in different countries access to the facial recognition template encoded on their phones on an 'on demand' basis (see Box 12, below).

Other facial recognition programs generally apply to all travellers by default, but permit some travellers to 'opt out'. United States CBP's facial recognition program remains optional to some travellers including American citizens and some Canadian tourists,[242] while Australia's legal regime explicitly provides for manual processing as an alternative to automated facial recognition at border control contexts.[243]

These opt-out mechanisms have proven difficult to exercise. It is not clear that travellers are aware that manual processing is an option,[244] while the opaque nature of facial recognition will mean that at times travellers will not even be aware they are submitting to facial recognition at all. Canada's Primary Inspection Kiosks, for example, are now facial recognition-enabled, but it is not clear if travellers are aware that facial recognition is occurring, nor is it clear whether travellers are permitted to opt-out at all.[245] Border control agencies have been criticized for failing to ensure travellers are adequately notified that they are being subjected to facial recognition, and that alternative options exist.[246]

---

[241] For example, the Canada Border Services Agency is seeking to implement facial recognition in its dedicated secure traveller kiosks (NEXUS). To access these kiosks, travellers must first choose to enroll in NEXUS and second to use a dedicated NEXUS line-up: Canada Border Services Agency, "NEXUS – Privacy Impact Assessment", Executive Summary, last modified January 14, 2020, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/nexus-eng.html.

[242] Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 11; United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, footnote 4: "any alien may be required to provide biometric identifiers on entry, except certain Canadian tourists or businesspeople; aliens younger than 14 or older than 79; and diplomatic visa holders, among other listed exemptions."

[243] *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, p 3: "... travellers will also retain the option of choosing manual processing, with the physical identity document, by a clearance officer if preferred." See also: *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum.

[244] Allie Funk, "I Opted Out of Facial Recognition at the Airport—It Wasn't Easy", July 2, 2019, *WIRED*, https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/.

[245] See discussion in Section 1.6 at page 59, below. See also: In public statements, the CBSA has suggested that travellers do not have any choice in submitting to facial recognition where PIKs have been implemented:

> **Do I have to use a Primary Inspection Kiosk?**
>
> You are asked to use the kiosks where they are available as this allows us to provide you the best service. If you are ineligible or unable to use a kiosk, you will make your declaration to a border services officer when you arrive.

Canada Border Services Agency, "Primary Inspection Kiosks – Frequently Asked Questions", *cbsa.asfc.gc.ca*, last modified February 13, 2010: https://www.cbsa-asfc.gc.ca/travel-voyage/pik-bip-eng.html. The public version of CBSA's Privacy Impact Assessments are equally silent on the question of voluntariness.

[246] Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 11; United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, pp 42-44.

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.

1.5 Beyond Recognition: Emerging Facial Analytic Tasks

Facial recognition is a subset of a broader and growing category of automated face analysis technologies. As some facial recognition infrastructure can be reconfigured to accomplish some of these analytical tasks, this section briefly outlines emerging facial analytical capabilities and their potential application in the border control context.

Face analysis encompasses a growing range of inference-drawing capacities that extend beyond recognition. This can include attempts to algorithmically infer age, gender, race, health conditions, and behavioural traits based on facial characteristics or impressions.[247]

Emotion or affect detection is an emerging field of automated face analysis that is posited for inclusion in facial recognition-based surveillance systems. Despite wide-ranging consensus in the scientific community that the relationship between facial expressions and internal mental states is not measurable in a consistently objective manner, a number of face analytic researches and vendors are developing systems that claim to provide insight into internal mental states based on external facial expression.[248] In a border control context, this category of facial analytics would seek to identify 'malintent' – the intention to commit a terrorist act or crime – in travellers.[249]

A related algorithmic process that increasingly seeks to leverage facial detection infrastructure is lie detection. A number of European states are currently piloting a system called IBorderCtrl, which analyzes 'micro gestures', including facial expressions, of travellers as they respond to questions at automated border control kiosks in order to algorithmically determine whether they are lying or not.[250] Both Canada and the United States have tested a similar lie-detection program to assess whether it could help border control officials determine whether an individual is travelling with ulterior motives and should be subjected to enhanced questioning or denial of entry.[251]

---

[247] Joy Buolamwini, Testimony before United States House Committee on Oversight and Government Reform, May 22, 2019, *In Re Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*, pp 5-7.

[248] Meredith Whittaker, Kate Crawford, Roel Dobbe, et al, AI Now Report 2018, December 2018, pp 14-15; Jay Stanley, "The Dawn of Robot Surveillance: AI, Video Analytics and Privacy", (2019) *American Civil Liberties Union*, pp 38-39; Sarah Myers West, Meredith Whitaker & Kate Crawford, "Discriminating Systems: Gender, Race, and Power in AI", April 2019, *AI Now Institute*, pp 31-32.

[249] While there is no evidence of a border control agency piloting emotion-based facial analytics to date, border control agencies have sought to develop similar capabilities in the past: Jay Stanley, "The Dawn of Robot Surveillance: AI, Video Analytics and Privacy", (2019) *American Civil Liberties Union*, p 39.

[250] Ryan Gallagher, "We Tested Europe's New Lie Detector for Travelers – and Immediately Triggered a False Positive", July 26, 2019, *The Intercept*, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/; Amit Katwala, "The Race to Create a Perfect Lie Detector – and the Dangers of Succeeding", September 5, 2019, *The Guardian*, https://www.theguardian.com/technology/2019/sep/05/the-race-to-create-a-perfect-lie-detector-and-the-dangers-of-succeeding. See also: https://www.iborderctrl.eu/The-project.

[251] Jeff Daniels, "Lie-detecting Computer Kiosks Equipped with Artificial Intelligence Look Like the Future of Border Security", May 15, 2018, https://www.cnbc.com/2018/05/15/lie-detectors-with-artificial-intelligence-are-future-of-border-security.html. Note that, as of August 22, 2018, there was no testing of this lie-detecting capability in live border control locations. While the testing consisted of video and audio recordings, all the testing was internal and used 'fake data': (Email from Canada Border Services Agency, dated August 22, 2018, on record with author).

1.6 Covert Operation & Opaque Decision-Making

By its nature, facial recognition provides more opportunities for covert operation than other identification mechanisms, making it possible for facial recognition to occur without the knowledge and participation of impacted travellers. Algorithmic determinations are further characterized by opacity, posing accountability challenges for many automated decision-making systems.[252] The very concept of interpretability becomes difficult to articulate when attempts are made to explain how algorithmic systems reach determinations.[253] This can be problematic where sophisticated but opaque algorithms are used as the basis for identification in border control scenarios. Compounding this surreptitious capacity, government policy frequently seeks to shroud details regarding the operation of facial recognition systems in secrecy, withholding critical details such as bias and accuracy ratings.

Unlike some other biometrics such as fingerprinting and iris scans, enrollment in a facial recognition system can occur from a distance and without a traveller's knowledge or participation.[254] The United States Customs and Border Protection, for example, captures images of non-US travellers during encounters with the Department of Homeland Security and enrolls these images into its facial recognition database.[255] The greater speed and efficiency of this approach leads many border security agencies to favour 'capture at a distance' approaches at cost to transparency.[256] Even where travellers

---

[252] European Union, Article 29 Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679", WP251rev.01, last revised February 6, 2018, pp 25-26:

> The growth and complexity of machine-learning can make it challenging to understand how an automated decision-making process or profiling works. The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.

See also: International Conference of Data Protection & Privacy Commissioners, Declaration on Ethics and Data Protection in Artificial Intelligence, adopted at *40th International Conference of Data Protection and Privacy Commissioners*, October 23rd, 2018, Brussels, https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_en_0.pdf, Association for Computing Machinery, US Public Policy Council (USACM), Principles for Algorithmic Transparency and Accountability, adopted in *Statement on Algorithmic Transparency and Accountability*, January 12, 2017, https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf; The Royal Society, "Machine Learning: The Power and Promise of Computers that Learn by Example", April 2017, https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf?la=en-GB&hash=B4BA640A1B3EFB81CE4F79D70B6BC234, Section 6.2.

[253] For an attempt to articulate these interpretability challenges, see: Finale Doshi-Velez & Been Kim, "Towards a Rigorous Science of Interpretable Machine Learning", *arXiv: Machine Learning*, March 2, 2017, https://arxiv.org/pdf/1702.08608.pdf; Been Kim, "Interpretable Machine Learning: The Fuss, the Concrete and the Questions", *ICML 2017*, https://people.csail.mit.edu/beenkim/papers/BeenK_FinaleDV_ICML2017_tutorial.pdf.

[254] United States, Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 9: "…facial recognition poses a unique set of privacy issues. Facial images can be captured at a distance, covertly, and without consent. Further, facial images are ubiquitous, and whereas individuals may take measures to avoid fingerprint and iris collection, there are fewer ways to hide one's face."

[255] United States, Government Accountability Office, "Border Security", February 2017, GAO-17-170, https://www.gao.gov/assets/690/683036.pdf, p 17.

[256] United States, Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 11:

> Due to the large volume of travelers and border crossers, it would not be practical for CBP to use formally-generated frontal head-on facial images, such as are taken for a driver's license or passport. Rather, CBP is increasingly employing technologies that do not require subjects to present their face directly to the camera. Given this new focus, technology providers are continuing to refine their solutions to collect face images with minimal participation from the subject. While a more streamlined capture of facial images (rather than a "stop and look" approach) poses operational benefits to CBP, it also poses increased privacy risks since the individual may be unaware that their photo is being captured.

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, para 37:

are aware that they are being photographed, such as at an automated customs kiosk, it would not be self-evident that biometric processing has occurred. In Canada, for example, customs self-service kiosks introduced in 2013 photographed travellers and printed the resulting image on a 'customs receipt', which was later presented to a border control official for manual recognition.[257] Since 2017, these 'Automated Passport Control' kiosks were replaced with 'Primary Inspection Kiosks', which similarly photograph travellers and print a customs receipt that is submitted to border control officials however, prior to printing the receipt, the new kiosks also employ facial recognition to verify travellers' passports.[258] By contrast, there is no border process for manual comparison of iris or fingerprint scans, and as a result collection of these biometrics would solely be associated with automated recognition.

A propensity for government secrecy further undermines the transparency and legitimacy of facial recognition systems.[259] This secrecy is not uniform. Some government agencies have embraced transparency and periodically report public statistics regarding error rates and other factors,[260] while others do not. The United States Federal Bureau of Investigation, for example, was criticized by the Government Accountability Office for only reporting the detection rate of its facial recognition program and refusing to measure and report on the rate at which individuals were erroneously implicated.[261] United States Customs and Border Protection, by contrast, have made available error rates for facial recognition systems used at airports.[262]

The Canada Border Services Agency (CBSA) has taken a more stringent approach to shielding its facial recognition program from scrutiny, arguing that error rates implicate national security and cannot be publicly disclosed.[263] CBSA has also refused to publish its privacy impact assessments for some (but

> While the technology itself can be fairly simply explained, once implemented it can accurately be described as obscure and opaque. Facial recognition requires no participation or consent from individuals.

[257] Candice So, "Toronto Airport Launches Self-Service Passport Kiosks", December 9, 2013, *IT Business*, https://www.itbusiness.ca/news/toronto-airport-launches-self-serve-passport-kiosks/45463; Toronto Pearson Airport, "Automated Passport Clearance at Toronto Pearson", December 4, 2013, https://www.youtube.com/watch?v=RW8SPrYOtuc [Video].

[258] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html.

[259] See, generally: Christopher Parsons & Adam Molnar, "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports", (2017) 16 *CJLT* 143.

[260] For example, see: Markus Nuppeney, "Automated Border Control (EasyPASS): Monitoring the System Performance", *NIST: IFPC 2018*, November 27, 2018, https://nigos.nist.gov/ifpc2018/presentations/05_nuppeney_20181127_IFPC2018_EasyPASS_Nuppeney.pdf, outlining error rates in Germany's EasyPASS e-Gate facial recognition system.

[261] United States, Government Accountability Office, "Face Recognition Technology", *Testimony Before House of Representatives, Committee on Oversight and Reform*, GAO-19-579T, June 4, 2019, https://www.gao.gov/assets/700/699489.pdf, pp 14-15.

[262] United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568.

[263] 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.

not all) of its facial recognition systems, instead publishing sparse summaries that fail to address accuracy rates at all.[264] 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.[265] Any adoption of a facial recognition system must therefore be accompanied by mandatory periodic auditing and publication of statistics regarding population-wide false positive and negative rates, as well as error rates disaggregated by gender, race and country of origin.[266]

The opacity in which facial comparison decisions are made poses additional problems, undermining attempts to mitigate the inherent fallibilities of the technology.[267] Many border control systems inject manual oversight as a supplement to automated facial recognition, adopting a so-called 'human in the decision-making loop' approach. This can mitigate some errors, including some false negatives (if the automated system fails to match a traveller with any facial image despite the fact that the traveller is enrolled in the reference dataset) and some false positives (if the automated system mistakenly matches a traveller with an individual who is in a watch list). However, some studies have suggested that, over time, border officials develop high levels of trust in biometric systems, and that this level of trust becomes difficult for travellers to overcome.[268] Generally speaking, this deference to algorithmic decision-making is often linked to the opacity of that decision-making process—where human supervisors are unable to understand the basis for an algorithmic decision it becomes difficult to second guess

[264] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html. By contrast, other branches of the Canadian government have willingly published full privacy impact assessments that included statistics regarding the general accuracy of facial recognition systems being used in border control systems: Passport Canada, "Facial Recognition Application Project – Privacy Impact Assessment: Executive Summary", June 28, 2016, https://www.international.gc.ca/gac-amc/publications/atip-aiprp/assessments-evaluation/facial-faciale.aspx.

[265] Adam Vaughan, "UK Launched Passport Photo Checker it Knew Would Fail with Dark Skin", October 9, 2019, *NewScientist*, https://www.newscientist.com/article/2219284-uk-launched-passport-photo-checker-it-knew-would-fail-with-dark-skin/; Frank Pasquale, "The Black Box Society", (Boston: Harvard University Press, 2015); Cathy O'Neil, "Weapons of Math Destruction", (NY: Crown Publishers, 2016), p 28.

[266] 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, p 2.

[267] 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, para 37:

> While the technology itself can be fairly simply explained, once implemented it can accurately be described as obscure and opaque. ... The software algorithms are complex mathematical formulas that most people cannot understand. Even if an individual were to go through the software code line by line it would be impossible to trace the connection between the code a person inspected and the code being executed by the software program.

[268] European Union, Fundamental Rights Agency, "Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security", May 2017, p 78, with respect to fingerprint systems:

> There is high trust in information provided in an IT-system, according to public officials, lawyers and experts interviewed by FRA. ... In case of inaccurate alphanumerical data, at least some obvious mistakes, such as a misspelt name, can be rebutted by showing for instance personal data in documents and comparing additional data. This is generally not possible for biometric identifiers. ... A police officer interviewed in Germany for FRA's biometrics project stated that there is a tendency among the staff of the competent authorities to assume that inaccuracies and mismatches are the result of right holders providing false information at some point. Partly for this reason, authorities tend not to take much into account the information provided by the migrant, unless they can verify it through entries in IT-systems or document evidence.

See also: Itiel Dror & Kasey Wertheim, "Quantified Assessment of AFIS Contextual Information on Accuracy and Reliability of Subsequent Examiner Conclusions", *National Institute of Justice*, July 2011 (automated fingerprint matches presented in top ranks can undermine manual fingerprint matching).

while its mathematical operation is perceived as authoritative.[269] The 'scientific mystique' in which automated determinations are reached creates a powerful cognitive bias in favour of those outcomes.[270]

The ability to instill some form of rigorous manual vetting of facial recognition matching algorithms is critical. Even including a human in the decision-making loop, however, is not sufficient to fully dispel the errors and racial biases inherent in facial recognition technologies. Indeed, the CBSA relies on manual vetting of determinations made by its automated customs and immigration PIKs, yet one analysis found that this human supervision did not alleviate travellers from specific countries of origin from being disproportionately referred to secondary screening.[271]

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.

[269] Safiya Umoja Noble, "Algorithms of Oppression", (NY: New York University Press, 2018), p 37, describes this deference in relation to algorithmic decision-making in the context of search engines:

> … renderings are delivered to users through a set of steps (algorithms) implemented by programming code and then naturalized as "objective." One of the reasons this is seen as a neutral process is because algorithmic, scientific and mathematical solutions are evaluated through procedural and mechanistic practices …

[270] Courts have recognized the disproportionate prejudicial impact that the "mystique of science" can have on decision-makers in other contexts as well: *R v Béland*, [1987] 2 SCR 398, para 64, per La Forest, J, concurring, in ruling polygraph tests inadmissible in jury trials, warned of the "human fallibility in assessing the proper weight to be given to evidence cloaked under the mystique of science." This can be the case even where individual decision-makers are aware of the inherent limitations of a tool. See also: Jason Millar, "Five Ways a COVID-19 Contact-Tracing App Could Make Things Worse", *Policy Options*, April 15, 2020, https://policyoptions.irpp.org/magazines/april-2020/five-ways-a-covid-19-contact-tracing-app-could-make-things-worse/; Cosima Gretton, "The Dangers of AI in Health Care: Risk Homeostasis and Automation Bias", *Towards Data Science*, June 24, 2017, https://towardsdatascience.com/the-dangers-of-ai-in-health-care-risk-homeostasis-and-automation-bias-148477a9080f?gi=e7b5eb341e4a.

[271] 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, specifically , human supervision did little to mitigate PIK selective immigration referrals in higher proportion for travellers from Iran or Jamaica.

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.

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.

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.

2.1 Core Functionality: Verification, Identification & Screening

The particular functionality driving adoption of a given facial recognition border control system will impact the type of facial recognition being used as well as its scope of impact. Specifically, as described in more detail in Section 1.2.2, above, facial recognition algorithms can have different levels of intrusiveness and different functionality depending on whether a 1:1 or 1:N comparison method is being employed. This section provides specific examples where 1:1 and 1:N facial recognition systems are being used for border control purposes and distills some insights regarding the capabilities, shortcomings and impacts of each.

2.1.1 Travel Document Verification [1:1 Facial Comparison]

Perhaps the most widely used border control facial recognition technique is to verify that an individual as the owner of the passport they present at a border control juncture. This will typically involve photographing a traveller at the border control location and comparing the face in that photograph to a single reference image already associated with the traveller's physical passport. This facial image is often encoded on the traveller's physical passport, although in some instances the facial image might be retrieved from a remote database by querying a unique identifier, such as a passport number. One-to-one (1:1) facial recognition is best suited for validating identity rather than for identifying individuals, as a 1:1 system must be provided with some form of independent identification so that it can know which single facial image to use as a reference for comparison.[272] This can be a name, a passport number, or the facial image itself.

Some states have adopted facial recognition mechanisms designed to verify travellers against their passports. As described in Section 1.1.1, above, the International Civil Aviation Organization (ICAO) requires the inclusion of a digital facial image to be encoded on a passive contactless Radio Frequency Identification (RFID)-enabled memory chip on compliant passports.[273] ICAO compliant passports will also include machine-readable elements with information such as the traveller's name, nationality, date of birth and passport number. Many states have adopted this requirement, including Canada, which began issuing biometric passports with ICAO compliant facial images in 2013. [274]

[272] For a description of 1:1 and 1:N comparison, see Section 1.2.2, at p 26, above.

[273] ICAO Doc 9303, "Machine Readable Travel Documents", 7th Edition, 2015, Part 3, https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf. Doc 9303 requires two images, one of which is specifically designated for the purpose of facilitating biometric recognition processes.

[274] See description in Section 1.1.1, at p 6, above. See also: Passport Canada, "International Comparison of Passport-Issuing Authorities", March 2012, https://www.canada.ca/content/dam/ircc/migration/ircc/english/department/consultations/passport/pdf/2012-03-compare-eng.pdf, p 14:

> All of the Five Nations countries except Canada fully implemented the ePassport between 2005 and 2007. One major incentive for this change was a new requirement adopted in 2006 by the United States, requiring Visa-Waiver Program countries to adopt the ePassport if they wished to continue enjoying visa-free access to the United States. Canada is in a privileged position, as it is currently exempt from this program. This means that Canadians may visit the United States for tourism without a visa, even without holding an ePassport. Canada has been issuing diplomatic and special passports as ePassports since 2009, as a pilot project. The full national implementation of the Canadian ePassport is scheduled to be complete in 2013.

Facial verification can facilitate automated processing of passengers. Beginning in 2017, Canada expanded its use of these biometric enabled passports by installing Primary Inspection Kiosks (PIKs) with advanced tools for automated border control processing at major Canadian air ports of entry.[275] These advanced tools include a mobile application integration that allows travellers to complete customs declaration forms on their mobile devices and transmit this data to a Kiosk upon arrival in Canada.[276] The PIK automatically processes the traveller's customs information, and then relies on facial recognition to verify their passport.[277] The PIK prompts Travellers to pose for a photograph, extracts the ICAO compliant image encoded on the traveller's passport, and compares the two images.[278] The facial recognition process employed by these PIKs currently employs 1:1 comparison. The facial image captured by the kiosks from individual travellers is only compared to the digital image contained on the passport for the purpose of verifying that the document belongs to the traveller who produces it.[279]

Facial passport verification can also be used as an automated means of enrolling travellers into more expansive facial recognition systems by providing states with a pre-vetted and high quality facial image associated with a specific identity document. Australia's border control biometric system, for example, largely operates on a 1:N identification basis but retains a 1:1 passport verification capability (detailed in the following section) as a means of enrolling new foreign travellers. Travellers carrying ICAO-compliant passports can verify their identities automatically and, once verified, become enrolled in the Australian 1:N identification system. While the enrollment process remains voluntary, it is illustrative of how foreign states can repurpose biometric capabilities adopted under more constrained presumptions.

Government of Canada, "History of Passports", last modified April 10, 2014, https://www.canada.ca/en/immigration-refugees-citizenship/services/canadians/celebrate-being-canadian/teachers-corner/history-passports.html: "On July 1, 2013, Passport Canada started issuing a new, even more secure electronic passport, known as the ePassport. This new-generation passport has an electronic chip embedded in the book to provide greater protection against fraud and tampering, and contribute to domestic and international travel security."

[275] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html.

[276] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html.

[277] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html.

[278] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html.

[279] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html. Australia previously operated SmartGates that operated on similar principles.

> Currently, all travellers (citizens and non-citizens) are required to present evidence of identity, such as a passport, to a clearance officer or authorised immigration clearance system when entering or leaving Australia at an airport or seaport. The automated immigration clearance system (SmartGate) allows arriving and departing eligible travellers to self-process through immigration clearance by presenting their passport to confirm their identity. The SmartGate takes a photo of the traveller for comparison against the image in the traveller's passport.

Migration Amendment (VISA Revalidation and Other Measures) Bill 2016, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5751_ems_2fb75e14-e450-4d1c-9c16-e0c27f0913b0%22, para 208. These are currently being superseded by a 1:N automated facial recognition system, described in the next section.

Facial verification can also operate as a means of linking physical and digital identities across a range of border control encounters. Canada is currently piloting an expansive World Economic Forum proposal (described in greater detail in Box 12) which will create a comprehensive digital identity and trust rating system that can be relied upon by various border entities to assess participating travellers for customs control and security assessment purposes.[280] Facial recognition (1:1) is integral to the proposal, verifying travellers' passport information upon initial enrollment into the program and linking travellers to their digital profiles, which contain facial templates. The digital profile itself contains passport information and a 'trust' assessment based on the number of times a traveller's digital identity has been 'attested' to by various border control entities.[281] In order to receive these attestations, travellers are prompted to populate their digital profile with additional—education credentials, bank statements, health information (e.g. vaccinations), trip itineraries, and criminal history—and to volunteer this information to border officials on request.[282] Facial recognition permits the automation of KTDI profile use, such as by allowing automated border control infrastructure to reliably identify travellers when dropping off baggage, exiting security areas or boarding a flight.[283] The KTDI proposal is intended to be user-centric, permitting travellers to decide on a case-by-case basis whether they will share their biometric and other profile data with border control and other entities.[284] It is not clear how states would be prevented from compelling disclosure at border control or other

[280] The proposal is described in detail in Box 12, p 95, below. 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; Canada, Netherlands & World Economic Forum, "Known Traveller Digital Identity: Pilot Project", June 18, 2019; 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.

[281] 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, pp 14-15:

> The Known Traveller Digital Identity concept is designed to enable the voluntary sharing of information whereby the individual builds up trust in their digital identity. To build a trusted "Known Traveller" status, travellers need attestations – authenticated claims as declared by a trusted entity – to be added to their Known Traveller Digital Identity each time a trusted entity – such as a post office or a governmental or educational institution – verifies a claim. In this concept, these attestations are the backbone of trust and the basis of reputation and, ultimately, how security decisions can be made. Examples of attestations are proof of citizenship in country X, an educational degree from college Y and proof of vaccination for viral disease Z. In the future, country A might authorize a traveller to enter the nation based on a previous risk assessment and the resulting attestation by country B.
>
> Importantly, as it is currently proposed, travellers will consolidate attestations into a Known Traveller profile and increasingly strengthen their claim to compliance, trust and legitimacy as a traveller. People continue to build the Known Traveller status by acquiring more attestations, thereby contributing to a more secure and seamless traveller journey for all stakeholders.

[282] 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, Figure 5 and p 17:

> The Known Traveller Digital Identity concept provides the potential for law-enforcement agencies to request a structured packet of data from a traveller before travel. The table below shows the sections of data that, if integrated into a passenger's Known Traveller profile, could help facilitate border security screening. As in the Guidelines on Advance Passenger Information, sections A–C represent the maximum data fields recommended that countries request from carriers through Advance Passenger Information systems. Section D represents additional information that a passenger could integrate into their Known Traveller profile to improve their profile credibility and provide authorities with more information than the maximum data collected currently through Advance Passenger Information systems.

[283] 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, Table 4, "Arrival at Airport".

[284] 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, pp 14-15 and 17:

> The concept is based on the idea that an individual is in control of providing specific identity information (e.g. biometric, biographic and travel history) to governmental and private-sector players along the journey, such as border control agencies, car rentals, hotels and airlines, for risk profiling, verification and access (Figure 4). The traveler can select which information is shared for a specific time according to the authority or private entity's requirements to access the services. The identity of the traveller is authenticated through biometric verification and protected by distributed ledger technology and cryptography.

settings once the capability is developed.[285] If established in the border context, the KTDI is envisioned as having far broader application as a general-purpose national identity capable of reliably linking rich digital profiles to real-world identities.[286]

Where 1:1 facial recognition is limited to its most basic replication of passport verification tasks currently carried out manually, it can be problematic to the degree it injects additional inaccuracy in the form of false positives and racial discrimination and generally normalizes facial recognition as a means of interaction with the government. The basic task of automating document verification through the adoption of 1:1 facial verification can also increase the frequency in which travellers are called upon to self-identify by removing what are otherwise pragmatic barriers associated with the inconvenience that arises from manual document verification. In other contexts, some border control facial verification proposals are envisioned as a means of creating a universal digital identity that reliably links individuals to sophisticated digital profiles in day to day conduct. Such a vision has far-reaching potential implications for privacy and identity management, at the border and well beyond. Finally, 1:1 facial verification is increasingly being used as a means for automated border control mechanisms to interact with travellers in the absence of any human intervention. This, in turn, allows automated border control decision-making to be implemented with much greater frequency and less manual interaction, raising challenges related to privacy, accuracy and discrimination, as described in further detail in section 2.2, below.

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.

2.1.2 Traveller Identification & List-based Screening [1:N Facial Comparison]

Some states are adopting facial recognition mechanisms that allow for more than verification. Facial verification requires an individual to self-identify by providing a name or other identification

[285] *R v Fearon*, 2014 SCC 77; British Columbia Civil Liberties Association, Electronic Device Privacy Handbook, July 2018, https://bccla.org/wp-content/uploads/2018/10/Electronic-Devices-Privacy-Handbook-BCCLA_2.0.pdf; Joseph Cox, "China is Forcing Tourists to Install Text-Stealing Malware at its Border", July 2, 2019, *VICE: Motherboard*, https://www.vice.com/en_us/article/7xgame/at-chinese-border-tourists-forced-to-install-a-text-stealing-piece-of-malware.

[286] 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 35 and 37.

number, so that the facial recognition system can know which reference facial image to compare the traveller's photographed face against. By contrast, 1:N systems are able to pick an individual's face out of large reference datasets comprising many (often millions of) facial images. Once a match has occurred, the system can return any identification information (name, passport number, etc) previously associated with the reference facial image. Whereas 1:1 systems can verify whether a specific traveller is who they claim to be, 1:N systems can therefore identify individuals on the basis of their live image alone. Comparison systems of the 1:N variety are also capable of automating screening processes by matching travellers' photographed facial images against those stored on specific prepared lists.

At times, 1:N systems are used to verify, rather than identify, individuals. United States Customs and Border Protection (CBP), for example, operates a Traveler Verification Service (TVS), an automated 1:N facial recognition service initially generated to biometrically confirm the identities of travellers exiting the United States.[287] While CBP operates the TV Service, a number of entities are able to submit probe images of travellers in order to verify their identity. To biometrically verify that departing travellers are who they claim, airlines use cameras at airport gates to capture facial images of travellers as they board their flights.[288] The resulting facial images are submitted to TVS, which compares the images against a pre-existing reference dataset comprising facial images and identification data of travellers expected to be departing the United States. For international flights, a manifest of travellers scheduled for pending outbound international flights is prepared based on United States flight information (Advanced Passenger Information System (APIS)).[289] A similar gallery is generated at land ports of entry, comprised of 'frequent travellers' that CBP identifies as crossing often at a particular land port of entry.[290] These galleries of travellers are then populated with facial images that have been previously acquired and vetted

[287] These biometric capabilities were initially developed by CBP as an exit confirmation program designed to confirm departure of individuals from foreign jurisdictions in order to prevent overstays. See: Department of Homeland Security, "Comprehensive Biometric Entry/Exit Plan: Fiscal Year 2016 Report to Congress", April 20, 2016, pp 3-4. See also: United States, Transportation Security Administration, "TSA Biometric Roadmap: For Aviation Security & The Passenger Experience", September 2018, p10.

[288] United States, Department of Homeland Security, Privacy Impact Assessment Update: Traveler Verification Service, DHS/CBP/PIA-030(d), September 25, 2017, pp 3-4:

> "…the TVS uses CBP's biographic APIS manifest data16 and existing photographs of all travelers boarding international flights to confirm the identity of the traveler, create an exit record, and biometrically confirm the exit of in-scope non-U.S. citizens.
>
> As boarding begins, each international traveler approaches the departure gate to present a boarding pass and stands for a photo in front of a camera, which is owned either by CBP or by a partner airline or airport authority. In either case, the camera securely transmits usable images to CBP's cloud-based TVS facial matching service. The matching service generates a template from the departure image and uses that template to search the historical photo templates for all travelers on that particular international flight manifest. The TVS returns faces that best match the reference face, thus verifying the identities of individual travelers. If a match is found, the traveler proceeds to the aircraft, and the TVS returns the positive results, along with the respective unique identifier … CBP creates a record of the traveler's departure in APIS, which updates the traveler record from "reported" to "confirmed."

[289] United States, Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, pp 4-5.

[290] Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 5: "If CBP has access to advance passenger manifest information, the CBP will build galleries of photographs based on upcoming flight or vessel arrivals or departures. If CBP does not have access to advance passenger information, such as for pedestrians or privately owned vehicles at land ports of entry, CBP will build galleries using photographs of "frequent" crossers for that specific port of entry, taken at that specific port of entry, that become part of a localized photographic gallery."

through a variety of means, including photographs captured by CBP during entry inspections, photographs from previous encounters between a given traveller and the Department of Homeland Security, and photographs initially acquired as part of the US passport or visa application process and provided by the Department of State.[291]

It is envisioned that, once fully implemented, TVS will replace the need for presenting travel documents, and even boarding passes, at some boarder control checkpoints, such as when boarding an international flight.[292] In implementing TVS, CBP has also moved towards a 'capture from a distance' approach where travellers are not prompted to stop at a kiosk and stare into a camera, but are photographed remotely.[293] As a result, travellers are less likely to be aware that they are participating in biometric identification,[294] and image capture quality is likely to be inferior. Capture from a distance can only be accomplished using 1:N recognition, as it offers limited opportunity for travellers to provide identity information for verification.

Australia is in the process of transitioning its existing facial recognition systems from a 1:1 to a 1:N modality as part of a larger initiative to integrate facial recognition into a range of border controls.[295] The objective is to move towards a border control process that is fully contactless and no longer dependent on physical documents.[296] While travellers are still required to carry physical passports, the *primary* border control mechanism is biometric identification—your face will be your new passport.[297] Under this emerging system, travellers' faces are photographed as they

[291] Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 4 and footnote 16: "For all biometric matching deployments, the TVS relies on biometric templates generated from pre-existing photographs that CBP already maintains, known as a "gallery." These images may include photographs captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters. ... U.S. passport and visa photos are available via the Department of State's Consular Consolidated System. *See* Privacy Impact Assessment: Consular Consolidated Database. Other photos may include those from DHS apprehensions or enforcement actions, previous border crossings, and immigration records."

[292] United States, Customs and Border Protection, "Traveler Verification Service for Simplified Travel", CBP Publication #0726-0518, August 2018, https://www.cbp.gov/sites/default/files/assets/documents/2018-Aug/Traveler_Verification_Service_For_Simplified_Travel3.pdf: "Airports and airlines will be able to verify traveler identity using the facial biometric matching service throughout the travel process by simply capturing a live traveler photo. The captured photo is compared against the cloud-based matching service's photo gallery in real-time. The service responds with identity verification match results, eliminating manual processing such as document checks or the use of boarding passes."

[293] Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 11.

[294] Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, pp 11 and 20.

[295] Initially proposed in *Migration Amendment (Visa Revalidation and Other Measures) Bill 2016*, Schedule 3 – Immigration Clearance, https://www.legislation.gov.au/Details/C2016B00172, but ultimately adopted through regulation in: *Migration Amendment (Seamless Traveller) Regulations 2018*, https://www.legislation.gov.au/Details/F2018L01538.

[296] *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5751_ems_2fb75e14-e450-4d1c-9c16-e0c27f0913b0%22, paras 208-210:

> Currently, all travellers (citizens and non-citizens) are required to present evidence of identity, such as a passport, to a clearance officer or authorised immigration clearance system when entering or leaving Australia at an airport or seaport. The automated immigration clearance system (SmartGate) allows arriving and departing eligible travellers to self-process through immigration clearance by presenting their passport to confirm their identity. The SmartGate takes a photo of the traveller for comparison against the image in the traveller's passport. … Contactless technology will remove the need for eligible travellers to present a passport to verify their identity in automated immigration clearance. … The live facial image of the traveller at the SmartGate will be matched against an image previously verified as the unique identifier associated with that identity.

[297] *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text, Attachment C, p 9: "This supports the digital transformation agenda by allowing reliance on electronic information already collected and removing the need to present a physical document, where possible. This is colloquially referred to as 'contactless processing' as little contact is made with clearance authorities other than presenting to a SmartGate for the purpose of having a facial image taken and compared with existing data."; *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory

approach cameras mounted on automated gates called 'SmartGates'. These photographs will then be compared against a large set of previously acquired reference images.[298] As with CBP's 'capture from a distance' proposal, a contactless system of this nature requires a 1:N mode of operation as there is no opportunity for travellers to provide the border control system additional information that would identify a single historical reference image to use as a base of comparison.[299] By contrast, automated gates that are reliant on 1:1 verification require individuals to physically interact with the gate (by, for example, swiping a biometric enabled passport) before any facial recognition processing can occur.

The new Australian system relies on a large reference dataset, consisting of most Australian citizens and many non-Australian travellers and comprising two separate databases. One of these databases is operated by the Australian Department of Foreign Affairs and Trade (DFAT) and includes biometric facial images developed through its passport control function.[300] Australians are enrolled into this database as part of the passport application process, and the database operates under a policy agreement and technical overlay that allows border control SmartGates to query its store of facial images for identification purposes.[301]

Travellers who are not present in this DFAT database are enrolled in a second database, operated by the Australian Department of Home Affairs (DHA) the first time they attempt to self-process through a SmartGate.[302] The SmartGate will first attempt a contact-less identification of the traveller, but will fail to match the travellers face as no facial image will be associated with a valid travel document in the reference dataset. Following such a failure to match, the traveller will be directed by the SmartGate to facially verify their physical machine-readable passport against the ICAO compliant image it contains

---

Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text, Attachment B, p 2: "This is colloquially referred to as 'Contactless Processing' as little contact is made with clearance authorities other than presenting to a SmartGate for the purpose of having a facial image taken and compared with existing data."

[298] *Migration Amendment (Seamless Traveller) Regulations 2018*, https://www.legislation.gov.au/Details/F2018L01538.

[299] *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text, Attachment B, p 2: "This is colloquially referred to as 'Contactless Processing' as little contact is made with clearance authorities other than presenting to a SmartGate for the purpose of having a facial image taken and compared with existing data."

[300] *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text, p 1: "For Australian citizens, these details may be obtained either the first time a person travels on that passport or they may also be able to be obtained from the Department of Foreign Affairs and Trade."

[301] *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5751_ems_2fb75e14-e450-4d1c-9c16-e0c27f0913b0%22, para 212: "The Australian Passport Office database which holds images collected as part of the Australian passport identity verification process. The Department has arrangements in place for access to this database which is currently used for border clearance. Access to images of Australian citizens supports Contactless Automated Immigration Clearance."

[302] Note that this database was initially slated to be operated by the Department of Immigration and Border Protection (DIBP), until that department was subsumed into the newly created Department of Homeland Affairs in late 2017: Commonwealth of Australia, Department of Homeland Affairs, "Our History", last updated November 11, 2018, https://www.homeaffairs.gov.au/about-us/who-we-are/our-history: "On 20 December 2017 the Department of Home Affairs was established as a part of the Home Affairs Portfolio. The Department of Home Affairs continues to deliver immigration and customs border policy functions previously delivered by the Department of Immigration and Border Protection." As a result, some documentation refers to this dataset as a DIBP database while other documentation refers to it as a DHA database.

(a 1:1 comparison).[303] If successful, the traveller's facial image and passport details can be enrolled into DHA's reference database for contactless 1:N identification in future entry/exit attempts.[304] First time travellers that are not carrying biometrically-enabled passports will need to be processed manually by a clearance officer, and an accompanying manual enrollment process might be established by Australian DHA as well.[305]

While it is clear that travellers will be notified regarding the general operation of these SmartGates through on-site signage and pamphlets,[306] it is not clear whether individuals that rely on physical facial verification or manual passport processing will be notified that they are being enrolled in a centralized biometric identification system, or whether they will be given an opportunity to refuse enrollment.

Some other 1:N implementations will also seek to screen individual travellers against watch lists that are biometric enabled, and contain reference facial samples of individuals who have been flagged as flight or other security risks, or for other purposes.[307] This screening process is versatile—a range of consequences can result if a given traveller matches (or does not match) against the screening list. A non-match might indicate that a traveller is not qualified to enter an airline's preferred traveller lounge, a match might indicate that a traveller is not permitted to fly. The consequence of matching/not matching will be dependent on the attributes assigned to the list.

---

[303] *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text, Attachment C, p 9: "If a person's identity or visa status cannot be ascertained by comparing the facial image with existing data, then the person may be required to present their physical passport to the SmartGate."

[304] *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5751_ems_2fb75e14-e450-4d1c-9c16-e0c27f0913b0%22, p 57: "Images provided by the traveller (both citizens and non-citizens) to the SmartGate are stored in departmental systems. A document based identity verification process occurs at the time the traveller self-processes through the SmartGate. This verified image and others collected during subsequent travel, become the images used by the Department to confirm identity on future travel."

[305] *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text, Attachment C, pp 9-10:

> If the person's identity or visa status ... cannot be ascertained using the authorised system, or there is another concern, then a clearance officer may require the passport to be presented to a clearance officer under subsection 166(2). ... There is no longer a reference to a person being registered for an automated identification processing system. While this registration process has not changed, it is considered unnecessary to refer to it in the regulation because administrative practices guide registered persons to use the SmartGate, while unregistered persons are guided toward manual processing. If an unregistered person attempted to use the SmartGate, they would be referred for manual processing.

See also: *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5751_ems_2fb75e14-e450-4d1c-9c16-e0c27f0913b0%22, p 57:

> An added benefit of this technology is that as contactless SmartGates will not be reliant on the presentation of a passport, arrivals SmartGates will also be able to process travellers who do not hold an ePassport. ... A greater number of travellers will be able to selfprocess through the Contactless automated immigration clearance system. The current arrivals SmartGates can process travellers only if they present an ePassport. As the Contactless Automated Immigration Clearance process is not reliant on the presentation of a passport, it is expected that most arriving travellers will use contactless SmartGates.

[306] *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text, Attachment B, p 3: "Travellers are notified about the collection of personal information by the SmartGates in advance. This notification occurs through dedicated signage which contains the Department of Home Affairs' (the Department's) privacy statement, which, amongst other things, informs individuals why their personal information is being collected and how it may be used by the Department. Further information is available in pamphlets at the airport and on the Departmental website."

[307] International Civil Aviation Organization, ICAO TRIP Guide on Evidence of Identity, *ICAO Security and Facilitation*, ver 5.3, May 2018, Section 2.8.3:

> A record on the watchlist may contain only biometric data for a wanted individual or may also have identity information, depending on what is known. Everyone who passes the screening process provides a biometric sample, which is checked for matches against the watch-list. The key feature of a watch-list is that people are not, on-the-whole, identified; they will only be identified if they appear on the list.

The Canada Border Services Agency (CBSA) has piloted a program that would use live camera feeds to screen all travellers against a facial recognition database comprising thousands of foreign nationals who were historically deemed inadmissible for entry into Canada.[308] The live camera feeds would be initially confined to CBSA-controlled areas. If the facial recognition system identifies a traveller that is sufficiently similar to an image in its database, a CBSA officer is informed and, if the match is manually confirmed, the traveller in question is referred to secondary inspection.[309] CBSA piloted the program in 2016, but has not published its results or any further plans to institute the monitoring program in full.

The United Kingdom has announced that it is piloting an automated facial recognition system that would attempt to match travellers' facial images against biometrically enabled criminal watch lists.[310] A number of United Kingdom policing forces currently operate facial recognition-enabled watch lists containing wanted or suspected criminals and other persons of interest.[311] The United Kingdom Home Office proposed to test similar lists at border control settings in order to inform border control decisions.[312] Historical mechanisms for screening persons of interest at United Kingdom border control settings have been manual rather than biometrically-enabled,[313] and have suffered from an overreliance on the 'quantity' of underlying data rather than on its quality, which lead to outdated entries and an unreliable system.[314] Simply adding a biometric recognition capability to these mechanisms could act to exacerbate existing data quality challenges.

Brazil uses a 1:N mechanism to screen for travellers deemed to be 'high risk'. In 2016, for example, Brazil installed high resolution cameras pointing at customs declaration lines in 14 major international

---

[308] Canada Border Services Agency, "Faces on the Move: Multi-Camera Screening—Privacy Impact Assessment", Executive Summary, last modified July 22, 2016, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/fotm-eng.html.

[309] Canada Border Services Agency, "Faces on the Move: Multi-Camera Screening—Privacy Impact Assessment", Executive Summary, last modified July 22, 2016, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/fotm-eng.html.

[310] United Kingdom, Home Office, "Biometrics Strategy: Better Public Services Maintaining Public Trust", June 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf, para 35; *R (Bridges) v Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin), paras 14-16, rev'd [2020] EWCA Civ 1058.

[311] United Kingdom, Information Commissioner's Office, "ICO Investigation into How the Police Use Facial Recognition Technology in Public Places", October 31, 2019, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf, pp 13-18.

[312] United Kingdom, Home Office, "Biometrics Strategy: Better Public Services Maintaining Public Trust", June 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf, para 35; *R (Bridges) v Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin), paras 14-16, rev'd [2020] EWCA Civ 1058.

[313] United Kingdom, National Audit Office, "E-Borders and Successor Programmes", December 7, 2015, paras 1.20-1.24; United Kingdom, National Audit Office, "The UK Border: Issues and Challenges for Government's Management of the Border in light of the UK's Planned Departure from the European Union", October 20, 2017, p 27.

[314] United Kingdom, National Audit Office, "E-Borders and Successor Programmes", December 7, 2015, paras 3.17-3.20. Specific challenges relating to the UK Warnings Index in its use for border control purposes include (references omitted):

> For example, our 2013 Border Force report found that out-of-date information stored on the warnings index system was delaying processing of passengers at arrival as officers sometimes need to leave passport control to double-check entries. ... In general, though, before 2013 the e-borders programmes and its successors focused on the quantity of advance passport data the Department was collecting and did not consider the quality of the data. ... Although the Department measures the outputs of new capabilities, such as the number of arrests and quantity of seizures, it does not measure the effectiveness of the new capabilities. For example, it could not provide us with information on how many people would have been arrested without new capabilities, the impact on arrest numbers of the growth in passenger volumes, and how many people were not arrested that should have been.

airports.[315] These ceiling-mounted cameras record facial samples from individuals as they walk past, extract facial samples, and compare these to a pre-populated dataset of reference facial samples associated with individuals who have been flagged on the basis of pre-arrival risk assessments designed to identify travellers who should be subjected to enhanced customs screening.[316] A collaboration between customs officials, law enforcement and Agencia Brasileira de Inteligencia (ABIN, the Brazilian intelligence agency) generates a second reference dataset comprised of the facial samples of individuals targeted through additional risk assessments as potential drug traffickers, security threats, or otherwise suspect.[317] Note that this process merges two layers of algorithmic assessment in a manner that compounds their respective false positive rates.

Australia has announced the use of facial recognition-enabled watch lists at international ports of entry. The Enterprise Biometric Identification Services (EBIS) system will "consolidat[e] biometrics collected through visa and detention programs with biometric data collected at the border", allowing Australia's automated SmartGates to screen travellers seeking to enter the country against criminal and terrorist biometric watch lists.[318]

National and international counter terrorism border control screening lists continue to rely primarily on alpha numeric querying at the time of this writing, while international security bodies have stopped short of adding a biometric requirement to watch list mechanisms specifically.[319] This is perhaps understandable. Watch lists such as the No Fly List embody several features that render the adoption of facial verification particularly inapt. This includes the serious consequences that can result from a false positive, and the historic immutability of such lists—an immutability that is exacerbated by the use of biometrics.[320] Despite these challenges, however, the ICAO believes that states are in an advanced level of readiness to implement biometrically-enabled watch lists, and believes that such lists should become an international obligation in the future.[321] The ICAO further points out that most

[315] Felipe Mendes Moraes, Deputy Chief, Brazilian Federal Revenue Service Customs Office, Customs Special Control Division, "Improving Security and Facilitation Through Collaboration", (2017) 12(1) *ICAO TRIP Magazine* 16, https://www.icao.int/publications/journalsreports/2017/TRIP_Vol12_No1.pdf, p 18.

[316] Felipe Mendes Moraes, Deputy Chief, Brazilian Federal Revenue Service Customs Office, Customs Special Control Division, "Improving Security and Facilitation Through Collaboration", (2017) 12(1) *ICAO TRIP Magazine* 16, https://www.icao.int/publications/journalsreports/2017/TRIP_Vol12_No1.pdf, pp 18-19.

[317] Felipe Mendes Moraes, Deputy Chief, Brazilian Federal Revenue Service Customs Office, Customs Special Control Division, "Improving Security and Facilitation Through Collaboration", (2017) 12(1) *ICAO TRIP Magazine* 16, https://www.icao.int/publications/journalsreports/2017/TRIP_Vol12_No1.pdf, pp 18-19.

[318] The Honourable Alex Hawke, Assistant Minister for Home Affairs, "Enormous boost to Australia's biometric capability", *media release*, March 19, 2018, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/5855662/upload_binary/5855662.pdf;fileType=application%2Fpdf#search=%22media/pressrel/5855662%22; Justin Hendry, 'Unisys to provide Australia's new biometrics travel platform', *iTnews*, March 19, 2018, https://www.itnews.com.au/news/unisys-to-provide-australias-new-biometrics-travel-platform-487293.

[319] United Nations, Security Council, Resolution 2396, paras 13, 15, 48 and 50. Note that while this resolution advocates the long-term adoption of effective biometric identification in general as a counter-terror tool, it does not require biometric capabilities in the context of watchlists specifically.

[320] For one example, see: CBC Radio: As It Happens, "Why This 4-Year-Old Girl's Mom is Demanding Canada Make Changes to its No-Fly List", *CBC Radio*, November 6, 2017, https://www.cbc.ca/radio/asithappens/as-it-happens-monday-edition-1.4389370/why-this-4-year-old-girl-s-mom-is-demanding-canada-make-changes-to-its-no-fly-list-1.4389376; CBC Radio: As It Happens, "Getting Off a No-Fly List: The Never-Ending Saga", *CBC Radio*, January 6, 2016, https://www.cbc.ca/radio/asithappens/as-it-happens-wednesday-edition-1.3391862/getting-off-a-no-fly-list-the-never-ending-saga-1.3391868; Lex Gill, "The No-Fly List and Bill C-59", *Canadian Civil Liberties Association*, September 12, 2017, https://ccla.org/no-fly-list-bill-c-59/.

[321] ICAO TRIP, Guide on Border Control Management, Part 2: Assessment Tool, *ICAO Security and Facilitation*, Ver 1, 2018,

watch-lists already include facial images of sufficient quality that they could be repurposed for biometric screening without difficulty.[322]

Facial recognition operating in a 1:N mode is inherently more intrusive than facial verification conducting 1:1 comparison. In terms of functionality, 1:N recognition can be implemented in a manner that effectively replicates the same 'task' as facial verification—confirming that a known traveller is who they claim to be. Even in these contexts, however, a 1:N approach is more intrusive as it requires comparison between the probe image and *all* facial images and profiles in a reference dataset.[323] Often this will involve using the personal information of millions in order to determine whether the traveller is who they claim to be and as such is an intrusive search. In addition, even when used to replicate facial verification functionality, a 1:N system poses an insidious threat to anonymity because it is capable of identifying unknown individuals and doing so from a distance. Biometric screening is similarly an invasive function, particularly if automated and subject to the higher error rates inherent in 1:N comparison using large datasets.

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.

https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%202%20Assessment%20Tool-FINAL.pdf, p 16.

[322] ICAO Doc 9303, "Machine Readable Travel Documents", Part 9, 7th Edition, 2015, https://www.icao.int/publications/documents/9303_p9_cons_en.pdf, pp 7-8.

[323] Hong Kong, Office of the Privacy Commissioner for Personal Data, Guidance on Collection and Use of Biometric Data, *Guidance Note*, August 2020, https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf, p 3.

2.2 Automating Infrastructure: Kiosks, e-Gates & Decision-making

In recent years, the prevalence of automated passport verification has increased, beginning with pre-clearance programs and rapidly expanding to all travellers. The ultimate goal of the push towards automation is for facial recognition to displace travel documents—your face will be your passport.[324]

Automated Border Control infrastructure or systems ("ABC") tie control over physical barriers to automated traveller recognition, often based on facial comparisons between the traveller's face as photographed by the gate and the digital facial image encoded on their passport. ABCs can take various forms. The most common are kiosks and e-Gates. Kiosks are typically stands that include an interactive display, a camera, and some form of electronic document reader.

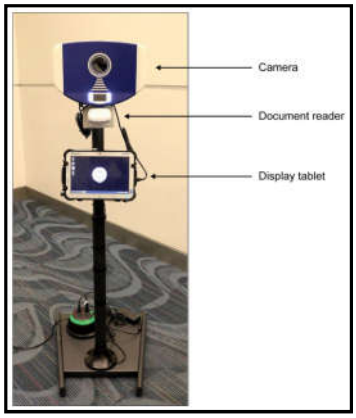

Figure 11: US Customs and Border Protection facial verification service pilot testing apparatus[325]

Kiosks often provide independent automated recognition of travellers, which is then transmitted to border control officials digitally or through printed receipts.[326] Increasingly, kiosk-based traveller recognition is integrated with other physical infrastructure, such as automated gates.[327] When

[324] Nathan Munn, "More Facial Recognition and Drones Wanted for the US-Canada Border", August 25, 2020, *Vice*, https://www.vice.com/en/article/889bwz/more-facial-recognition-and-drones-wanted-for-the-us-canada-border; World Economic Forum, "Known Traveller Digital Identity: Pilot Project", June 18, 2019, slide 11.

[325] Image Source: United States Customs and Border Protection, Departure Information System Test Concept of Operations, May 2016, as displayed in: United States, Government Accountability Office, "Border Security", February 2017, GAO-17-170, https://www.gao.gov/assets/690/683036.pdf, p 19, Figure 4.

For this pilot test, passengers presented their boarding pass to the electronic document reader on the apparatus, while the system searched their live facial images against a pre-generated manifest of images associated with all passengers scheduled for that particular flight.

[326] Canada's Primary Inspection Kiosks, for example, use printed receipts with traveller's images and as well as the result of the automated facial recognition comparison and some customs information. These receipts are presented to a border control official. See description in 1.6, at p 59, above.

[327] As noted in Section 2.1.2 above, Australia is currently moving towards a 'seamless' exit/entry process. However, the outgoing system of SmartGates (which operates on the basis of 1:1 passport verification) employs a mechanism of this nature. See: Office of the Australian Information Commissioner, "Assessment of Schedule 5 of the Foreign Fighters Act", October 1, 2016, https://www.oaic.gov.au/privacy/privacy-assessments/assessment-of-schedule-5-of-the-foreign-fighters-act-department-of-immigration-and-border-protection/:

> 3.17 Citizens who choose to have their identity verified through the arrivals SmartGate process first go to a computer kiosk, and insert their passport open at the photo page into a slot in the kiosk. The kiosk scans the passport and collects data from it, including biographical information, a scan of the passport photo and photo data stored in the passport's electronic chip.
>
> 3.18 After the passport scan, the kiosk prompts the citizen to review an electronic privacy notice. The citizen must press the computer screen to acknowledge the notice. The kiosk then generates a ticket for the citizen to collect and feed into the SmartGate. The ticket contains the data collected by the kiosk in a format that can be read by the SmartGate.
>
> 3.19 After the SmartGate reads the ticket to recall the information collected at the kiosk, the citizen is directed to look at a camera positioned inside the SmartGate. The camera captures a facial image of the citizen. The SmartGate then generates a biometric template from the image captured by the camera. This template is compared against a second biometric template generated from the image captured at the kiosk.

integrated, a successfully recognized traveller is issued a temporary 'token' that is submitted to an automated gate which controls physical exit from a border control area.[328] Other ABC solutions will integrate traveller recognition directly into physical infrastructure, generally referred to as 'e-Gates'.[329] e-Gates will typically 'trap' a traveller in a physical space, and physically direct them in one direction or another depending on whether automated recognition succeeds or fails.

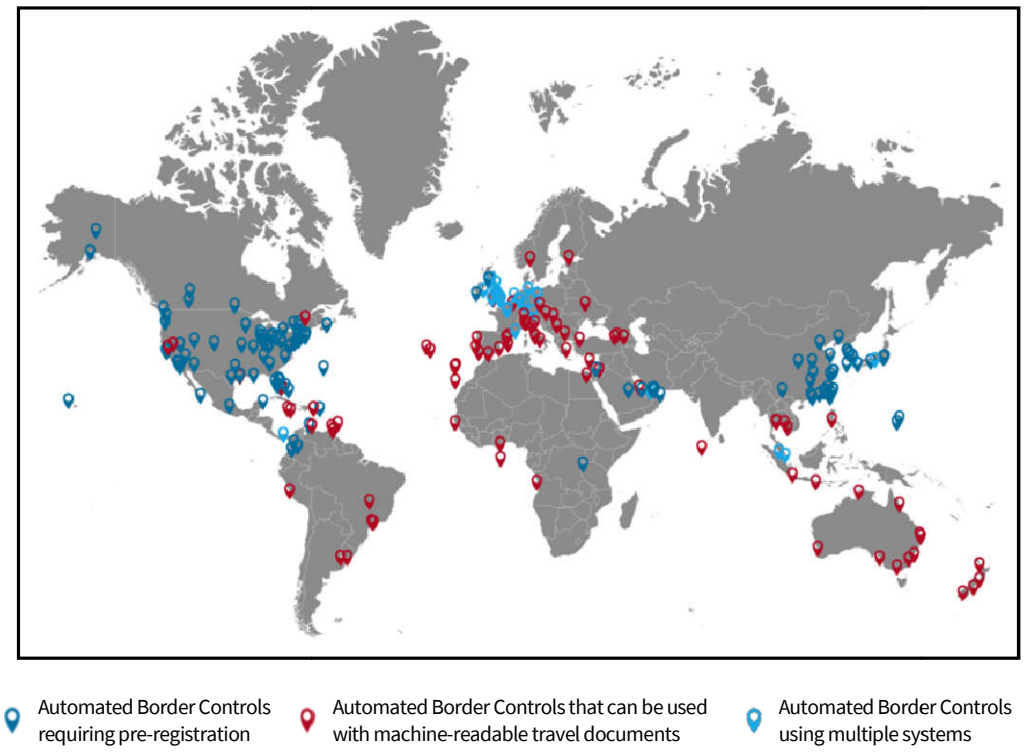

Figure 12: Automated Border Controls at Air Ports of Entry
IMAGE SOURCE: International Air Transport Association (IATA)[330]

Other means of integrating automated recognition into physical border control infrastructure can include the use of strategically mounted cameras, recognition-enabled baggage drop-offs, and recognition-enabled airline check-in.

3.20 The SmartGate uses an algorithm to verify the citizen's identity by calculating the compatibility of the two biometric templates that have been generated. If the biometric templates are matched above a pre-determined threshold, the SmartGate will allow the citizen to proceed. If the biometric templates do not match above this threshold, the citizen is directed to the manual border clearance process by moving back out of the SmartGate.

3.21 After the citizen has passed through the SmartGate, the scanned passport photo and the facial image of the citizen taken by the SmartGate camera are both transferred to the same DIBP information database that holds passport photo scans collected during the manual arrivals process. The biometric templates are not retained beyond the border clearance process.

[328] European Union, Frontex, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", September 2015, https://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_ABC.pdf, p 26 (see description of 'Segregated two-step ABC systems) and Annex 3: "…in the case of the 2-step segregated solution there are 19 kiosks and 4 e-Gates."

[329] Note, the 'e-Gate' and 'Automated Border Control' systems terminology is not used consistently. In some contexts, 'ABC' refers directly to automated gates with integrated facial recognition capabilities, or to specific types of recognition-enabled kiosks. In other contexts, 'e-gate' is used to refer to any automated physical gate, regardless of whether it is facial recognition-enabled or not. However, for the purposes of this report, 'Automated Border Control' systems refer to any physical infrastructure that forms a component of a recognition-enabled border control system, and 'e-Gate' is specifically used to refer to automated physical barriers with an integrated facial recognition capability.

[330] International Air Transport Association (IATA), "Automated Border Control Implementation", last updated March 2019, archived at: https://web.archive.org/web/20190527155531/https://www.iata.org/whatwedo/passenger/Pages/automated-border-control-maps.aspx. Note that the dataset referenced in this Figure does not differentiate between automated border controls that use facial recognition and those that use some other mechanism.

ABCs facilitate a greater degree of border automation in general. This includes fully automating the recognition process by directly linking recognition to physical access. It can also provide a means of injecting other forms of automated decision-making into border control mechanisms, including automated risk assessment, and other automated border control determinations.[331] By removing the necessity for human input at various stages of the border control journey, the impact of automated decision-making becomes far ranging. While most border control systems will still incorporate human decision-making as a final arbiter, individuals who fail the automated assessment process will be locked out of a growing range of automated checkpoints.

ABC systems with various branding ('ePassport Gates', 'SmartGates', 'Parafe Gates', and others) are experiencing rapid adoption (see Figure 12). Some e-Gates mix automated and manual verification, allowing border control officials to remotely view live images, passport details and other intelligence, and to override automated conclusions verifying a travel against their passport or failing to do so.[332]

Data from some jurisdictions suggests rapid growth and normalization of facial recognition-enabled e-Gates, in particular, as automated passport control mechanisms. The United Kingdom has seen the deployment of hundreds of 'ePassport' gates at international air, as well as some train, ports of entry.[333] These ePassport Gates can fully automate the entry approval process through facial verification. Initially, automated entry of this nature was open to all holders of biometric passports issued by the UK, EU, EEA or Switzerland, as well as pre-registered holders of passports from various countries.[334] Beginning in 2019, automated entry through facial passport verification became possible with biometric passports issued to nationals of eight additional countries (including Canada).[335] In fiscal 2017/18 alone, close to 48 million passengers were processed by these

[331] An overview of emerging automated decisions in border processes can be found in: 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*.

[332] UK ePassport Gates. Gemalto ABC, France: "The Coesys ABC eGates provide passengers with a fast and secure passage through immigration, relying on a fully automated verification of the electronic passport and on biometric traveller authentication. Border protection officers can monitor the information in real-time for increased detection of potential fraud cases."

[333] Currently, automated entry is available at all major UK airports and for Eurostar trains terminating in the UK, at terminals in Brussels, Lille and Paris: United Kingdom, "Where You can Use Registered Traveller", *Travelling to the UK: Registered Traveller: Faster Entry Through the UK Border*, accessed April 10, 2019, https://www.gov.uk/registered-traveller/where-you-can-use-registered-traveller. A description of how these eGates operate can be found at: United Kingdom, nidirect Government Services, "Using ePassport Gates at Airport Border Control", last accessed July 4, 2020, https://www.nidirect.gov.uk/articles/using-epassport-gates-airport-border-control.

[334] United Kingdom, nidirect Government Services, "Using ePassport Gates at Airport Border Control", last accessed July 4, 2020, https://www.nidirect.gov.uk/articles/using-epassport-gates-airport-border-control; and United Kingdom, "Eligibility", *Travelling to the UK: Registered Traveller: Faster Entry Through the UK Border*, accessed April 10, 2019, https://www.gov.uk/registered-traveller/eligibility.

[335] Visitors from Canada, the United States, Australia, New Zealand, Japan, Singapore and South Korea who are over the age of 12 who are entering as standard visitors, who will be permitted to use facially recognized-enabled gates as a means of automated entry authorization for a period not exceeding 6 months: United Kingdom, The Immigration (Leave to Enter and Remain)(Amendment) Order 2019, February 18, 2019, SI 2019/298, https://www.legislation.gov.uk/uksi/2019/298/pdfs/uksi_20190298_en.pdf, clause 4, enacting article 8B. The explanatory note to SI 2019/298 states, in part:

> This enables a person who meets the description in the article to obtain leave to enter the United Kingdom as a visitor by passing through an automated gate with no authorisation by an immigration officer. Where such a person passes through an automated gate, the person will automatically be given leave to enter for six months (subject to the conditions set out in article 8B).

automated ePassport gates using facial recognition as the core identity validation technique.[336] The primary driver for this rapid adoption, which saw the deployment of 461 ePassport gates over two years, appears to be political pressure to demonstrate that the UK's impending departure from the European Union will not lead to unmanageable delays at the border.[337]

Some form of biometric recognition is necessary in any automated border control system, and facial recognition is rapidly becoming the biometric of choice as it removes barriers that have deterred widespread adoption of other biometric recognition in some jurisdictions. Facial recognition is faster and more efficient, whereas other biometric techniques such as fingerprint and iris scans require more time. Additionally, facial recognition is more surreptitious, and can be carried out without active traveller awareness that they are participating in a biometric process, forestalling many objections that might otherwise be raised.[338] Finally, facial recognition does not carry the stigma still associated with other biometric recognition mechanisms such as fingerprinting in many jurisdictions.[339] While recognizing that other biometrics such as fingerprinting may continue to play a role in machine-driven border control, facial recognition is rapidly emerging as the leading biometric mode.[340]

For example, the United States Department of Homeland Security (DHS) was able to implement its 'biometric exit' obligations by relying on facial recognition, where multiple attempts relying on fingerprinting had proven impracticable. In 2004, DHS was legally obligated to facilitate 'biometric exit' – the biometric confirmation of travellers who are departing the country against biometrics collected upon their entry.[341] DHS was unable to implement biometric exit using automated fingerprint recognition solutions (using mobile readers called BE-Mobile), and listed two core impediments to

[336] A freedom of information requests indicates that 47,939,884 passengers were processed by automated ePassport gates in fiscal 2017/18. This is a 29% increase over fiscal 2016/17: Kevin, "UK ePassport Gates: Some Interesting Numbers…. And Interesting Data Withheld", *Economy Class & Beyond*, September 1, 2019, https://economyclassandbeyond.boardingarea.com/2019/01/09/investigation-uk-epassport-gates-some-interesting-numbers-and-interesting-data-withheld/.

[337] A freedom of information request indicates that UK Border Force has deployed 461 ePassport gates in fiscal years 2016-17 and 2017-18: Kevin, "UK ePassport Gates: Some Interesting Numbers…. And Interesting Data Withheld", *Economy Class & Beyond*, September 1, 2019, https://economyclassandbeyond.boardingarea.com/2019/01/09/investigation-uk-epassport-gates-some-interesting-numbers-and-interesting-data-withheld/.

[338] Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 11; Jason Kelley, "Skip the Surveillance By Opting Out of Face Recognition at Airports", April 24, 2019, *Electronic Frontier Foundation*, https://www.eff.org/deeplinks/2019/04/skip-surveillance-opting-out-face-recognition-airports.

[339] Raj Nanavati & Pierre Meunier, "Biometric Border Security Evaluation Framework", Defence R&D Canada, DRDC CSS CR 2011-16, October 2011, p 209:

> The association of fingerprints with criminal justice activities has negatively impacted public perception of the technology, although once acclimated users are much less likely to find the technology objectionable. … Face images are already a part of nearly every identity document program in the world, such that the acceptability of acquiring face images is not in question. Whether this blanket acceptability extends to use of face images for automated searches is another question: it seems that there is more resistance to face imaging as a biometric technology than to simple face imaging for the purposes of placement in a document.

[340] ICAO Doc 9303, "Machine Readable Travel Documents", Part 9, 7th Edition, 2015, https://www.icao.int/publications/documents/9303_p9_cons_en.pdf, p 7:

> After a five-year investigation into the operational needs for a biometric identifier which combines suitability for use in the eMRTD issuance procedure and in the various processes in cross-border travel consistent with the privacy laws of various States, ICAO specified that facial recognition become the globally interoperable biometric technology. A State may also optionally elect to use fingerprint and/or iris recognition in support of facial recognition.

[341] United States, Government Accountability Office, "Border Security", February 2017, GAO-17-170, https://www.gao.gov/assets/690/683036.pdf, generally and figure 1 specifically, outlines DHS' various attempts to implement fingerprint-based exit beginning in 2004, when the *Intelligence Reform and Terrorism Prevention Act*, encoded at 8 USC 1365b required the creation of an automated biometric entry and exit system.

doing so. First, airlines were expected to implement biometric exit confirmation by fingerprinting passengers as they boarded flights, but refused to do so on the basis that fingerprinting was a 'public sector function'.[342] Second, fingerprinting is disruptive, slowing down the flow of travellers at airports and consumes substantial human resources, even where fingerprint achieved accuracy:

> During our observations, [Customs and Border Protection] officials noted that the BE-Mobile pilot demonstrated that while the technology can effectively capture biometric data and match that data against DHS databases, it requires too much time and manpower to be a solution for biometric exit capabilities on all flights departing the United States...[343]

In 2015, DHS abandoned its decade-long attempt to rely on fingerprinting as its primary means of meeting its biometric exit obligations and instead shifted its focus to facial recognition. The greater efficiency of facial recognition allowed for biometric identification to occur absent significant impediment to the flow of passengers, while requiring far less human resources.[344] Secondly, whereas the airline industry initially objected to playing a role in the overtly intrusive collection of fingerprints from passengers seeking to leave the United States,[345] there appears to be far less resistance to participation in facial recognition on exit.[346]

Automated infrastructure allows border security agencies to apply a range of algorithmic decision-making processes to travellers in a direct manner. It is possible to fully automate decision-making without ABCs in place—policy or law can remove human discretion and compel deference to automated determinations, or systems can be implemented in a manner that provides human decision-makers with no information beyond the output of algorithmic determinations.[347] However,

---

[342] United States, Government Accountability Office, VISA Waiver Program, September 2008, GAO-08-967, https://www.gao.gov/assets/290/280861.pdf, pp 23-24. By contrast, DHS describes facial recognition solutions as follows:

> In this context, facial recognition has presented CBP with the best biometric approach because it can be performed relatively quickly, with a high degree of accuracy, and in a manner perceived as less invasive to the traveler (e.g., no actual physical contact is required to collect the biometric).

Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf, p 3.

[343] United States, Government Accountability Office, "Border Security", February 2017, GAO-17-170, https://www.gao.gov/assets/690/683036.pdf, pp 12-15.

[344] United States, Government Accountability Office, "Border Security", February 2017, GAO-17-170, https://www.gao.gov/assets/690/683036.pdf, p 25:

> CBP officials noted that they are exploring biometric exit capabilities that minimize the involvement of CBP officials, either by having the collection of biometric information done automatically through facial recognition technology or using airline personnel to process passengers.

Canadian border control officials have similarly recognized that facial recognition is faster, cheaper and more efficient than iris biometrics, and is in the process of replacing its NEXUS kiosks, historically used to process known travelers using iris recognition, with facial recognition:

> Existing NEXUS kiosks are now reaching their end-of-life. In response, the CBSA has developed a new initiative, NEXUS Modernization, which aims to reduce program costs and improve processing by replacing iris biometric with facial biometric verification.

Canada Border Services Agency, "NEXUS – Privacy Impact Assessment", Executive Summary, last modified January 14, 2020, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/nexus-eng.html.

[345] United States, Government Accountability Office, VISA Waiver Program, September 2008, GAO-08-967, https://www.gao.gov/assets/290/280861.pdf, pp 23-24.

[346] United States, Government Accountability Office, "Border Security", February 2017, GAO-17-170, https://www.gao.gov/assets/690/683036.pdf, p 23:

> In November 2016, CBP officials also told us the agency had changed its approach to the biometric exit capability and was working with airlines and airports on strategies for using public/private partnerships to both reduce the cost to taxpayers and give industry more control over how a biometric exit capability is implemented at airport gates. CBP's previous planned approach had been for CBP to acquire and deploy biometric technology at airports, and to be responsible for collecting biometric information from passengers.

[347] Similarly, ABCs can be implemented in a manner that requires remote human interaction before any determination becomes final.

the use of ABCs reduces the practical need for human intervention, and encourages the use of automated decision-making as human intervention undermines the efficiency gains made by automating infrastructure. Decision-making automation becomes the default.

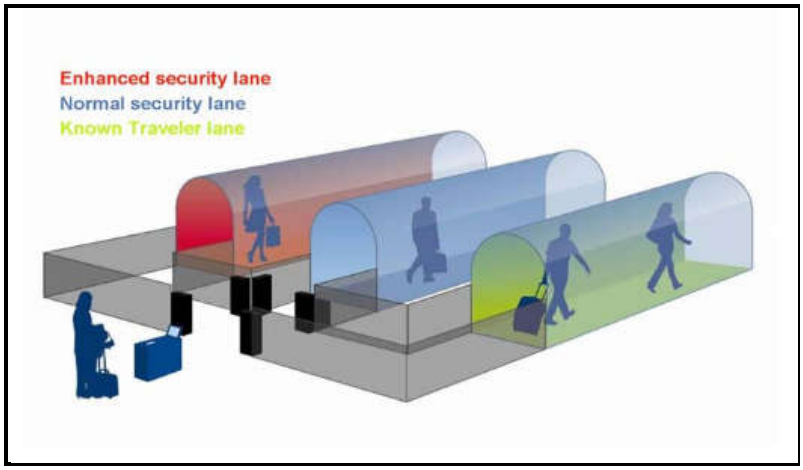

Figure 13: Automated Sorting of High Security, Normal and Trusted Travellers
IMAGE SOURCE: IATA, Checkpoint of the Future[348]

Yet other automated decision-making tools suffer from similar racial biases as facial recognition.[349] Where facial recognition is used as an identification basis for facilitating other automated border control decision-making, these discriminatory impacts can be compounded.

For example, the CBSA's Primary Inspection Kiosk (PIK) automated secondary inspection referral mechanism uses a range of assessment tools and relies on facial recognition to verify travel documents.[350] An internal CBSA analysis obtained by CBC found wide discrepancies in the proportion of travellers directed to secondary inspection on the basis of country of origin.[351] Specifically, PIKs disproportionately referred travellers from Iran, Jamaica, Chad, the Philippines and Nigeria to secondary screening for immigration purposes on a purely selective, as opposed to mandatory, basis.[352] It remains unclear to what degree bias in the PIK facial recognition system or

[348] International Air Transportation Association, "Checkpoint of the Future: Blueprint", ver 2, March 14, 2011, http://aci-aviation.com/presentations/Checkpoint_of_the_Future_IATA.pdf.

[349] For example, United Kingdom border control officials have been criticized for over-reliance on an algorithmic risk assessment tool that undermined reliance on individualized criteria, leading to non-meritorious rejection of visa applications for African countries: United Kingdom, All-Party Parliamentary Group Report, "VISA Problems for African Visitors to the UK", June 2019, p 21. See also: 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; 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); Safiya Umoja Noble, "Algorithms of Oppression: How Search Engines Reinforce Racism", (New York: NYU Press, 2018).

[350] 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.

[351] 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.

[352] 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.

bias in the PIK assessment system are compounding or even contributing factors in this disproportionate referral process as CBSA will not publicly disclose any error ratings for its facial recognition system, claiming national security concerns.[353] Similarly, no data is available as to the number and demographics of travellers who were unable to benefit from the speed and convenience of the automated PIK process and were subjected to standard manual processing because the facial recognition system was unable to verify their passports. However, it is notable that purely manual referrals did not exhibit the same country of origin-specific disparities.[354]

Adoption of facial recognition additionally renders more disruptive forms of identification and search more practical. For example, the efficiency gains that result from wide-spread automation may be unevenly distributed among travellers. For example, while automated fingerprint recognition was too disruptive for DHS to implement as the primary means of border control biometric recognition, it becomes feasible to implement as a 'backup' for those travellers who cannot be processed by facial recognition.[355] More generally, adoption of facial recognition removes resource constraints that can be reinvested in more prolonged or aggressive screening for those who cannot successfully navigate the standard border control process.[356]

Facial recognition-dependent ABCs are not limited to e-gates, and can include automated flight check-in, baggage drop, airline lounge access and even airport-based car rental. Often these elements will be controlled by airlines or other private sector entities.

[353] 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.

[354] 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.

[355] Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf, p 31:

> If the image created by the facial recognition camera system does not match the photograph template on file associated with the individual's travel document, the operator directs the traveler to a CBPO stationed at the passenger loading bridge. The CBPO uses the wireless BE-Mobile handheld device72 to verify the traveler's identity using either fingerprints for aliens, via a query in the OBIM IDENT, or by conducting an inspection to ensure the traveler is holding valid travel documents.

[356] United States, Transportation Security Administration, "TSA Biometrics Roadmap: For Aviation Security & Passenger Experience", September 2018, https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf, p 18: "Biometrics can enable TSA to automate current manual procedures and reinvest screening personnel time saved into performing other critical security tasks and biometric error resolution."

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.

2.3 Location: Expanding Border Identification Reach & Purpose

Facial recognition can be incorporated into multiple points of the border control ecosystem, with varying implications.

Pragmatically, the specific location at which facial recognition is implemented can have implications for its efficiency, accuracy and general feasibility. Normatively, some automated recognition 'nodes' are added at locations that have always included an identification capability, but extend the animating objectives or scope of the recognition task beyond the border control purposes that were historically proportionate in character. Other recognition 'nodes' are added at border control locations that did not historically require identification, extending the ability to track travellers and to collect additional information about them. Additionally, adoption of automated facial recognition systems permits greater integration of information collected at disparate points of the border control process.

2.3.1 Facial Recognition at the ...

Identification has long been a clearly established component of international travel, with different locations within the border crossing journey justifying different forms of collection for different border control objectives. Facial recognition is increasingly being used to extend the scope of collection, the locations where collection occurs, and the objectives animating collection and subsequent use.

... customs & immigration checkpoint.

Facial recognition is most widely adopted at customs control and immigration checkpoints, where identification has been historically well established. As a result, airports, border control agencies, and the overall border crossing 'flow' already accounts for the need to identify travellers in some manner at these locations. Facial recognition at these checkpoints also largely supports established border control objectives related to regulating the entry of goods and persons into a state's territorial boundaries. While the adoption of automated facial recognition at established checkpoints raises many of the privacy and related implications identified throughout this document, these are not driven by the location of the implementation in question.

Facial recognition at checkpoints most commonly takes the form of kiosks or automated e-gates. Frequently, facial recognition will be combined with other forms of automated or semi-automated traveller processing, including the completion and assessment of customs declarations and immigration processing and the use of risk-assessment decision-making tools.

The creation of a facial recognition-enabled profile upon entry can raise additional and distinct privacy challenges if the resulting capability is used as a multi-purpose surveillance tool. The European Union, for example, recently adopted a controversial regulation that would compel all foreign nationals seeking to enter the EU to enrol in a facial recognition-enabled database with the primary objective of monitoring EU entry/exit.[357] A secondary objective of the system, however, is to support general internal law enforcement and crime investigation,[358] and the regulation explicitly authorizes Europol and Member States' policing agencies to use the facial recognition capability it creates.[359] It should be noted that the necessity and legality of this component of the regulation has been questioned.[360]

... departure gate.

It has been historically common to impose rigorous identification obligations on entities seeking to enter a country, as states carefully control who and what is permitted within their territorial borders. A state's ability to prevent a traveller from leaving, however, is much more attenuated, and the right to depart any country is enshrined in international law.[361] As a result, exit identity confirmation is a relatively recent development in many states, typically justified by the need to identify overstays. It should be noted that the utility of exit identity confirmation in terms of achieving border control objectives has been challenged.[362]

In Canada, the CBSA is not obligated to collect personal information departing travellers but recently received statutory authorization to collect departure information, at its discretion, for the first time.[363]

---

[357] European Union, Regulation 2017/2226, Entry/Exit System (EES), November 30, 2017, Article 1(1):

> This Regulation establishes an 'Entry/Exit System' (EES) for: (a) the recording and storage of the date, time and place of entry and exit of third–country nationals crossing the borders of the Member States at which the EES is operated; (b) the calculation of the duration of the authorised stay of such third-country nationals; (c) the generation of alerts to Member States when the authorised stay has expired; and (d) the recording and storage of the date, time and place of refusal of entry of third-country nationals whose entry for a short stay has been refused, as well as the authority of the Member State which refused the entry and the reasons therefore.

[358] European Union, Regulation 2017/2226, Entry/Exit System (EES), November 30, 2017, Article 1(2): "For the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences, this Regulation also lays down the conditions under which Member States' designated authorities and Europol may obtain access to the EES for consultation."; European Commission, Impact Assessment Report on the Establishment of an EU Entry Exit System", SWD(2016)115, June 4, 2016, p 19.

[359] European Union, Regulation 2017/2226, Entry/Exit System (EES), November 30, 2017, Article 32 (4)(b) and 5(e and Article 33.

[360] European Data Protection Supervisor, Opinion 6/2016, Opinion on the Second EU Smart Borders Package, September 21, 2016, paras 83-89.

[361] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, p 79.

[362] See, for example, European Union, Committee of the Regions, Opinion on 'Smart Borders package', 2014/C 114/15, paras 26-29:

> 27. notes that the main objective of the EES is to identify third country nationals who enter the Schengen area legally, with or without a short-term visa, and stay longer than the authorised period. To this end, the authorised period of stay is calculated electronically and an alert is sent to the national authorities concerning overstayers, with a view to intercepting illegal immigrants and repatriating them;
>
> 28. believes that the EES's added value in terms of achieving this objective is not clear, as the existence of an alert regarding the illegal presence of an individual is based on the assumption that people who enter the EU with a short-term visa or without a visa are required to leave it within a maximum of three months, without taking into consideration particular circumstances such as an application for asylum or the regularisation of a person's presence under national law;
>
> 29. notes that the analysis of the necessity and proportionality of the EES is even more necessary, as there is no detention for unauthorised residence. The system would only be able to detect unauthorised immigrants when they leave the Schengen area, which makes the EES 'little more than an extremely expensive mechanism for gathering migration statistics'.

[363] Bill C-21, SC 2018, c 30, which received royal assent on December 13, 2018, enacted sections 92-95 of the *Customs Act*, RSC 1985, c 1, which permit the

Similarly, the European Union has only recently adopted a comprehensive system for exit tracking of non-nationals and is in the process of implementing it.[364]

The rationale for extensive customs and immigration vetting upon departure from a state remains more attenuated than upon arrival, and few jurisdictions require travellers to report to customs or Immigration officials prior to departing a country.[365] As a result, exit confirmation is often realized by airlines and other commercial conveyances. In Canada, for example, CBSA intends to rely on airlines in order to achieve its objective of compiling complete travel history records on all travellers leaving Canada by air.[366] Australia, by contrast, requires all citizens to undergo a complete immigration process upon departure—citizens must either report to a border control official or self-process at an automated facial recognition-enabled e-Gate upon departure.[367]

While Canada's newly adopted exit confirmation regime expressly and legislatively excludes the collection of biometric information,[368] other states have incorporated biometric identification obligations into their exit confirmation obligations. Notably, the United States Department of Homeland Security has been attempting to realize biometric exit confirmation since it was congressionally mandated to in 2004.[369] This obligation is only now being implemented at departure gates with the assistance of airlines, and its expedited implementation has been adopted as a priority by Executive Order.[370] A central contributing factor to the viability of this

---

CBSA to adopt various measures to collect information on persons departing Canada.

[364] European Commission, Impact Assessment Report on the Establishment of an EU Entry Exit System", SWD(2016)115, June 4, 2016, p 16: "At the moment, the entries and exits of third country nationals in the Schengen area are recorded only in their travel documents..."; European Union, Regulation 2017/2226, Entry/Exit System (EES), November 30, 2017.

[365] *Exit Information Regulations*, Regulatory Impact Analysis Statement, Part I, 153(11) *Canada Gazette*, March 16, 2019: "By collecting the information from reliable partners, rather than requiring travellers to report to the CBSA when leaving Canada, the process would be seamless for travellers.".

[366] *Exit Information Regulations*, Regulatory Impact Analysis Statement, Part I, 153(11) *Canada Gazette*, March 16, 2019.

[367] Office of the Australian Information Commissioner, "Assessment of Schedule 5 of the Foreign Fighters Act", October 1, 2016, https://www.oaic.gov.au/privacy/privacy-assessments/assessment-of-schedule-5-of-the-foreign-fighters-act-department-of-immigration-and-border-protection/, paras 3.25-3.30; Australia, Minister of Home Affairs, "Removal of the Outgoing Passenger Card", June 25, 2017, https://minister.homeaffairs.gov.au/peterdutton/Pages/removal-of-the-outgoing-passenger-card-jun17.aspx.

[368] *Customs Act*, RSC 1985, c 1, as amended by Bill C-21, SC 2018, c 30, sections 92-93 expressly lists the data elements that can be collected upon departure, to the exclusion of biometric information such as facial images. Legislative amendment would therefore be required to impose a biometric solution. See: *Exit Information Regulations*, Regulatory Impact Analysis Statement, Part I, 153(11) *Canada Gazette*, March 16, 2019, https://cippic.ca/uploads/ExitInformationRegulations-SOR2019_241.pdf:

> Risk: The scope of the Entry/Exit Initiative could inadvertently be expanded to include additional personal information beyond what is strictly necessary to manage travel history information (biometric information, licence plates, passenger name record data, etc.).
>
> Mitigation: New legislative authorities have been enacted to ensure that the collection of personal information is limited by a statutory framework, namely, the data elements outlined in sections 92 and 93 of the *Customs Act*. The collection of any additional personal information is not currently in scope, nor are there any plans to collect this information in the immediate future.

By contrast, the regime governing information collection upon arrival in Canada established collected data elements and mechanisms by regulation, making it far easier to expand: *Customs Act*, RSC 1985, c 1, section 107.1, compels any prescribed class of persons can be compelled to provide any prescribed information relating to any person on board or expected to be on board a conveyance. The *Passenger Information (Customs) Regulations*, SOR/2003-219 currently defines obligations under section 107.1.

[369] United States, Government Accountability Office, "Border Security", February 2017, GAO-17-170, https://www.gao.gov/assets/690/683036.pdf, generally and figure 1 specifically, outlines DHS' various attempts to implement fingerprint-based exit beginning in 2004, when the *Intelligence Reform and Terrorism Prevention Act*, encoded at 8 USC 1365b required the creation of an automated biometric entry and exit system.

[370] United States, Executive Order 13780, March 6, 2017, https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states-2/, Section 8: "The Secretary of Homeland Security shall expedite the completion and implementation of a biometric entry exit

program has been its ability to implement facial recognition at departure gates by airlines, as direct DHS collection would require additional staffing and physical space/infrastructure that is not readily available.[371] However, there is no guarantee that airlines will apply facial recognition with the breadth and consistency required to achieve DHS' objectives.[372] It has been argued that no clearly documented need for the addition of biometrics in order to provide a clear picture of United State departures has been established, and the legality of biometric collection has not been established with respect to US nationals.[373]

... security checkpoints.

Facial recognition is often introduced at established border crossing security checkpoints. Confirming traveller identification or boarding passes at security checkpoints is historically common, but the primary objective of this identification has historically been to screen people and property in order to prevent unauthorized individuals or objects from entering sterile airport locations.[374]

Identification at security screening checkpoints has not historically been as robust as is the case at customs and immigration checkpoints, as the objective of identification at security screening is to confirm that a traveller is authorized to access a sterile area. This is largely achieved by confirming that a traveller's identification matches the name on their airline-issued boarding pass.[375] Some agencies

---

tracking system for in-scope travelers to the United States...". United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.

[371] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, pp 12-13 and 26.

[372] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, pp 22-23 and 29:

> CBP cannot successfully advance beyond initial operating capability without the airlines' investment and partnership. While CBP had not developed back-up plans for funding or staffing an entirely CBP-operated model, it estimated that costs and staffing levels would increase dramatically without airline support. Specifically, CBP estimated that the biometric program budget would increase from $1 billion to $8 billion without airline assistance. Likewise, CBP staffing requirements would increase from 441 to as many as 6,000.

[373] 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*.

[374] United States, Department of Homeland Security, "Privacy Impact Assessment: Travel Document Checker Automation Using Facial Recognition", January 5, 2018, DHS/TSA/PIA-046, p 1.

[375] United States, Department of Homeland Security, "Privacy Impact Assessment: Travel Document Checker Automation Using Facial Recognition", January 5, 2018, DHS/TSA/PIA-046, p 1:

> The TSA employee performing Transportation Document Checker (TDC) functions typically manually verifies identity at the checkpoint by comparing the facial photograph on a passenger's identity document to the passenger's actual face and the credential's biographic information to the biographic information on the passenger's boarding pass. The TDC also checks the boarding pass and identity credential for authenticity. Once those steps are successfully completed, the passenger proceeds to security screening.

The authenticity of documents such as boarding passes, passports or other forms of identification is also frequently confirmed at security checkpoints: United States, Department of Homeland Security, "Privacy Impact Assessment Update: Credential Authentication Technology/Boarding Pass Scanning System", January 18, 2013, DHS/TSA/PIA-024(b), p 1:

> Using CAT/BPSS, TSA verifies the authenticity of a passenger identity document by comparing its format and security features against a known set of security features for that particular identity document type.

Canadian Air Transport Security Authority, Boarding Pass Security System (BPSS) and CATSA Plus, Privacy Impact Assessment – Public Summary, October, 2016, https://www.catsa-acsta.gc.ca/sites/default/files/imce/BPSSandCATSAPlus.pdf.

further compare a traveller's name against security watch lists, known traveller lists, and risk assessment protocols in order to determine what level of security screening a traveller will be subjected to prior to entering a sterile airport location.[376]

Facial recognition adoption at security checkpoints has been driven by disparate objectives. It has been tested as an alternative means of achieving biometric exit confirmation and as a means of increasing the efficiency of current manual identification confirmation. It will also be used to confirm security screening status, including eligibility for voluntary known traveller expedited processing.

The United States Department of Homeland Security has piloted a joint facial recognition operation at airport security checkpoints as a means of achieving its biometric exit confirmation obligations (described above, at p. 85). Biometric exit screening at security checkpoints is substantially similar to its operation in departure gates, with a few key differences. First, security checkpoints are staffed and operated by DHS Transportation Security Agency officials, and it is therefore the TSA, rather than an airline, that becomes responsible for staffing and operating facial recognition equipment. Second, whereas facial recognition at departure gates is limited to a 1:N comparison of travellers' live image against a pre-populated reference image gallery of travellers premised on a specific flight manifest, recognition at TSA security screening points requires comparison against all anticipated departing travellers as the location is not inherently tied to a single departing flight.[377] As noted above, facial recognition against a larger gallery of reference images is, all other factors being equal, more difficult to achieve with comparable speed and accuracy.[378] Finally, where biometric exit confirmation occurs at departure gates, it is anticipated that airlines will absorb some or all of the equipment and staffing costs. It is not clear that sufficient funds are available to replicate this capability through the TSA.[379]

Independently from its biometric exit trials, TSA has been testing automated facial recognition as a means of verifying traveller documents such as passports and boarding passes.[380] This has, to date, included two trials, one using e-Gates and a more recent trial equipped document authentication

[376] United States, Department of Homeland Security, "Privacy Impact Assessment Update: DHS/TSA/PIA-018(f), pp 2-3. TSA's Secure Flight program determines a screening status for each traveller based on presence on a security watch list, the outcome of a risk assessment, and presence on a 'known traveller' expedited security list. The travellers' Secure Flight screening status is then transmitted to TSA officials at security checkpoints when travellers present their boarding pass and identification: DHS/TSA/PIA-024(b), p 2: "TSA will transmit passengers' full name, gender, date of birth, Secure Flight screening status, reservation control number, and flight itinerary from the Secure Flight database to STIP.5 STIP will then send the Secure Flight data to the CAT/BPSS devices."

[377] United States, Department of Homeland Security, Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, p 7:

> The primary difference in the CBP-TSA matching process, as opposed to the process outlined with CBP owned and operated cameras, is that each template will be matched against multiple galleries, based on that day's flight manifests for that particular international terminal, rather than being matched against the templates for only one departing flight's manifest.

[378] See discussion of reference dataset size and 1:1 vs 1:N modes of comparison, at Sections 1.1.1 and 1.2.2, above.

[379] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, pp 22-23, 27 and 29.

[380] United States, Department of Homeland Security, "Privacy Impact Assessment: Travel Document Checker Automation Using Facial Recognition", January 5, 2018, DHS/TSA/PIA-046.

devices with facial recognition capabilities.[381] Both trials employed a 1:1 comparison mode, comparing travellers' live images against the reference image encoded on their ICAO-compliant biometric passports.[382] The e-Gate trial only verified a traveller's passport using automated facial recognition. The second trial added facial recognition to a document authentication device already in use by TSA ("Credential Authentication Technology" or "CAT"), and confirmed travellers' boarding passes as well as their travel documents.[383] TSA's CATs are also used to access a traveller's pre-determined security screening status so that TSA agents at security checkpoints can direct the traveller accordingly.[384] At this point in the trials, security screening status is not premised on facial recognition-based identification, which has so far been limited to document verification in both trials.[385] Facial recognition-based identification is merely the vehicle by which pre-determined security status is applied to a specific traveller.

The higher volume of travellers at security checkpoints present a more challenging environment for facial recognition than departure gates. Adoption of facial recognition for security screening objectives might ultimately lead to a high level of automation at security checkpoints if e-Gates are adopted in its final implementation. This level of automation will be heightened if TSA decides to apply its security screening status determinations to travellers through the use of facial recognition-enabled e-Gates.

---

[381] United States, Department of Homeland Security, "Privacy Impact Assessment: Travel Document Checker Automation Using Facial Recognition", August 23, 2019, DHS/TSA/PIA-046(a).

[382] United States, Department of Homeland Security, "Privacy Impact Assessment: Travel Document Checker Automation Using Facial Recognition", January 5, 2018, DHS/TSA/PIA-046, p 3:

> Unlike biometric matching efforts by ... Customs and Border Protection (CBP), which involve comparing biometrics of international travelers against pre-populated galleries created from previously collected images, TSA seeks to verify identity by comparing the face of individuals presenting themselves to the technology against the image contained in their identification document (in this case, their passport). This approach may provide greater opportunities in future technology testing and developing requirements for biometric matching against other trustworthy identification documents such as REAL-ID compliant driver's licenses, permitting greater passenger throughput and security posture.

See also United States, Department of Homeland Security, "Privacy Impact Assessment: Travel Document Checker Automation Using Facial Recognition", August 23, 2019, DHS/TSA/PIA-046(a), p 2.

[383] United States, Department of Homeland Security, "Privacy Impact Assessment: Travel Document Checker Automation Using Facial Recognition", August 23, 2019, DHS/TSA/PIA-046(a).

[384] United States, Department of Homeland Security, "Privacy Impact Assessment Update: DHS/TSA/PIA-018(f), pp 2-3. TSA's Secure Flight program determines a screening status for each traveller based on presence on a security watch list, the outcome of a risk assessment, and presence on a 'known traveller' expedited security list. The travellers' Secure Flight screening status is then transmitted to TSA officials at security checkpoints when travellers present their boarding pass and identification: United States, Department of Homeland Security, "Privacy Impact Assessment Update: Credential Authentication Technology/Boarding Pass Scanning System", January 18, 2013, DHS/TSA/PIA-024(b), p 2: "TSA will transmit passengers' full name, gender, date of birth, Secure Flight screening status, reservation control number, and flight itinerary from the Secure Flight database to STIP. STIP will then send the Secure Flight data to the CAT/BPSS devices."

[385] United States, Department of Homeland Security, "Privacy Impact Assessment: Travel Document Checker Automation Using Facial Recognition", August 23, 2019, DHS/TSA/PIA-046(a), p 2:

> The CAT-C device will compare the live facial image of the individual to the image from the passenger's identity document using a proprietary facial matching algorithm to verify that the document belongs to the person presenting it. Once the facial matching result is recorded, TSA personnel staffing the CAT-C will direct the passenger to the standard TDC.

United States, Department of Homeland Security, "Privacy Impact Assessment: Travel Document Checker Automation Using Facial Recognition", January 5, 2018, DHS/TSA/PIA-046, p 3:

> Finally, the facial recognition technology will compare the extracted e-Passport photo with the real-time facial images using a NIST-compliant facial matching algorithm. For passengers with a positive match, the e-Gate electronic security gates will open and the passengers will proceed to the TDC. For passengers who receive a negative facial match, or experience any error during the process, the e-Gate will not open and the passenger will be directed to the TDC. All passengers must complete the standard TDC process for manual identity and travel document verification, regardless of the e-Gate biometric matching results.

... curb.

Some airports or airlines are implementing 'curb to gate' facial recognition solutions that permit travellers to navigate entire airports using their face as their sole or primary means of identification.

India's third busiest airport, Kempegowda International Airport (Bengaluru), for example, is in the process of launching a fully biometric, all of airport implementation.[386] Once complete, travellers will be able to interact with 350 facial recognition 'touchpoints' throughout the airport, removing the need to rely on physical passport-based verification.[387]

Delta has also announced the installation of a 'biometric terminal' at Atlanta's Hartsfield-Jackson International Airport in collaboration with TSA and CBP.[388] The full 'curb to gate' solution enables travellers to use facial recognition at:

- automated self-service check-in kiosks;
- automated baggage drops;
- a TSA security screening checkpoint;
- at the gate, for boarding international flights (biometric exit);
- to navigate customs upon entry.[389]

CBP's Traveler Verification Service (TVS), created in order to meet its legal obligation to verify travellers departing the territorial United States using biometric recognition, allows private airlines to facilitate biometric exit by querying TVS with facial images live-captured at international departure gates.[390] Delta uses the same TVS capacity in order to facilitate facial recognition at other identification points throughout the airport, such as at check-in kiosks and baggage drops.[391] Delta indicates that 7% of travellers note they have an issue with the program and 28% state they prefer standard boarding.[392] Also according to Delta, only about 2% of travellers opt-out of the program which, when combined with a 97% reported matching accuracy rate, suggests that about 5% of

[386] Vision-Box, "Kerb-to-Gate Biometric Journey Goes Live at Kempegowda International Airport", *International Airport Review*, August 2, 2019, https://www.internationalairportreview.com/news/99430/biometric-journey-kempegowda-international-airport/.

[387] Vision-Box, "Kerb-to-Gate Biometric Journey Goes Live at Kempegowda International Airport", *International Airport Review*, August 2, 2019, https://www.internationalairportreview.com/news/99430/biometric-journey-kempegowda-international-airport/

[388] Initially only available in one terminal, the program has since been expanded to all terminals: Kathryn Steele, "Delta Unveils First Biometric Terminal in US in Atlanta; Next Stop: Detroit", *Delta: News Hub*, accessed January 31, 2020, https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit; Kathryn Steele, "Delta Expands Optional Facial Recognition Boarding to New Airports, More Customers", *Delta: News Hub*, December 8, 2019, https://news.delta.com/delta-expands-optional-facial-recognition-boarding-new-airports-more-customers.

[389] Delta, "A Blueprint for the Future: How Delta is Driving Industry Change in International Travel with Biometrics", *Delta: News Hub*, October 22, 2019, https://news.delta.com/blueprint-future-how-delta-driving-industry-change-international-travel-biometrics.

[390] United States, Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018.

[391] Delta, "How it Works: The First Biometric Terminal in the US", *Delta: News Hub*, September 20, 2018, https://news.delta.com/how-it-works-first-biometric-terminal-us.

[392] Kathryn Steele, "Delta Expands Optional Facial Recognition Boarding to New Airports, More Customers", *Delta: News Hub*, December 8, 2019, https://news.delta.com/delta-expands-optional-facial-recognition-boarding-new-airports-more-customers.

travellers are manually processed.[393] It remains unclear whether this disparity results from a lack of alignment between self-reported preferences and actual behaviour or of it results from a lack of adequate awareness of alternative options.[394]

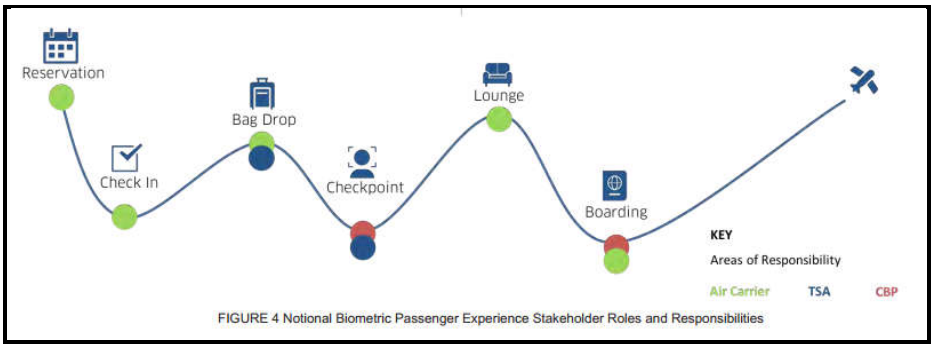

Figure 14: Checkpoints & Beyond
IMAGE SOURCE: TSA Biometric Roadmap[395]

Many of the identification points adopted in a 'curb-to-gate' facial recognition already involve some form of identification verification by either an airline, the TSA or CBP. However, as more entities rely on CBP's Traveler Verification Service for carrying out the facial recognition task, CBP is provided with an increasingly complete picture of a traveller's movements throughout the airport at large.

... your mobile phone.

Mobile devices are increasingly being incorporated into border control processes, often in a manner that is integrated with or reliant on facial recognition capabilities.

In 2017, the Canada Border Services Agency (CBSA) launched the CanBorder eDeclaration mobile application that travellers can use to complete customs inspection questions when arriving in Canada.[396] Travellers enter customs data into the application while still in flight, and transmit it to

[393] Kathryn Steele, "Delta Expands Optional Facial Recognition Boarding to New Airports, More Customers", *Delta: News Hub*, December 8, 2019, https://news.delta.com/delta-expands-optional-facial-recognition-boarding-new-airports-more-customers.

[394] Allie Funk, "I Opted Out of Facial Recognition at the Airport—It Wasn't Easy", July 2, 2019, *WIRED*, https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/:

> Last month, I was at Detroit's Metro Airport for a connecting flight to Southeast Asia. I listened as a Delta Air Lines staff member informed passengers that the boarding process would use facial recognition instead of passport scanners.
>
> As a privacy-conscious person, I was uncomfortable boarding this way. I also knew I could opt out. Presumably, most of my fellow fliers did not: I didn't hear a single announcement alerting passengers how to avoid the face scanners.
>
> To figure out how to do so, I had to leave the boarding line, speak with a Delta representative at their information desk, get back in line, then request a passport scan when it was my turn to board. Federal agencies and airlines claim that facial recognition is an opt-out system, but my recent experience suggests they are incentivizing travelers to have their faces scanned—and disincentivizing them to sidestep the tech—by not clearly communicating alternative options. Last year, a Delta customer service representative reported that only 2 percent of customers opt out of facial-recognition. It's easy to see why.

[395] United States, Transportation Security Administration, "TSA Biometrics Roadmap: For Aviation Security & Passenger Experience", September 2018, https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf, Figure 4, p 18.

[396] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html.

their Primary Inspection Kiosk (PIKs) once they have landed by scanning a QR code.[397] The PIKs rely on facial recognition in order to fully automate the customs and immigration process.[398] As a security measure, this mobile application is designed to retain minimal data and to automatically delete customs information after 24 hours.[399]

One ambitious program being piloted by Canada and the Netherlands relies on mobile devices and facial recognition as two of its four primary enabling technologies. The World Economic Forum's Known Traveler Digital Identity (KTDI) proposal, detailed in Box 12 and in Section 1.1.1, stores an ICAO compliant facial image on a traveller's mobile device and crates an interface that permits travellers to share this image for biometric recognition with border control officials on demand.[400] Enrolment in the program, however, will occur only once, meaning the biometrics and any additional enrollment data will be permanently stored on the traveller's device. Additional information such as traveller credit scores, education certificates, banking and vaccination statements can be made accessible through the mobile device as well.[401]

Integrating mobile devices into the border control processes raises a number of privacy implications. First, travellers are required to decrypt and unlock their mobile devices in order to access any embedded border control functionality such as the customs application, a virtual boarding pass, or the KTDI suite of capabilities. As border control officials are granted expansive search powers, decrypting a mobile device in the presence of a border control officials puts all the data contained on that device at risk of exposure to a cursory examination.[402] Second, data in mobile applications is difficult to secure. In some instances, operating systems or classes of applications are granted broad rights to access data contained on mobile devices for a variety of reasons. In other instances, data is accessed without active individual intention through permission systems that are all too fluid. Additionally, mobile applications are difficult to secure

[397] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html: "PIK will also provide an expedited functionality for travellers to complete their on-screen declaration by using the CanBorder-eDeclaration app. The app users will be prompted, at the beginning of the kiosk session, to scan their eDeclaration QR code which will pre-populate the kiosk screens, reduce typing and expedite processing at the kiosk."

[398] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html. For a more detailed discussion of Primary Inspection Kiosks see Section 2.1.1 at p 65 and Box 19 at p 139.

[399] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html: "The mobile app operates without any connection to CBSA systems (i.e., in airplane mode) and retains only basic, non-protected, traveller information, used to pre-populate a portion of the kiosk data entry. Declarations on the app are deleted after 24 hours, and may be manually deleted at any time."

[400] 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.

[401] 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 15, Figure 5.

[402] See: British Columbia Civil Liberties Association and Samuelson Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), Electronic Devices Privacy Handbook, October 2018, https://bccla.org/wp-content/uploads/2018/10/Electronic-Devices-Privacy-Handbook-BCCLA_2.0.pdf; 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.

against unauthorized intrusion by malicious applications or other intrusion tools loaded onto the same device. Given the richness of the potential dataset, a border control mobile application might become a tempting target for malicious crime or foreign state actors.

Finally, even where measures are taken to impose proportionate state access, other states will not necessarily respect such measures. For example, the KTDI proposal is intended to be voluntary in nature, and user-centric by design, so that travellers will choose what information or biometric capabilities to share with specific border control officials.[403] However, this does not prevent any given border control agency from ignoring KTDI's user-centric principles and compelling travellers to provide access to an existing profile.[404]

2.3.2 Cross-Location Integration: OneID to Rule Them All

Facial recognition and other assessment tools are also increasingly integrated with the intention of creating a detailed picture of a traveller's movements and actions throughout their trip.[405]

The International Air Transport Association (IATA)'s OneID initiative would implement a centralized identity management platform that will interact with various biometrically enabled touchpoints throughout the port of entry/exit.[406] Each time a traveller biometrically interacts with a touchpoint, the touchpoint will register with the identity management platform, allowing for "real-time visibility of where passengers are in the airport process."[407] This real-time visibility along with other traveller data encoded on the centralized identity management platform would then be made available to various border control entities on a 'need and authorized to know' basis.[408]

---

[403] 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 14:

> The concept is based on the idea that an individual is in control of providing specific identity information (e.g. biometric, biographic and travel history) to governmental … players along the journey, such as border control agencies … for risk-profiling, verification and access. The traveller can select which information is shared for a specific time according to the authority … requirements.

[404] *R v Fearon*, 2014 SCC 77; British Columbia Civil Liberties Association, Electronic Device Privacy Handbook, July 2018, https://bccla.org/wp-content/uploads/2018/10/Electronic-Devices-Privacy-Handbook-BCCLA_2.0.pdf; Joseph Cox, "China is Forcing Tourists to Install Text-Stealing Malware at its Border", July 2, 2019, *VICE: Motherboard*, https://www.vice.com/en_us/article/7xgame/at-chinese-border-tourists-forced-to-install-a-text-stealing-piece-of-malware.

[405] See D.O. Gorodnichy, S.N. Yanushkevich & V.P. Shmerko, "Automated Border Control: Problem Formalization", *CBSA Science & Engineering Directorate*, Division Report 2014-41, September 2014, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc203/p801324_A1b.pdf, pp 3-4; and 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, for example.

[406] International Air Transport Association, OneID: Concept Paper, ver 1, January 2018, https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/oneid-concept-paper.pdf, pp 3-4 and International Air Transport Association, "One ID End State and Key Principles", December 14, 2018, https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/oneid-endstate-key-principles.pdf:

> 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.

[407] IATA, OneID: Concept Paper, ver 1, January 2018, https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/oneid-concept-paper.pdf, p 5.

[408] IATA, "One ID End State and Key Principles", December 14, 2018, https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/oneid-

A number of airports around the world are implementing OneID with facial recognition. Narita Airport in Japan will soon allow travellers to enrol in OneID when checking in for their flight—facial recognition will be used to validate the traveller's identity upon enrollment, and to re-verity the traveller at baggage drop-off, security screening and boarding.[409]

The WEF's Known Traveller Digital Identity similarly envisions a single biometrically-enabled identity system. Using facial recognition, the traveller collects 'attestations' of their identity each time it successfully interacts with a border control and other touchpoint.[410] Attestations become the "backbone of trust and the basis of reputation" in the KTDI system. Allowing foreign border control entities to review a traveller's history of attestations as well as related travel history allows travellers to become 'known' and access expedited security screening.

By establishing an integrated facial recognition-based identification, traveller interactions and movements become consolidated, creating a detailed and complete profile of their movements.

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.

2.4 Known Travellers: Opting in to Facial Recognition

Some border control biometric programs are introduced on an opt-in basis, typically in the context of secure traveller programs.

endstate-key-principles.pdf, p 1: "One ID facilitates the sharing of the passenger's biographical, biometric and travel document information between the various public and private stakeholders that interact with the passengers across the journey and have a valid reason (need-to-know / authorized-to-know) to access certain data in order to process passengers correctly, safely and securely. This is the "core" of One ID."

[409] Rachel Harper, "Smart Check-in Services to be Implemented at Narita Airport", October 24, 2019, *International Airport Review*, https://www.internationalairportreview.com/news/106120/smart-check-services-narita-airport/; NEC, "NEC to Provide Facial Recognition System for New 'OneID' Check-in to Boarding Process at Narita Airport", February 28, 2019, *NEC.com*, https://www.nec.com/en/press/201902/global_20190228_01.html; Narita Airport, "'OneID' Facial Recognition, a New 'Check-In to Boarding Experience' Using Biometric Authentication will be Introduced at Narita Airport", February 28, 2019, *Narita Airport; News Release*, https://www.naa.jp/en/20190228-OneID_en.pdf.

[410] 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, Figure 14, p 33.

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.

[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, http://www.aci-europe-events.com/wp-content/uploads/docs/post-event/aga2018/presentations/lisette-looren-de-jong.pdf Slide 11. See also World Economic Forum, "The Known Traveller: Unlocking the Potential of Digital Identity for Secure and Seamless Travel", 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.

Frequently, biometric collection forms part of a broader opt-in enhanced security screening process that allows qualifying travellers to enjoy expedited processing at border control crossing on the basis that they are allotted a 'trusted' status. Opting in to a facial recognition program, in this context, is distinct from individual choice as exercised in the context of a particular facial recognition interaction.

Trusted traveller programs incentivize travellers to opt-in by emphasizing 'pain points' in the standard travel experience that might be avoided by travellers who are willing to submit to more intrusive advance scrutiny. The border control context is extraordinary in society, allowing far greater state intrusion and interference than in most other contexts of life.[411] Against this backdrop of greater intrusion and coercion, trusted traveller programs can offer a compelling value proposition to many travellers.[412] Some initiatives seek to further leverage this highly incentivized context to usher the adoption of society-wide biometric identification systems.

2.5 Creeping Beyond Border Control

Border control facial recognition systems are at high risk of being expanded beyond the border control objectives that animated their adoption, or of being wholly repurposed. In a related development, systems are becoming increasingly interoperable on a technical basis, removing technical obstacles to broad-ranging repurposing by a range of government bodies.

First, facial recognition systems implemented at border control settings are increasingly used in order to achieve general law enforcement objectives. In the United States, legislation was introduced in 2017 that, if passed, would have required border control facial recognition systems to become interoperable with law enforcement biometric databases.[413] The United Kingdom is also piloting a program that would attempt to match travellers' facial images against biometrically enabled criminal watch lists.[414] Australia is also developing an ability to screen travellers against facial recognition-enabled watch lists to identify persons of interest to law enforcement.[415] The European Union has similarly adopted a controversial border control facial recognition system that explicitly encompasses general law enforcement considerations as a secondary objective of the system.[416]

Second, in contexts where no general-purpose facial recognition system is available, state agencies will occasionally seek to make singular use of capabilities created for specific purposes. For example,

[411] 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.

[412] European Data Protection Supervisor, Opinion on the Proposals for a Regulation Establishing an Entry/Exit System (EES) and a Regulation Establishing a Registered Traveller Programme (RTP), July 18, 2013, paras 79-80.

[413] Harrison Rudolph, Laura M Moy & Alvaro M Bedoya, "Not Ready for Takeoff: Face Scans at Airport Departure Gates", *Center on Privacy & Technology*, December 21, 2017, p 13.

[414] United Kingdom, Home Office, "Biometrics Strategy: Better Public Services Maintaining Public Trust", June 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf, para 35; *R (Bridges) v Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin), paras 14-16, rev'd [2020] EWCA Civ 1058.

[415] Chris Duckett, "Unisys Pockets AU$90m in Border Biometrics and Defence IT Support", March 19, 2018, *ZDNet*, https://www.zdnet.com/article/unisys-pockets-au90m-in-border-biometrics-and-defence-it-support/.

[416] European Union, Regulation 2017/2226, Entry/Exit System (EES), November 30, 2017, Article 1(2): "For the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences, this Regulation also lays down the conditions under which Member States' designated authorities and Europol may obtain access to the EES for consultation."; European Commission, Impact Assessment Report on the Establishment of an EU Entry Exit System", SWD(2016)115, June 4, 2016, p 19. Note that the legality of the system has been questioned: European Data Protection Supervisor, Opinion 6/2016, Opinion on the Second EU Smart Borders Package, September 21, 2016, paras 77 *et seq*.

the British Columbia driver's license database (operated by a crown corporation, ICBC) was updated with facial recognition capabilities in order to help prevent the issuance or usage of fraudulent licenses.[417] An investigation conducted by the Information & Privacy Commissioner for British Columbia discovered that ICBC had repurposed its facial recognition database in order to identify anonymous individuals in photographs submitted to it by various policing agencies.[418] Similarly, the CBSA's Privacy Impact Assessment for its facial recognition-enabled Primary Inspection Kiosks explicitly notes that information requests from law enforcement partners will be assessed on a case-by-case basis if required for enforcement or public safety concerns.[419]

Finally, large-scale repurposing of border control facial recognition systems has also occurred or been proposed. The United States Customs and Border Protection (CBP), for example, has created a facial recognition capability to achieve congressionally-mandated border control biometric recognition objectives.[420] This capability is now marketed to airlines and other entities as a broader 'Identity as a Service' mechanism and is queried by airlines and others to achieve a range of customer service identity-related objectives that are not directly related to the congressional mandate that justified its creation.[421] A World Economic Forum facial recognition proposal being piloted by Canada and the Netherlands (described in Box 12, above) actively seeks to gain voluntary adoption in the airport context, with the ultimate objective of creating a general purpose digital identification tool that will be available for use in a range of public and private domestic contexts.[422]

Australia's Identity Matching Services initiative also envisions wide-scale repurposing of border control facial recognition capabilities. In 2017, Australian federal, state and territorial leaders signed an Intergovernmental Agreement (IGA) on Identity Matching Services (IMS), with the objective of establishing a national facial recognition services.[423] The Agreement and proposed enabling legislation

[417] 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.

[418] 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.

[419] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html: "As per the CBSA's existing practices, in the event it is required for enforcement, program integrity or to address health and safety concerns, information may be requested on a case-by-case basis by law enforcement partners, Employment and Social Development Canada (ESDC) and the Public Health Agency of Canada (PHAC) respectively."

[420] The Open Identity Exchange, "Biometric Boarding using Identity as a Service: The Potential Impact on Liability in the Aviation Industry", July 2018, https://oixuk.org/wp-content/uploads/2018/08/Biometric-Boarding-white-paper-FINAL-v3-1.pdf; Michael Hardin, Director, Office of Field Operations, Customs and Border Protection, "CBP Innovation: Identity as a Service (IDaaS) Solution", *ICAO TRIP19*, June 28, 2019, https://www.icao.int/Meetings/TRIP-Symposium-2019/PublishingImages/Pages/Presentations/CBP%20Innovation%20Identity%20as%20a%20Service%20(IDaaS)%20Solution.pdf.

[421] See discussion in Section 2.6, p 102, below. See also: The Open Identity Exchange, "Biometric Boarding using Identity as a Service: The Potential Impact on Liability in the Aviation Industry", July 2018, https://oixuk.org/wp-content/uploads/2018/08/Biometric-Boarding-white-paper-FINAL-v3-1.pdf.

[422] 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 37.

[423] Intergovernmental Agreement on Identity Matching Services, October 5, 2017, https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf [IGA]. See also: Australia, Identity-Matching Services Bill 2019, first reading, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6387_first-reps/toc_pdf/19156b01.pdf [*IMS Bill*]; Australia, Identity-Matching Services Bill 2019, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6387_ems_f8e7bb62-e2bd-420b-8597-

(the *IMS Bill*) identifies a broad range of purposes, ranging from law enforcement, to national security, to road safety, to standard administrative identity verification.[424] It establishes facial verification as a *de facto* general purpose national identifier for administrative government and private sector services while creating a facial identification tool that fails to preclude generalized surveillance in national security and law enforcement contexts.

Box 13: Australia's Identity Matching Service: National ID & 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 was 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.[1] Absent this authorization, the Australian *Privacy Act* would limit sensitive biometric profiles from being repurposed.[2]

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 the building blocks for a *de facto* national identification system with facial recognition as its core 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.

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

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

Collectively, the IMS initiative encompasses three core components: a set of facial recognition comparison services, two facial recognition reference data aggregation tools, and a framework authorizing the repurposing of existing facial recognition capabilities for a set of itemized activities.

8881422b4b8f/upload_pdf/713695.pdf [*IMS EM*]; Australia, Parliament Library, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019: Bills Digest", August 26, 2019, Bills Digest No 21, 2019-20, https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6875141/upload_binary/6875141.pdf [*IMS Bill Digest*]; Government of Australia, Parliamentary Joint Committee on Intelligence and Security, Advisory Report on the Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-Matching Services) Bill 2019, Parliamentary Paper 458/2019, October 14, 2019, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/CTLA2019MeasuresNo1/Report [*PJCIS Report*].

For a history of the initiative, see: *IMS Bill Digest*, pp 12-15.

[424] IGA, clause 1.2; *IMS Bill*, clause 6.

The first of these components authorizes the Department of Homeland Affairs (DHA) to operate a range of facial recognition querying services. These include a 1:1 Face Verification Service (FVS) and a 1:N Face Identification Service (FIS). These services can only be used to query biometric databases already included in the IMS reference dataset aggregation tools (described below) and as a result they cannot be used to query live camera feeds or social media sites. However, facial images from live photographs, CCTV stills, social media profiles, or a range of other sources can be submitted electronically to these querying services.[425] The FV Service can be used to verify identity claims made by individuals to various entities, and is broadly available across government and private sector bodies.[426] However, local government bodies and approved private sector entities are restricted from using it without consent.[427] The FVS thereby has potential to transforms facial images into a *de facto* national identification.[428]

Given its capacity to identify unknown individuals, the *IMS Bill* recognizes the FIS capability as more intrusive and provides additional safeguards for its use. For example, the FIS service will only be available to specifically itemized government agencies in relation to their law enforcement and national security mandates.[429] In addition, the FIS cannot be used to facilitate road safety or administrative identity verification in the provision of government services.[430] As a law enforcement tool, the FI Service poses a tangible threat to anonymity, as the *IMS Bill* places no limits on its use for trivial offences or in the absence of individualized suspicion.[431] There are additional concerns its identification capability will be used as evidence of identity in judicial proceedings, as the *IMS Bill* does not prohibit the use of FIS to produce evidence.[432]

---

[425] *IMS EM*, para 122: "An example of a use for the FIS would be a police force using a CCTV image obtained from the scene of an armed robbery to assist in identifying the suspect." See also: *IMS Bill Digest*, p 7.

[426] *IMS Bill*, see sub-clauses 6(8) and 10(2). Sub-clause 6(8) includes "verifying the identity of an individual" as one of the purposes for which the IMS' 1:1 facial verification service can be queried and is "intended to reflect clauses 1.2(g) of the IGA" (*IMS EM*, para 100). Clause 1.2(g) of the IGA states: "Identity verification — the verification of an individual's identity, where this is done with the consent of the individual or as authorised or required by law, for example in the delivery of government services or for private sector organisations to meet regulatory identity verification requirements."

See also *PJCIS Report*, para 3.85: "The Face Verification Service would provide efficiencies in providing government services electronically, without the need for an individual having to present in person to a shopfront."; and *IMS EM*, paras 120: "The FVS is a service that will allow a participating government agency or non-government entity to verify an individual's known or claimed identity using a facial image of the person on a government identification record."

[427] *IMS Bill*, paragraphs 10(2)(c)-(d), sub-clause 6(2) and sub-clause 6(3). However, it is clear that freely given explicit consent will not be required in all contexts: *IMS EM*, paras 106, 104 and 232 "The concept of 'consent' in the Bill is intended to have the same meaning as in the Privacy Act. ... It is intended to include express consent or implied consent."

See also: *PJCIS Report*, paras 3.112-3.116: "the Department stated that private sector users of the Face Verification Service will need to meet their obligations under the Privacy Act and this may mean that a private sector organisation would have to provide 'alternative options for identity verification..." [emphasis added].

[428] The FVS permits 1:1 querying across all participating government profiling systems through a single unique identifier: the facial image.

[429] *IMS Bill*, sub-clauses 8(2)-(3) limit the types of agencies that can use the FIS, primarily focusing on agencies pursuing a law enforcement or national security objective. See also: *PJCIS Report*, para 3.59.

[430] *IMS Bill*, paragraph 8(1)(b) defines Face Identification Services to include facial comparison carried out for purposes itemized in sub-clauses 6(2)-(6), which are, respectively, the prevention and detection of identity fraud, law enforcement activities, national security activities, protective security activities and community safety activities. Paragraph 8(1)(b) excludes 'road safety activities' and identity verification (sub-clauses 6(7)-(8), respectively) from the definition of FIS.

[431] *PJCIS Report*, paras 3.66, 5.56, 5.68 and 5.69. See also *IMS Bill Digest*, pp 30: "Australian Lawyers for Human Rights ... objected to the use of identity-matching services where there is no clear connection to a likely offence." and 31 "The absence of any lower limit in the Bill in regards to offences appears to envision future changes to the IGA that expand the offences for which the *FIS* may be used."

[432] *PJCIS Report*, paras 2.68 and 5.69.

The second component of the IMS initiative authorizes DHA to establish and operate two reference dataset aggregation tools: an interoperability hub (Hub) and a National Drivers License Facial Recognition Solution (NDLFRS). The NDLFRS will create a new electronic database containing digitized versions of various state and territorial identification (but not federal) documents, initially anticipated to consist of driver's licenses.[433] It will then create biometric templates of all facial images included in the NDLFRS and a querying system to search those templates. The Hub is essentially a centralized querying interface. It will interconnect with existing facial recognition-enabled government databases, and permit entities to search across all of these by submitting facial images and related identifying information through one single web interface.[434]

Finally, the IMS initiative provides the lawful authority necessary to repurpose a number of existing digitized government documents such as driver's licenses, visas and passports. The IGA and the *IMS Bill* both encode seven distinct and broadly framed activities that govern use of its services: preventing and detecting identity fraud, law enforcement activities, national security activities, protective security activities, community safety activities, road safety activities and verifying identity.[435] The Australian *Privacy Act* treats biometric data as 'sensitive' and generally requires express consent or clear legislative authorization if such data is to be repurposed by a government agency.[436] Yet many of the biometric databases aggregated for querying in the NDLFRS and the interoperability Hub were initially created for other purposes. In this respect, the *IMS Bill* itself authorizes DHA to collect, use, and disclose personal information when operating the NDLFRS or interoperability hub in support of these seven activities.[437] The *IMS Bill* itself does not provide independent lawful authority for other entities wishing participate in the broader IMS initiative, yet other elements of the broader IMS legislative package provide this legal basis.[438] For example, companion legislation to the *IMS Bill* would amend the *Passports Act*, providing lawful authority for the Australian Department of Foreign Affairs and Trade (DFAT) to make facial recognition-enabled travel documents available through the IMS initiative and in pursuit of the

[433] *IMS Bill*, section 15; *IMS EM*, paras 174-179: "The main documents that will initially have their identification information incorporated into the system are driver licences. However, identification information from other state or territory identification documents may also be incorporated, such as fishing, firearm and marine licences and proof of age or identity cards."

[434] *IMS EM*, paras 170-172.

[435] Encoded in sub-clauses 6(2)-(7) of the *IMS Bill*.

[436] Australia, *Privacy Act 1988*, No 119, 1988, section 6, "sensitive information means … (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or; (e) biometric templates"; APP 6.2(a)(i). See also, *IMS Bill Digest*, p 17:

> Under the *Privacy Act*, biometric information used for the purpose of automated biometric verification or identification, as well as biometric templates, is classified as 'sensitive information'. Sensitive information is generally afforded a higher level of protection than other personal information, in recognition of the adverse consequences which may flow from the inappropriate handling of such information. Limitations include that sensitive information can only be collected with consent (unless a specified exception applies) and can only be used or disclosed for a secondary purpose to which it was collected if this is directly related to the primary purpose of collection. However, it is an exception to these restrictions if the collection, use or disclosure is required or authorised by an Australian law.

[437] *IMS Bill*, clauses 17-18; *IMS EM*, para 5. See also: *PJCIS Report*, paragraphs 3.112 – 3.116 "The Department stated that it would 'rely on [*Privacy Act*] APP 6.2(b), which permits use or disclosure where authorised by a … law – in this the case, the Bill. This will enable the Department to lawfully fulfil its role in transmitting information between agencies participating in the identity-matching services.'"

[438] *IMS EM*, para 71. *IMS Bill Digest*, pp 14-15, describes some state and territorial legislation introduced to authorize participation in the IMS initiative.

activities described therein.[439] It is presumed that some agencies will already have the requisite legal basis to query the IMS system in connection with one of the seven activities identified by the IMS Bill.[440]

Repurposed border control facial recognition profiles play a central role in the IMS initiatives. The interoperability Hub will be populated by the NDLFRS and a number of federal biometrically-enabled databases, all of which include border control-related documents such as passports and visas.[441] While the NDLFRS will not be operational until DHA creates it and regional governments begin populating it, the border control-related databases already exist and are already enabled for facial recognition querying. Indeed, much of the querying functionality envisioned by the interoperability Hub is already operational in relation to border control databases. The 1:1 Face Verification Service that the *IMS Bill* introduced has been in operation since 2016, with both DFAT and the Australian Federal Police (AFP) using its facial recognition querying capabilities against images initially collected for processing of travel documents.[442] The querying system used in this initiative has since been expanded to provide a 1:N matching capability as well.[443] More generally, travel documents are issued with a higher degree of vetting than other forms of government identification, such as driver's licenses. The repurposed border control related facial recognition profiles will therefore play a central role in facilitating the integrity of the overall IMS initiative.

The IMS initiative has been criticized for the intrusive capabilities it envisions.[444] Attempts by the federal government to implement the inter-governmental agreement through legislation have, to

---

[439] *Australian Passports Amendment (Identity-Matching Services) Bill 2019*, clause 3; *Australian Passports Amendment (Identity-Matching Services) Bill 2019*), Explanatory Memorandum, para 1, 15-16, 22 and 35: "This Bill … [provides] a legal basis for ensuring that the Minister is able to make Australian travel document data available for all the purposes of, and by the automated means intrinsic to, the identity-matching services to which the Commonwealth and the States and Territories agreed in the Intergovernmental Agreement on Identity Matching Services (IGA), signed at a meeting of the Council of Australian Governments on 5 October 2017."

[440] *IMS EM*, para 71: "Clause 6 is not intended to authorise the use of identity-matching services by participating entities for the activities set out in the clause. Participating entities will need to have their own legal basis to collect and share identification information in relation to one or more of the identity or community protection activities in order to use the identity-matching services for that activity. This need not be a specific reference in legislation to the use of identity-matching services by the participating entity. However, it would need to have a sufficient connection to one of the identity or community protection activities. For example, a police force would need to have a legal basis to collect, use and disclose identification information for preventing, detecting, investigating or prosecuting an offence in order to rely on the law enforcement activity in subclause 6(3) to use an identity-matching service."

[441] *IMS EM*, para 62: "The definition of identification information set out subclause 5(1) is intended to capture the range of information that is likely to be transmitted via the interoperability hub or contained in the NDLFRS for the purposes of Home Affairs providing identity-matching services. This includes any information contained in the databases to which the interoperability hub will be connected that is required to support the services. The initial databases that the interoperability hub will be connected to are: the database of visa and citizenship information maintained by Home Affairs; the database of passport information maintained by DFAT; and the database within the NDLFRS."

[442] *IMS Bill Digest*, pp 12-13.

[443] Stephen Gee, Assistant Secretary, Department of Foreign Affairs and Trade, Australia, "Biometric Systems: Can They Be Cheap and Simple?", (2018) 13(1) *ICAO TRIP Magazine* 12, cross-posted to: *Uniting Aviation*, January 9, 2019, https://www.unitingaviation.com/strategic-objective/security-facilitation/cheap-and-simple-biometric-systems/; *Migration Amendment (VISA Revalidation and Other Measures) Bill 2016*, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5751_ems_2fb75e14-e450-4d1c-9c16-e0c27f0913b0%22, "The Australian Passport Office database which holds images collected as part of the Australian passport identity verification process. The Department has arrangements in place for access to this database which is currently used for border clearance. Access to images of Australian citizens supports Contactless Automated Immigration Clearance."

[444] *PJCIS Report*, paras 3.66, 5.56, 5.68 and 5.69. See also *IMS Bill Digest*, pp 30: "Australian Lawyers for Human Rights … objected to the use of identity-matching services where there is no clear connection to a likely offence." and 31 "The absence of any lower limit in the Bill in regards to offences appears to envision future changes to the IGA that expand the offences for which the *FIS* may be used."

date, failed.[445] In 2019, an Australian parliamentary committee took the unusual step of rejecting the government's most recent legislative proposals, recommending a complete redraft to address privacy and civil liberties concerns.[446]

2.6 Private Sector Use of Border Control Capabilities

Facial recognition capabilities created in the border control context are increasingly being posited for use by the private sector for a range of purposes.

Adoption of facial recognition at state controlled checkpoints creates a technological capability that can be purchased and implemented by private companies. For example, Air New Zealand implemented facial recognition enabled baggage drop using technology that is similar to the SmartGates used for passport control at New Zealand airports.[447]

Airlines are frequently enlisted to achieve facial recognition objectives at various locations in an airport that are under their control. In the United States, airlines are relied upon to biometrically confirm the identity of travellers departing the territorial United States. Without airline participation, United States Customs and Border Protection (CBP) would lack the staffing, resources and physical space necessary to biometrically confirm international departures as required by law.[448] To facilitate airline-based biometric confirmation, CBP operates a facial recognition system, the Traveler Verification Service (TVS), which can be queried by airlines with facial images captured at departure gates. Facial images submitted by airlines are compared by CBP to an image gallery of travellers that CBP compiled based on advance passenger flight information (APIS) indicated the anticipated manifest of the specific international flight being boarded.[449] The TVS service will return a 'match' or 'no match' result to the airline, and no additional data.[450]

---

[445] Parliament of Australia, Parliament Library, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019: Bills Digest", August 26, 2019, Bills Digest No 21, 2019-20, https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6875141/upload_binary/6875141.pdf:

> The purpose of the Identity-matching Services Bill 2019 (IMS Bill) is to authorise the Commonwealth to facilitate the sharing of identification information, including facial images, between the Commonwealth, states and territories for the purposes of identity-matching. The Bill provides a legal basis for certain aspects of the *Intergovernmental Agreement on Identity Matching Services*, signed by Council of Australian Governments (COAG) leaders on 5 October 2017.

[446] *PJCIS Report*.

[447] Justin Lee, "Air New Zealand Installs Biometric Bag Drop at Auckland Airport", December 10, 2015, *Biometric Update*, https://www.biometricupdate.com/201512/air-new-zealand-installs-biometric-bag-drop-at-auckland-airport.

[448] United States, Department of Homeland Security, Office of the Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide", September 21, 2018, OIG-18-180, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf, pp 12-13 and 26:

> CBP cannot successfully advance beyond initial operating capability without the airlines' investment and partnership. While CBP had not developed back-up plans for funding or staffing an entirely CBP-operated model, it estimated that costs and staffing levels would increase dramatically without airline support. Specifically, CBP estimated that the biometric program budget would increase from $1 billion to $8 billion without airline assistance. Likewise, CBP staffing requirements would increase from 441 to as many as 6,000.

[449] Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf, pp 5-6.

[450] Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018,

Although partner airlines are required by CBP business arrangements to delete any facial images specifically collected through the TVS program,[451] this requirement does not appear to be rigorously enforced. For example, a company contracted by CBP to conduct automated license plate recognition at land borders was subject to similar business restrictions on the retention of images. The company broke its agreement and collected images of travellers crossing the land border in order to develop a proprietary algorithm that would allow it to match drivers' identities with their license plates using facial recognition, yet the company faced no long term sanctions once the breach was discovered.[452] Further, airlines are free to establish their own image gathering and facial recognition capabilities, leveraging the normalization and legitimacy obtained through operation of official recognition services.

Airlines are also permitted to leverage government facial recognition capabilities created to achieve specific public policy goals in order to achieve their own customer service objectives. For example, Delta has extended its use of CBP's TVS program to automate various customer service functions such as baggage check and check-in kiosks.[453]

Delta not only leverages CBP's technological facial recognition capabilities to achieve its customer service objectives, but also emphasizes its integration with CBP in customer-facing materials explaining and legitimizing its adoption of the technology.[454] While Delta and other airlines making

---

https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf, p 22:

> Under the TSA exit demonstration and the partner process initiative, CBP may share the result of the TVS match (i.e., simply a "match" or "no match" result) with the approved partner agency or organization in order to allow the traveler to proceed. For instance, in air exit, the TVS provides a "green light" for the partner airline or TSO to permit the traveler to continue through the screening process. Similarly, the TVS provides a "green light" for the partner airline to permit the traveler to depart the United States and board the aircraft. In the case of a negative result, the TSO or partner organization would either adjudicate the "no match" and/or direct the traveler to a CBPO. This limited sharing of information will be covered by business requirements that CBP is developing for its partner organizations.

[451] Department of Homeland Security, Privacy Impact Assessment: Traveler Verification Service, DHS/CBP/PIA-056, November 14, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf, p 22:

> Privacy Risk: There is a risk that a partner airline, airport authority, or cruise line will retain biometric information longer than is necessary.
>
> Mitigation: This risk is partially mitigated. CBP's business requirements for its partners, along with this PIA, govern partner retention practices. CBP requires its partners to delete the TVS photos following transmission to the TVS. While an approved partner may collect photos of travelers using its own equipment under its own separate business process for commercial purposes, as of the publication of this PIA, no such partner had communicated to CBP any plans to do so.

[452] 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/; Drew Harwell, "Surveillance Contractor That Violated Rules by Copying Traveler Images, License Plates Can Continue to Work with CBP", October 10, 2019, *The Washington Post*, https://www.washingtonpost.com/technology/2019/10/10/surveillance-contractor-that-violated-rules-by-copying-traveler-images-license-plates-can-continue-work-with-cbp/; See also: 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.

[453] Brandi Vincent, "Inside the CBP-Built 'Backbone' of Atlanta's Biometric Terminal", January 21, 2020, *NexGov*, https://www.nextgov.com/emerging-tech/2020/01/inside-cbp-built-backbone-atlantas-biometric-terminal/162558/: ""Those photos provide enough of a basis for the system to compare your live face and verify that it's actually you," [Privacy and Civil Liberties Oversight Board Chairman, Adam] Klein said."; Delta, "How it Works: The First Biometric Terminal in the US", September 20, 2018, https://news.delta.com/how-it-works-first-biometric-terminal-us,

[454] Delta, "How it Works :The First Biometric Terminal in the US", September 20, 2018, https://news.delta.com/how-it-works-first-biometric-terminal-us; https://news.delta.com/sites/default/files/ig%200927ATL%20F%20biometrics%20how%20it%20works.pdf: "CBP creates photo gallery based on manifest"; "Encrypted, de-identified photo sent via secure CBP channel to verify against flight manifest gallery"; "CBP sends verification back with indicator to proceed"; "CBP's encrypted matching service keeps customer ID private."

use of TVS state they do not currently retain any facial images through this process, airlines are nonetheless able to extract value from the ability to query the system.[455] CBP, for its part, has been marketing these broader 'Identity as a Service' (IDaaS) capabilities as a means of transforming digital identity management at airports.[456]

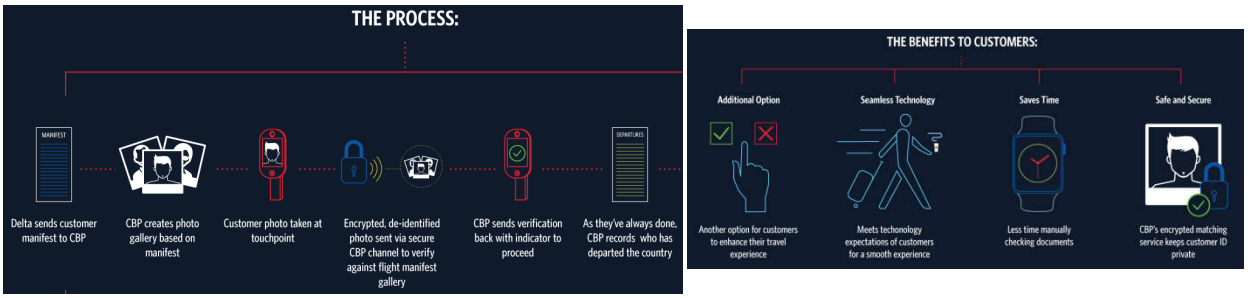

Figure 15: Customer-Facing Materials Explaining Airline's Use of Facial Recognition
IMAGE SOURCE: Delta, "How it Works: The First Biometric Terminal in the US", 2018

In this way, the use of TVS with partner airlines to achieve a lawful border control objective can have a legitimizing and normalization impact on the broader use of facial recognition by airlines. Partner programs allow airlines to expose customers to facial recognition under government fiat. Additionally, these partnerships establish and apply standards for accuracy, data security, information integrity, and passenger experience (in terms of delay and inaccuracy thresholds) that airlines can later replicate to achieve their own customer service needs. The United States Transportation Security Agency, for example, is undertaking a standardization process of this nature while working with industry partners to achieve wide-spread adoption of front-end solutions.[457]

Australia has similarly been leveraging facial recognition systems created to achieve border control objectives in order to facilitate private sector digital identity management objectives. Australia's Identity-Matching Service (IMS), described in greater detail in Box 13 at p 98 above, leverages facial recognition matching capabilities created in large part to achieve border control objectives in order to create an open-ended identification capability that can be queried by various entities.[458] The IMS

[455] 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*, pp 14-15, Hudson Hongo, "What Your Airline Won't Tell You About Those Creepy Airport Face Scans", *Gizmodo*, April 23, 2019, https://gizmodo.com/what-your-airline-wont-tell-you-about-those-creepy-airp-1834218228.

[456] The Open Identity Exchange, "Biometric Boarding using Identity as a Service: The Potential Impact on Liability in the Aviation Industry", July 2018, https://oixuk.org/wp-content/uploads/2018/08/Biometric-Boarding-white-paper-FINAL-v3-1.pdf; Michael Hardin, Director, Office of Field Operations, Customs and Border Protection, "CBP Innovation: Identity as a Service (IDaaS) Solution", *ICAO TRIP19*, June 28, 2019, https://www.icao.int/Meetings/TRIP-Symposium-2019/PublishingImages/Pages/Presentations/CBP%20Innovation%20Identity%20as%20a%20Service%20(IDaaS)%20Solution.pdf.

[457] United States, Transportation Security Administration, "TSA Biometrics Roadmap: For Aviation Security & Passenger Experience", September 2018, https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf, 17-18:

> TSA will work with industry partners to define requirements, interfaces, and standards for aviation security touchpoints across the passenger experience (e.g., bag drop, checkpoint) against the backdrop of aviation stakeholders' regulatory obligations to verify passenger identity. Solution providers and aviation security partners will benefit from consistent requirements (e.g., for passenger throughput) and common standards for accuracy, throughput, data exchange, and cybersecurity. Interfaces and standards for front-end solutions will enable an extensible, futureproofed architecture to support a variety of concepts and processes.

[458] See also discussion in Section 2.5, beginning at p 96, above.

capability will be available to some private sector entities for identity verification purposes.[459] The objective of extending access to private sector entities is to increase identity assurance and facilitate cost savings.[460] Private sector entities may only use the IMS if identity verification is reasonably necessary for a particular function and on the basis of individual consent,[461] although it appears as though consent will not necessarily need to be express and freely given in all instances.[462] The IMS is only available to private sector entities to verify individual identity claims, while a more invasive IMS facial recognition service capable of identifying unknown individuals based on their facial image will only be available to the public sector.[463] Functionally, private sector entities will be able to query the facial verification service with a facial image and a name or other identifier and the IMS will return a 'match' or 'no match' outcome.[464] Examples of anticipated uses include verifying a new customer's identification documents when seeking to open a new bank account or phone plan, or to verify the identity of employees working with sensitive information.[465]

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 the backbone of a *de facto* general purpose national 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.

[459] The IMS legislation defines "non-government entity" to include private sector entities: *IMS Bill*, section 4: "non-government entity"; *IMS EM*, paras and 34-35.

[460] *IMS EM*, Attachment A, Statement of Compatibility with Human Rights, p 48: "Providing for access by local government authorities and non-government entities is necessary to achieve the legitimate objectives of providing for the FVS, in particular in relation to fighting identity crime. Through their day-to-day service delivery activities, local government authorities and non-government entities handle a significant volume of identification documents for the purpose of verifying identity. For this reason, these organisations play a significant role in detecting the use of stolen or fraudulent identification documents and fighting identity crime. In order to achieve the objectives of the Bill to fight identity crime, it is necessary for these front-line organisations to have access to the fast and secure face-matching provided by the FVS."

[461] *IMS Bill*, paragraph 10 (2)(d), and paragraphs 7(3)(a) "verification of the individual's identity is reasonably necessary for one or more of the functions or activities of the … non-government entity" and (b) "the individual has given consent for the local government authority or non-government entity to use and disclose, for the purpose of verifying the individual's identity, the identification information about the individual that is included in the request."

[462] *IMS EM*, paras 106, 104 and 232 "The concept of 'consent' in the Bill is intended to have the same meaning as in the Privacy Act. ... It is intended to include express consent or implied consent."

[463] The 1:1 verification capability (the Face Verification Service) generally available through the IMS initiative is available to qualifying non-government entities (*IMS Bill*, paragraph 10(2)(d), while the 1:N Face Identification Service is limited to public sector entities (*IMS Bill*, sub-section 8(2).

[464] *IMS, EM*, para 145: "It should be noted that under access policies and data sharing agreements supporting the implementation of the Bill, any private sector usage of the FVS will only return a 'match' or 'no match' response, without returning images or biographic information about the person."

[465] *IMS EM*, para 155; Henry Belot, "Government's Facial Recognition Scheme Could be Abused, Lawyers Warn", *ABC News*, May 3, 2018, https://www.abc.net.au/news/2018-05-03/facial-recognition-scheme-could-be-abused-law-council/9723494: "Private companies, [Home Affairs deputy secretary Maria Fernandez] said, would only be able to access the data for verification purposes and with that person's consent. The information is valuable for businesses like banks or telecommunication companies to prevent identity fraud. Other companies may also want to check someone working with sensitive information is who they say they are."; Elise Thomas, "Coalition Could Allow Firms to Buy Access to Facial Recognition Data", *The Guardian*, November 25, 2017, https://www.theguardian.com/technology/2017/nov/26/government-could-allow-firms-to-buy-access-to-facial-recognition-data;

Section 3. Legal & Human Rights Implications

The invasive potential of facial recognition, including its propensity for racial bias, presents several potential challenges even in the border context, where higher levels of coercion are often legally acceptable. A full legal analysis of all potential facial recognition border control implementations is beyond the scope of this report. Instead, this section attempts to convey a general impression of what legal considerations might be triggered by facial recognition in different border control contexts.

Section 3.1 provides a detailed outline of facial recognition-related legal considerations that might arise at border crossings. The general legal principles it draws upon are described in much greater detail in Section 3.2, which provides a description of the broader legal and human rights landscape in the border control context. This broad and general description is punctuated by select case studies intended to provide some additional indication of how these principles would apply to different facial recognition systems. Finally, Section 3.3 closes with examples of different legislative treatment that various facial recognition implementations have operated under in a few select jurisdictions.

3.1 Facial Recognition: Summary of Legal Considerations

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.[466] Even the ephemeral creation and use of a facial template has been held to involve the capture, storage and sensitive processing of personal

[466] *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).

data.[467] 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.[468] 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.[469] More generally, the capabilities of facial recognition systems emphasize the intrusive nature of the technology.[470]

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.[471] 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.[472] Facial recognition also provides a critical means for applying algorithmic decision-making tools directly to travellers. These various decision-making tools are equally susceptible to racial biases, compounding any biases in the underlying facial recognition algorithm.[473]

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.[474] Travellers may also find themselves referred to more intrusive border

---

[467] *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.

[468] *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.

[469] 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. See also: *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).

[470] *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."

[471] *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.

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

[473] 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*.

[474] *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.

control screening mechanisms as a result of these biases, exacerbating racial stereotypes and the stigma experienced by members of marginalized communities when crossing borders.[475] 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,[476] putting at risk the life and security of asylum seekers whose identities are erroneously rejected,[477] or damaging the reputation of falsely identified migrants.[478] 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.[479] 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.[480] 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.[481] This is inconsistent with transparency policies requiring agencies to publicly explain all components of a high-

[475] *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."

[476] 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.

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

[478] 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/.

[479] 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."; 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."

[480] 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.

[481] 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.

impact automated decision-making system and describe the nature of the training data that was used in its generation.[482] 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.[483] 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.[484]

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.[485] 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.[486] At times, consent is relied upon as a means of operating outside or beyond a clear grant of authorization.[487] However, the border control context is highly coercive and, as a result, freely given and meaningful consent is difficult,[488] if not impossible, to achieve.[489] In other instances, private sector tools

[482] 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.

[483] 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/.

[484] 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).

[485] 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,

[486] 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 choosing not to decide the matter on the ground of legality, however); *R (Bridges) v Chief Constable of South Wales Police*, [2020] EWCA Civ 1058, para 91.

[487] 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; 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; 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; See also: 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; 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.

[488] 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); European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018, pp 33, 80; see discussion in Section 1.6, p 59, above.

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.[490]

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.

[489] 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.

[490] 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; 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.

3.2 Privacy & Human Rights at the Border

Facial recognition systems can have wide-ranging legal implications in border control contexts, and a complete analysis of these is beyond the scope of this report. However, there are some general legal principles that would guide the assessment of any such implementation, and these are outlined in this section. Specifically, the statutory framework for border control decision-making is articulated, legal safeguards for privacy and detention are described, the scope of substantial and procedural review is briefly outlined, and the framework for assessing substantive equality is detailed. Case studies are included to provide some indication of how the legal principles described might apply in practice.

3.2.1 Border Control Objectives & Primary Legislative Instruments

The two primary border control agencies are the Canada Border Services Agency (CBSA) and Immigration, Refugees and Citizenship Canada (IRCC). CBSA is the frontline border control agency, with officers situated at Canadian ports of entry/exit. The Canadian Air Transport Security Authority (CATSA) is also tasked with securing elements of the air transportation system, and is primarily responsible for pre-boarding security screening of travellers and baggage, including at international and domestic ports of entry/exit.

Border control decisions are largely governed by two core statutory frameworks: the *Customs Act* and the *Immigration and Refugee Protection Act* (IRPA).[491] The *Customs Act* governs import and export of various goods, including through the imposition of customs tariffs or through the prohibition of certain goods. The IRPA and its related regulations govern immigration into Canada, controlling who can or cannot enter the country under what conditions.

In addition to these core statutory regimes, the *Canadian Air Transport Security Authority Act*, the *Aeronautics Act*, and related regulations govern air traffic security.[492] Under the *Canadian Air Transport Security Act*, CATSA is the primary entity responsible for ensuring that screening of air travellers and their belongings is carried out in an efficient, effective and consistent manner, as well as the consistency of some other air transport security functions.[493] The *Canadian Aviation Security Regulations*, for example, are issued to "enhance preparedness for acts or attempted acts of unlawful interference with civil aviation and to facilitate the detection of, prevention of, response to and recovery from acts or attempted acts of unlawful interference with civil

[491] *Customs Act*, RSC 1985, c 1 and *Immigration and Refugee Protection Act*, SC 2001, c 27.

[492] *Canadian Air Transport Security Authority Act*, SC 2002, c 9, s 2; *Aeronautics Act*, RSC 1985, c A-2; *Canadian Aviation Security Regulations, 2012*, SOR/2011-318.

[493] *Canadian Air Transport Security Authority Act*, SC 2002, c 9 s 2, section 6.

aviation."[494] They create a framework for traveller screening where it is tied to this aviation security objective.[495] CATSA currently operates as a crown corporation, yet plans have been announced to privatise the agency.[496] Given that CATSA's activities remain fundamentally a government function in character, the *Charter* should continue to apply.[497]

The *Canada Border Services Agency Act* outlines the mandate and operational parameters of the CBSA and its exercise of powers.[498] Many of these powers are circumscribed by the CBSA's itemized program legislation, which includes the *Customs Act*, the *Immigration and Refugee Protection Act*, and a range of food and health safety instruments.[499] The CBSA's primary mandate is to provide "integrated border services" in relation to the flow of persons and goods across borders,[500] and when achieving the objectives of its program legislation, the Agency mostly operates in a border control context.[501]

The specific statutory provisions that would underpin facial recognition in a border control context will vary depending on the specific implementation. The most common implementation will rely on general powers in the *Customs Act* and *Immigration and Refugee Protection Act* ("IRPA") which authorize information gathering for the purposes of controlling the goods and persons who enter or leave Canada. For example, section 11 of the *Customs Act* compels any

[494] *Canadian Aviation Security Regulations, 2012*, SOR/2011-318, section 191).

[495] *R v Neyazi*, 2014 ONSC 6838, paras 84-88 and 103-118 ("The *Aeronautics Act* governs state action in an airport setting. Under the *Act*, CATSA agents can only conduct a physical search of luggage where they have obtained the passenger's consent and the passenger is present, or if the passenger is unaccounted for. This demonstrates an objective recognition that passengers maintain some privacy interest in their luggage. Where CATSA screening tests are negative for the presence of any object or substance that may threaten airport security, passengers do not expect the contents of their luggage will be physically searched without consent. Where the state actor is a police authority and not CATSA, the police must have legal grounds to search a passenger or the passenger's luggage."). See also: *R v Chehil*, 2010 NSSC 255, paras 122-137, re'vd but aff'd on this point in 2011 NSCA 82, paras 34-35; rev'd but aff'd on this point in 2013 SCC 49, paras 12 and 59.

[496] Brett Ballah, "Sunday Reader: How Privatizing CATSA Became the Only Choice", March 24, 2019, *Western Aviation News*, https://westernaviationnews.com/2019/03/24/sunday-reader-catsa-replacement-privatization-federal-budget-2019/; Canadian Air Transport Security Authority, "About Us", last accessed August 7, 2020, https://www.catsa-acsta.gc.ca/en/about-us: "[CATSA] is a Crown corporation responsible for securing specific elements of the air transportation system – from passenger and baggage screening to screening airport workers… CATSA is governed by a Board of Directors with its operations directed by a Senior Management Team."

[497] Robert J Sharpe & Kent Roach, "The *Charter of Rights and Freedoms*", *6th Ed.* (Toronto: Irwin Law, 2017), pp 107-108: "Institutions such as hospitals, regarded as private for certain purposes, may still be subject to the *Charter* where they act on behalf of the government or in furtherance of some specific governmental policy or program. ... the test for determining whether entities such as hospitals, public broadcasters, or the post office are "government" for purposes of the *Charter* turns on the degree to which there is significant control by government ministers or their officials in their day-to-day operations and on the extent to which the entity acts on the government's behalf or furthers some specific governmental policy or program." See also *Douglas/Kwantlen Faculty Assn v Douglas College*, [1990] 3 SCR 570.

[498] *Canada Border Services Agency Act*, SC 2005, c 38, sections 5 and 12.

[499] *Canada Border Services Agency Act*, SC 2005, c 38, section 2, "program legislation". In 2014, the CBSA was tasked with administrating over 90 statutes, regulations and international agreements: Canada Border Services Agency, "What to Expect: Secondary Services and Inspections", *Canada Border Services Agency*, BSF5146-2014-E, https://www.cbsa-asfc.gc.ca/publications/pub/bsf5146-eng.pdf.

Some program legislation imposes regime-specific safeguards. For example, section 9(2)(c) of the *Agriculture and Agri-Food Administration Monetary Penalties Act*, SC 1995, c 40, some CBSA decisions are subject to review by the Canadian Agricultural Review Tribunal, potentially including a very limited mandate to reverse CBSA border control decisions if based on racial profiling, discriminatory stereotyping or other abusive criteria: *Ortiz v Canada (Canada Border Services Agency)*, 2013 CART 23. In practice, however, the evidentiary basis for establishing this form of abusive discrimination may be difficult to establish: *Bougachouch v Canada (CBSA)*, 2013 CART 20, rev'd *Canada (Attorney General) v Bougachouch*, 2014 FCA 63.

[500] *Canada Border Services Agency Act*, SC 2005, c 38, section 5.

[501] However, courts have recognized that 'border control' is a concept that "is broader than mere geographic boundaries" and, as a result, border-related powers can extend beyond the territorial boundary: *R v Jacques*, [1996] 3 SCR 312; *R v Le*, 2019 ONCA 961.

traveller entering Canada to present to truthfully answer any questions asked by of them by a border control official acting within their duties, while paragraph 99(1)(a) authorizes border control officials to examine any goods that have been imported into Canada.[502] Similarly, under sub-section 18(1) of the *IRPA*, any person seeking to enter Canada must submit to an examination in order to determine their eligibility for entry whereas sub-section 16(1) of IRPA requires migration applicant to answer any questions put to them truthfully and to produce any relevant documents required.[503]

The *Customs Act* places specific prohibitions on the use or disclosure of customs information.[504] Customs information includes any information relating to one or more persons that is obtained or prepared for the purposes of the *Customs Act* and itemized related statutory instruments.[505] Generally speaking, customs information can only be used by government officials for purposes of statutory instruments the CBSA or the Minister of Public Safety are authorized to enforce, including the *Immigration and Refugee Protection Act* and the *Customs Act* itself.[506] The *Customs Act* itemizes additional situations in which customs information may be disclosed to individuals, to government officials and to law enforcement.[507]

3.2.2 Privacy & Detention at the Border

The state is typically granted broad latitude to interfere with *Charter* rights when carrying out border control functions at ports of entry and exit. Canadian courts have held that it is common for travellers to be subjected to routine questioning and searches of their effects when crossing borders.[508] The stigma of being subjected to a search is therefore less than would be the case if an individual were singled out and searched in another context, as are the attendant privacy implications.[509] Similarly,

[502] *Customs Act*, RSC 1985, c 1, section 11 and paragraph 99(1)(a). Sections 98 and 99.2 and paragraph 99(1)(e) authorize comparable examinations at border control checkpoints on the basis of a reasonable suspicion that a traveller carrying evidence of customs contraventions or contraband on their person.

[503] *Immigration and Refugee Protection Act*, SC 2001, c 27, sub-sections 16(1) and 18(1). Section 139 authorizes border control officials to search travellers if there are reasonable grounds to believe that the traveller has failed to reveal their true identity and that the search will reveal documents relevant to determining their identity or reasonable grounds to believe that the search will reveal documents that could be used to commit certain immigration offences (smuggling, human trafficking or immigration-related document fraud). In some contexts, the IRPA recognizes broader powers with respect to non-citizens such as foreign nationals or permanent residents (see for example sub-section 16(3)).

[504] *Customs Act*, RSC 1985, c 1, sub-section 107(2).

[505] *Customs Act*, RSC 1985, c 1, sub-section 107(1).

[506] *Customs Act*, RSC 1985, c 1, sub-section 107(3): "An official may use customs information: (a) for the purposes of administering or enforcing this Act, the Customs Tariff, the Excise Act, 2001, the Special Imports Measures Act or Part 2 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act or for any purpose set out in subsection (4), (5) or (7); (b) for the purposes of exercising the powers or performing the duties and functions of the Minister of Public Safety and Emergency Preparedness under the Immigration and Refugee Protection Act, including establishing a person's identity or determining their inadmissibility; or (c) for the purposes of any Act or instrument made under it, or any part of such an Act or instrument, that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to enforce, including the Agriculture and Agri-Food Administrative Monetary Penalties Act, the Feeds Act, the Fertilizers Act, the Health of Animals Act, the Plant Protection Act, the Safe Food for Canadians Act and the Seeds Act."

[507] *Customs Act*, RSC 1985, c 1, 107 (4) – (6).

[508] See Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide", *The Citizen Lab and the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)*, May 2018, https://cippic.ca/uploads/20180514-shining_a_light.pdf.

[509] *R v Simmons*, [1988] 2 SCR 495.

courts have recognized that security concerns related to air travel (including domestic air travel) justify an attenuated expectation of privacy protection.[510]

Generally speaking, border control officials are able to detain and search all travellers without requiring any specific subjective or objective rationale as justification.[511] The 'border control' context generally governs travellers regardless of whether they are foreign nationals, temporary residents, permanent residents or citizens and upon exit and entry.[512] However, courts have recognized that foreign nationals and, to a lesser degree, temporary and even permanent residents do not have an unqualified right to be in Canada and, as a result, may be subject to different treatment in a border control context from citizens and asylum seekers.[513]

The latitude granted to border officials is not, however, limitless. While jurisprudence continues to evolve, the more intrusive a border search and the more attenuated its link to customs and immigration objectives that justify it, the more safeguards are imposed by the *Charter*, including the right to be free from unreasonable search and seizure, the right to counsel upon being detained, and the right to be free from arbitrary detention:

- Where a search extends beyond what is required to achieve customs or immigration objectives, border agencies must premise any interference with a reasonable expectation of privacy on objective grounds.[514]

[510] *R v Truong*, 2002 BCCA 315. Note, however, that the latitude courts grant the state at international borders is directly related to the state's interest in controlling the goods and persons who can enter Canada and privacy expectations are decisively lower than in other domestic settings, including domestic settings that raise security-related concerns: *R v Chehil*, 2013 SCC 49; *R v Jackman*, 2016 ONCA 121.

[511] *R v Simmons*, [1988] 2 SCR 495; *Dehghani v Canada (Minister of Employment and Immigration)*, [1993] 1 SCR 1053.

[512] *R v Nagle*, 2012 BCCA 373, paras 42-44.

[513] *Cha v Canada (Minister of Citizenship and Immigration)*, 2006 FCA 126.

[514] *R v Kwok*, [1986] 31 CCC (3d) 196 (ON CA)(with respect to the right to counsel: "…throughout the immigration and customs procedures, a person is under the restraint that he will not be allowed to enter Canada unless there is satisfactory compliance with the questioning and the searches provided for by the relevant statutes such as the Customs Act, R.S.C. 1970, c. C-40, and the Immigration Act, 1976, supra. These restraints do not by themselves constitute a detention within the meaning of the Charter. … there must be some action on the part of the immigration authorities to indicate that the restriction on an immigrant's freedom has gone beyond that required for the processing of his application for entry and has become a restraint of liberty … In my opinion, the appellant was detained when Leithead, having filled out the detained convocation letter, invited the appellant and Lam into his office with the intention of advising them of his decision to detain them."); *Canada (Citizenship and Immigration) v Gutierrez*, 2015 FC 1198, paras 44-45, aff'd on this point, 2016 FCA 211, para 54: "*Dehghani* involved an examination that was conducted at a port of entry for the purpose of processing an application for entry and determining the appropriate procedures that should be invoked in order to deal with an application for Convention refugee status. In other words, it was the sort of routine information gathering exercise that both parties agree does not give rise to a right to counsel. That is not this case. In this case, the information gathering stage was over. The officer had already determined the correct procedure and referred the Respondents' claims to the RPD for determination."; *Dehghani v Canada (Minister of Employment and Immigration)*, [1993] 1 SCR 1053; *Ha v Canada (Minister of Citizenship and Immigration)*, 2004 FCA 49, para 54; *R v Bialski*, 2018 SKCA 71, (in *obiter*), paras 108-109; *R v LE*, 2019 ONCA 961, paras 69-70: "But s.16(3) does not limit the subject matter of the search. It allows the CBSA officer to obtain 'any evidence' so long as that evidence is obtained to establish the subject's identity or determine compliance with the *IRPA*. ... They sought evidence from the LG Nexus cell phone in the appellant's possession on arrest, to determine the appellant's compliance (or lack thereof) with the *IRPA*, having information that could support a reasonably grounded belief the appellant was obstructing her removal from Canada."

See also: *United States v Cano*, (2019)(border searches of electronic devices are limited in looking for contraband, and cannot search for evidence of past or future crimes, including border-related crimes, without reasonable grounds); Steven Penney, "'Mere Evidence'? Why customs Searches of Digital Devices Violate Section 8 of the *Charter*", (2016) 49(1) UBC L Rev 485.

Similar considerations can arise in relation to security screening of luggage in the context of domestic travel: *R v Chehil*, 2013 SCC 49, para 59; *R v Crisby*, 2008 NTLD 185, paras 18-20 ("Obviously searching or screening the accused's bags for the presence of drugs does not fit into the category of purposes for which screening was authorized under the *Canadian Aviation Security Regulations*.").

- Where an individual is targeted based on particularized suspicion of criminal wrongdoing a border inspection may no longer be routine, attracting greater stigma and potentially giving rise to a reasonable expectation of privacy while triggering other rights such as the right to counsel and the right to silence.[515]
- Privacy incursions that are more intrusive (such as strip searches) must be premised on individualized grounds and cannot be conducted on a randomized or generalized basis, whereas even greater intrusion (such as X-rays and other intrusive bodily searches) may trigger additional safeguards such as the right to counsel and the right to demand a review from a senior border control officer.[516]
- Even routine and random generalized screening might be unconstitutional if it can be proven that individuals were singled out and targeted on the basis of discriminatory markers such as race, gender or religion,[517] while detention may no longer be considered

[515] *R v Simmons* [1988] 2 SCR 495, para 35: "At the time of the search the appellant was quite clearly subject to external restraint. The customs officer had assumed control over her movements by a demand which had significant legal consequences."); *R v Jones*, [2006] 81 OR (3d) 481 (ONCA), paras 23-24 and 41- 42; *R v Sinclair*, 2017 ONCA 287, paras 9-11 (in the context of assessing the right to counsel upon detention in border settings); *R v Jackman*, 2016 ONCA 121, (in *obiter*), paras 26-27. See also: *Dehghani v Canada (Minister of Employment and Immigration)*, [1993] 1 SCR 1053, generally and in particular para 118: "factual situations which are closer or analogous to criminal proceedings will merit greater vigilance by the courts"; *R v Nagle*, 2012 BCCA 373, paras 72-81 (routine questioning, including regarding potential criminality, is permitted while a border control officer forms a concrete suspicion of criminal wrongdoing).

See also: *R v Appleton*, [2011] 97 WCB (2d) 444 (ONSC), para 12 ("Officer Crawford said he was "looking for information" when he examined the cell phone. To me, this is an investigation conducted in furtherance of arrest and not a search for goods. As such, the officer has stepped out of the protection of the umbrella provided by the *Customs Act* and into the provisions of the *Charter*, where a search warrant would be required by a police officer conducting a similar search."; *United States of America v Almadi*, 2017 ONSC 3446, para 51.

In the domestic travel context, see: *R v Chehil*, 2010 NSSC 255, paras 122-137, aff'd on this point in 2011 NSCA 82, paras 34-35; aff'd on this point in 2013 SCC 49, paras 12 and 59 (a travellers' reasonable expectations of privacy are diminished with respect to security screening at domestic airports, but not with respect to general police investigations).

[516] *R v Simmons* [1988] 2 SCR 495, paras 27-28 51 & 54; *R v Monney*, [1999] 1 SCR 652, para 44 and 48 ("A second important distinction between the circumstances of this appeal and those present in *Stillman* is that the customs officers, in detaining the respondent in this case and subjecting him to a passive 'bedpan vigil', were not attempting to collect bodily samples containing personal information relating to the respondent. Cory J. in *Stillman* expressed particular concern that the actions of the police in gathering DNA evidence violated the respondent's expectations of privacy in using his body to obtain personal information."); *R v Hardy*, [1995] 103 CCC (3d) 289 (BCCA), paras 57-61.

See also: *United States v Cotterman*, (2013) 709 F.3d 952 (US, 9th Circuit, *en banc*).

[517] *R v Smith*, [2004] 26 CR (6th) 375 (ONSC), paras 29 and 34: "*Simmons*, and the related cases I have referred to, dealt with issues of search and seizure and detention and the right to counsel. They did not deal with the phenomenon of racial profiling. While all persons passing through customs may be subject to being scrutinized and searched, that does not diminish the potential affront to human dignity that occurs when someone is singled out for scrutiny on the basis of their race. It does not follow from the fact that a customs inspector does not need a reason to refer a person for secondary examination, that reliance upon race as a basis for doing so can be ignored. In my view, the potential affront to human dignity involved in the use of race in this way implicates the interests protected by s. 7. It calls for an analysis of whether race is being used in a manner that breaches the principles of fundamental justice, in the circumstances of the particular case. If there is no legitimate reason to use race to select an individual for scrutiny, the principles of fundamental justice will have been contravened. This will always be so in the case of racial profiling."); *R v Simpson*, 2017 ONSC 491, para 46: ("I am not aware of any appellant court decision on the issue of racial profiling and a person's referral to secondary inspection. However, in my consideration of this third party record application I will accept the principle of law that, despite the line of authorities as represented by *R. v. Simmons*, if racial profiling can be established as the reason for sending someone to secondary inspection, that person's *Charter* rights may have been violated."). In the domestic context, see: *R v Neyazi*, 2014 ONSC 6838.

See also: *R v Dudhi*, 2019 ONCA 665, paras 56-66 ("There are passages in the case law that can be taken to suggest that racial profiling does not occur unless there is no reasoned foundation for the suspect selection or subject treatment other than race or racial stereotyping. In other words, if there is other information that would meet the required legal standard – whether that required legal standard is "reasonable suspicion" [also known as "articulable cause"] or "reasonable grounds" – racial profiling does not exist even if race or racial stereotypes contribute to suspect selection or subject treatment. … This is not the law. … A body of law that permits officers to exercise their power when subjectively, their decisions are influenced by race or racial stereotypes, has little to commend it. Moreover, it would undermine other relevant interests at stake to accept that racial profiling does not occur even when race or racial stereotypes influence a decision, unless there is no reasonable foundation for that decision. In *Peart*, Doherty J.A. explained in simple terms, at paras. 91 and 93, why racial profiling is "wrong". It is "offensive to fundamental concepts of equality and … human dignity". It not only undermines effective policing by misdirecting resources and alienating members of the community, it "fuels negative and destructive racial stereotyping". This mischief, including the offence against equality and human dignity, operates whenever race or racial stereotypes contaminate decision-making by persons in authority." See also: *Peart v Peel Regional Police Services Board*, [2006] 43 CR (6th) 175 (ONCA).

> 'routine' if arbitrarily applied to members of marginalized groups with a stigmatizing history of forced interactions with the state.[518]

The intrusiveness of a border control screening activity is central to assessing the level of protection travellers can enjoy under the *Charter* in border areas.

Where a search must be premised on reasonable grounds and some form of individualized suspicion, the reasonable grounds assessment cannot be mechanical or formulaic. The search must be premised on legitimate and case-specific objective indicia of suspicion or probability that a given search will yield information relevant to the lawful purpose that animated it.[519] Indicia are not legitimate if they are discriminatory in character, rely on stereotypes, or rely on immutable characteristics of a traveller—racial profiling is not permitted.[520]

State agencies may access surveillance capabilities created in a border control context where no constitutionally protected reasonable expectation of privacy is implicated.[521] The sensitivity of the personal information being obtained in this manner is a central consideration when assessing whether prior judicial authorization will be required or not.[522]

Additionally, courts have placed limits on the conditions under which state agencies can receive personal data from private commercial companies. Specifically, obtaining sensitive personal information from commercial companies in the absence of clear lawful authorization can violate the *Charter's* prohibition of unreasonable search and seizure.[523]

Finally, practices at the Canadian border can implicate human rights frameworks abroad, and

---

Courts have also generally held that detention does not occur, in a constitutional sense, unless border control activities progress beyond 'routine screening' (*R v Nagle*, 2012 BCCA 373, para 52). However, courts have recently affirmed that race-related considerations might act as aggravating factors when assessing whether detention has occurred in non-border contexts (*R v Le*, 2019 SCC 34). If it can be shown that certain marginalized groups are systemically subjected to particularly aggressive and disproportionate screening at borders, this might elevate the constitutional relevance of some screening activities that are typically considered 'routine' when applied to members of racialized groups, and impact (*R v Le*, 2019 SCC 34, para 97: noting that "a common and shared experience of racialized young men: being frequently targeted, stopped, and subjected to pointed and familiar questions" affects the constitutional assessment of whether a detention has occurred or not). See also: *R v Thompson*, 2020 ONCA 264, para 63 ("Here, the appellant's race would contribute to a reasonable person's perception in all the circumstances that he was detained.").

[518] *R v Le*, 2019 SCC 34, para 109-110.

[519] *R v Chehil*, 2013 SCC 49, para 40-1; *R v Le*, 2019 SCC 34, para 78: "… racial profiling is primarily relevant under s. 9 when addressing whether the detention was arbitrary because a detention based on racial profiling is one that is, by definition, not based on reasonable suspicion."

[520] *R v Chehil*, 2013 SCC 49, para 43.

[521] *R v Flintroy*, 2018 BCSC 1692, paras 32-34 and 26, 28, 29, 30, 35-36, 37, 38; *R v Spencer*, 2014 SCC 43, paras 60-65; *R v Chehil*, 2009 NSCA 111, paras 36-38, 41, 45-46, 48-49 and 55; *R v Jarvis*, [2002] 3 SCR 757; *R v Quesnelle*, 2014 SCC 46. See also: *R v AM*, 2008 SCC 19, para 76; *R v Kang-Brown*, 2008 SCC 18, para 58; 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.

[522] *R v Flintroy*, 2018 BCSC 1692, paras 1 and 4; *R v Baldovi*, 2016 MBQB 221, para 20. See also: *Gaughran v United Kingdom*, Application No 45245/15, February 13, 2020, (ECtHR, 1st Section), paras 69, 85-86.

[523] *R v Spencer*, 2014 SCC 43.

undermine Canada's ability to access important security-related personal information relating to travellers.[524]

While biographic data such as facial photos and biometrics have long played a role in border control contexts, facial biometrics are increasingly recognized as sensitive in character in light of their high potential for intrusive, surreptitious and systematic identification.

Privacy Act at the Border

In general, the *Privacy Act* permits border control entities to collect personal information only if it relates directly to a lawfully authorized operating program or activity.[525] The Treasury Board of Canada Secretariat's (TBS) Directive on Privacy Practices further limits the collection (and creation) of personal information to instances where it is "demonstrably necessary" for an operating program or activity.[526] Absent consent, personal information can generally only be used and disclosed by border control entities for purposes that are consistent with those that animated its initial collection.[527] In addition, border control agencies have adopted additional policies and guidelines which guide the practices of their officers.[528] Except to the extent that these amount to interpretations of the *Privacy Act* or another underlying legal instrument, policies and guidelines are not legally binding and can be changed by TBS or a border control agency at any time.[529]

---

[524] 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. Similarly, it should be stated that the databases with which the PNR data is cross-checked must be reliable, up to date and limited to databases used by Canada in relation to the fight against terrorism and serious transnational crime.")

[525] *Privacy Act*, RSC 1985, c P-21, section 4; *Canada (Union of Correctionnel Officers) v Canada (Attorney General)*, 2019 FCA 212, paras 38 and 40.

[526] *Privacy Act*, RSC 1985, c P-21, paragraph 71(1)(d); Treasury Board of Canada Secretariat, Directive on Privacy Practices, effective as of May 6, 2014, section 6.2.8; *Union of Canadian Correctional Officers*, 2016 FC 1289, para 139: "…as part of the parliamentary business for the Act's reform, the Department of Justice took the position that section 4 need not be amended to include a necessity test because the test was already contained therein. The Department of Justice's legal representative provided the following explanation: "[t]he Treasury Board guidelines have said this expression "unless it relates directly" should mean a necessity test. Arguably, that's the only legal interpretation that's possible. If we say you shall not collect information unless it directly relates to a program, then basically it's saying you can't collect information you don't need".

[527] *Privacy Act*, RSC 1985, c P-21, section 7, subsection 8(1) and paragraph 8(2)(a); *Bernard v Canada (Attorney General)*, 2014 SCC 13, paras 30-31; 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, para 73.

[528] For example, the Canada Border Services Agency has adopted multiple policies and guidelines for screening travellers. These policies and guidelines are informed by the *Customs Act*, the *Privacy Act*, and the court's *Charter* jurisprudence.

[529] *Sauvé v Canada (Attorney General)*, 2016 FC 401, para 140 (TBS directives are administrative in nature and cannot change what is required by the *Privacy Act*); *Union of Canadian Correctional Officers*, 2019 FCA 212, para 40; 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, paras 22, 111-115 and 119:

> We note that the CBSA's Enforcement Manual requires that officers support their decisions by recording the indicators that provided *reasonable grounds* for the examination or search. It is problematic when there is no clear justification on record to support the secondary examinations of the complainants and the specific grounds that led the BSOs to believe at the time that the devices contained evidence of a contravention of CBSA-mandated legislation and justified examination. Moreover, our Office is unable to independently confirm the specific circumstances of those examinations or to determine whether there was in fact a clear link between the grounds relied on and a potential contravention of customs-related legislation that would support the progression of the examination and the searches of the complainants' digital devices. ... it is our conclusion that the Policy on its own has not proven an effective means of ensuring that examinations and searches of digital devices respect individuals' privacy rights.

In the border context, collection must be demonstrably linked to an underlying statutory or regulatory purpose.[530] Searches authorized by the *Customs Act*, for example, must be linked to a customs-related purpose.[531] Where the CBSA screens travellers who seek entry into Canada to determine national security threats, it cannot over-collect personal information where there is no evident connection to assessing the individual target.[532] Where an individual is a legitimate target of border control scrutiny, personal information of other individuals cannot be collected or used unless it directly relates to the specific target's assessment.[533] Additionally, if domestic law enforcement agencies disclose personal information to border control officials it must be 'consistent' with the policing objectives that animated its collection – mental health information collected by police officers is generally inconsistent with border control objectives and cannot be disclosed in the absence of a related risk to public safety.[534]

While consent is not an over-riding obligation in the *Privacy Act*, it plays a central role. Collection of personal information is not contingent on consent, but information must be collected directly from individuals wherever possible and individuals must be informed of the purpose for which the information is being collected.[535] Consent also plays a role where information will be used or disclosed for purposes that are inconsistent with those that animated its initial collection.[536] Consent must be based on information that is provided in a sufficiently timely manner as to allow individuals to make meaningful choices.[537] The form of consent may be implied, but must be express where the sensitivity of the information and the reasonable expectations of the individual indicate that disclosure would not be anticipated absent express notification.[538] Consent must also be freely given, in the absence of

[530] Office of the Privacy Commissioner of Canada, "Global Affairs Canada Fails to Demonstrate it Authority to Collect Personal Information Contained in Diplomatic Passports", *Complaint under the Privacy Act*, March 29, 2019, paras 11-14.

[531] 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, paras 26: "The CBSA submitted that paragraph 99(1)(a) of the *Customs Act* allows BSOs to examine any goods that have been imported into Canada on a no-threshold basis (i.e., without reasonable grounds) for customs-related purposes in order to ensure compliance with the laws administered or enforced by the CBSA."

[532] 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, para 16.

[533] 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 15-16: "CBSA collects and retains personal information that is not directly related to or demonstrably necessary for the objectives of the program. ... This included income tax records and social media information for individuals living at the same address as the individual referred for further examination. In approximately a third of case files that we reviewed we found evidence of social media and open source collection. In some of these cases, printouts of entire social media pages including lists of associates, postings, and photos of targets as well as their spouses, children and/or friends had been added to NTC files."

[534] 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 (facial images of all British Columbia drivers' license holders cannot be used to conduct a 1:N facial recognition comparison in order to identify an unknown individual on request of law enforcement as the *Freedom of Information and Protection of Privacy Act* only permits public bodies to use information that is specifically responsive to a law enforcement request in the absence of a court order).

[535] *Privacy Act*, RSC 1985, c P-21, section 5.

[536] *Privacy Act*, RSC 1985, c P-21, section 7, subsection 8(1) and paragraph 8(2)(a); *Bernard v Canada (Attorney General)*, 2014 SCC 13, paras 30-31; 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, para 73.

[537] 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.

[538] Office of the Privacy Commissioner of Canada, "TV Show Raises Numerous Questions of Consent", *Complaint under the Privacy Act*, June 6, 2016, paras 38-40.

constraint or duress.[539] As interactions with the CBSA are often coercive in nature, additional steps must be taken to ensure consent is meaningful and, in some contexts, it may not be possible to obtain freely given consent at all.[540]

The *Privacy Act* and related TBS policies also require adequate safeguards to avoid unauthorized use or disclosure of personal information.[541] These safeguards must be commensurate with the sensitivity of the data, the level of risk that the data will present a compelling target to internal or external actors, and the level of potential harm that might result if unauthorized access occurs.[542]

The *Privacy Act* also requires a measure of accuracy where personal information is being used by a border control agency. Where analytical tools are used as a means of identifying individuals for enhanced scrutiny, these tools require a measure of accuracy, otherwise the program may over-collect personal information if individual targets are disproportionately misidentified.[543] In addition, sub-section 6(2) of the *Privacy Act* requires that government institutions "take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible."[544] Accuracy becomes important when data about individual travellers is enrolled or used for the purpose of making border control decisions.[545] Further, analytical tools, including automated decision-making tools, used in a border control context should

[539] Office of the Privacy Commissioner of Canada, "TV Show Raises Numerous Questions of Consent", *Complaint under the Privacy Act*, June 6, 2016, paras 90 and 96.

[540] 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: "our Office questioned whether such consent is given freely, and whether individuals who are the subject of an interaction with the CBSA are in the best frame of mind to provide valid consent. For instance, individuals from countries with different legal systems may feel that they have to comply with uniformed individuals and have no choice but to sign documents presented to them. Moreover, individuals being detained or facing the prospect of deportation may not be in the best frame of mind to provide informed and free consent. ... due to the coercive nature of being detained by the CBSA, individuals that are detained may not have a clear frame of mind to provide truly voluntary consent."

[541] Office of the Privacy Commissioner of Canada, "Statistics Canada: Invasive Data Initiatives Should be Redesigned with Privacy in Mind", *Complaint under the Privacy Act*, December 9, 2019, para 124;); Treasury Board of Canada Secretariat, Directive on Privacy Practices, effective as of May 6, 2014, sections 6.2.19-6.2.23; Treasury Board of Canada Secretariat, Directive on Security Management, effective as of July 1, 2019; Treasury Board of Canada Secretariat, Policy on Government Security, effective as of July 1, 2019.

[542] Office of the Privacy Commissioner of Canada, "Statistics Canada: Invasive Data Initiatives Should be Redesigned with Privacy in Mind", *Complaint under the Privacy Act*, December 9, 2019, paras 124-125 and 134-135; 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.

[543] 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: CBSA must use an accurate success rate when calibrating scenario-based assessment tools: "without specifically aligning some of its measurement criteria to confirmed national security outcomes, CBSA cannot demonstrate that the personal information collected for purposes of the [Scenario-Based Targeting] program is necessary and proportionate for national security risk assessment purposes." See also: Opinion 1/15, *Draft Agreement Between Canada and the European Union – Transfer of Passenger Name Record Data*, July 26, 2017 (CJEU, Grand Chamber), para 172.

[544] *Privacy Act*, RSC 1985, c P-21, sub-section 6(2). Note that the *Privacy Act* defines "personal information" as information about an identifiable individual "that is recorded in any form", whereas "administrative purpose" is defined, in relation to an individual's personal information, as "the use of that information in a decision making process that directly affects that individual" (section 3). A purposive reading of these two terms suggests that the *Privacy Act* is intended to capture more than information-gathering and record-keeping (see: *Ewert v Canada*, 2018 SCC 30, para 42. Reading the broad definition of personal information (which can include information that is recorded *in any form*) in combination with the intent to capture information being used in decision-making processes (an intent that is included the definition of 'administrative purposes') and that even information that is stored only temporarily would be captured if it is included in a decision-making process.

[545] *HJ Heinz Co of Canada Ltd v Canada (Attorney General)*, 2006 SCC 13, para 22: "As is clear from the parliamentary debates at the time the Acts were introduced, Parliament intended the new, comprehensive access to information and privacy legislation to increase government accountability in two ways: ... second, by strengthening the rights of individuals to know "how personal information will be used . . . that the information used for decision-making purposes is accurate . . . and that information collected by government institutions is relevant to their legitimate programs and operations": *House of Commons Debates*, vol. VI, 1st Sess., 32nd Parl., January 29, 1981, at pp. 6689-91, Second Reading of Bill C-43 by the Hon. Mr. Francis Fox, then Minister of Communications."

be carefully calibrated to ensure they lead to accurate results if relied upon to make decisions that affect individual travellers.[546] As racial bias is a well-documented phenomenon in many automated decision-making tools,[547] it becomes particularly incumbent on state agencies to take active steps in order to avoid such known inaccuracies.[548]

TBS' Directive on Automated Decision-Making guides the use of automated tools by border control officials.[549] The Directive intends to reduce the risks of deploying automated decision-making tools within the Government of Canada, in part by encouraging more accurate, consistent and interpretable usage of automated decision-making tools.[550] Its obligations apply to "any system, tool, or statistical models used to recommend or make an administrative decision" about an individual,[551] with 'decision making systems' defined broadly to encompass any technological system that assists or replaces the judgement of human decision-makers.[552]

---

[546] *Ewert v Canada*, 2018 SCC 30, (interpreting *Corrections and Conditional Release Act*, SC 1992, c 20, subsection 24(1), which imposes comparable accuracy obligations).

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

[548] *Ewert v Canada*, 2018 SCC 30, paras 49 and 50:

> The trial judge noted that the CSC had long been aware of concerns regarding the possibility of psychological and actuarial tools exhibiting cultural bias. Such concerns had in fact led the CSC to conduct research into the validity of certain actuarial tools other than the impugned tools when applied to Indigenous offenders and to cease using those other tools in respect of Indigenous inmates. … As well, research into the validity of at least some of the impugned tools when applied to members of cultural minority groups had been conducted in other jurisdictions.
>
> By contrast, the trial judge found that the CSC had not taken any action to confirm the validity of the impugned tools and that it had continued to use them in respect of Indigenous offenders without qualification. This was true despite the fact that research by the CSC into the impugned tools, though challenging, would have been feasible. In these circumstances, the trial judge concluded that the CSC's failure to take *any* steps to ensure the validity of the impugned tools when applied to Indigenous offenders did not meet the legislated standard set out in s. 24(1) of the *CCRA*.

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:

> But internal CBSA communications hint at problems that may affect kiosk machines' even-handedness in dealing with different ethnicities. Emails obtained by CBC News through Access to Information discuss the roll-out of electronic inspection booths at Canadian airports and early efforts to measure their accuracy. CBC News also obtained a report entitled "Facial Matching at Primary Inspection Kiosks" that discusses 'false match' rates. False matches include 'false positives'…and 'false negatives'...
>
> While all discussion of Canadian findings was redacted from the documents CBSA released, the documents do include some revealing emails in which the evaluation team discusses U.S. findings. Referring to articles that suggested facial recognition technology had serious problems reading darker-skinned faces, one of the evaluation team wrote: "I thought maybe it was just the press making a fuss and actually it's not an issue. However … you do see that…NIST has found a similar bias. "The false match rate shows a massive increase for visa images when the imposter is from South Asia region, etc." "I never thought it was just press," responds a colleague, sharing a link with another US study that shows that facial recognition algorithms are wildly more inaccurate when dealing with dark-skinned travellers than with light-skinned travellers, and are also worse at assessing women."

[549] Treasury Board of Canada Secretariat, Directive on Automated Decision-Making, effective as of April 1, 2019. The Directive applies to CBSA as well as the Department of Citizen and Immigration: Directive, section 9.1; Treasury Board of Canada Secretariat, Directive on Service and Digital, effective April 1, 2020, section 6.1; *Financial Administration Act*, RSC 1985, c F-11, section 2 "Departments" and "Departmental Corporation", Schedule I (Department of Citizenship and Immigration) and Schedule II (Canada Border Services Agency). Note that this tool has been criticized for failing to provide meaningful protection for the human rights it implicates: 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).

[550] Treasury Board of Canada Secretariat, Directive on Automated Decision-Making, effective as of April 1, 2019, section 4.1.

[551] Treasury Board of Canada Secretariat, Directive on Automated Decision-Making, effective as of April 1, 2019. Administrative decision is defined (Appendix A: "Administrative Decision") broadly to include: "[a]ny decision that is made by an authorized official of an institution…pursuant to powers conferred by an Act of Parliament or an order made pursuant to a prerogative of the Crown that affects legal rights, privileges or interests. "However, it is notable that the Privacy Act's accuracy obligations apply even more broadly, encompassing any 'administrative purpose' which the Act defines as "the use of personal information…in a decision making process that directly affects [an] individual.": Privacy Act, RSC 1985, c P-21, sub-section 6(1) and 3 "Administrative Purpose".

[552] Treasury Board of Canada Secretariat, Directive on Automated Decision-Making, effective as of April 1, 2019, Appendix A: "Automated Decision System".

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.[1] However, automated facial recognition capabilities are intrusive in general, and categorically more intrusive then the routine collection of a facial image.[2]

Questionable privacy practices have been documented in the creation of datasets used to train many commercial comparison algorithms.[3] Arguably, the latitude granted to border control agencies does not extend to their use of algorithmic tools generated in violation of privacy laws.[4]

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.[5] Algorithms that can systematically search all images when seeking a match are also more intrusive than those that operate by comparing two known images.[6] 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, there are persistent challenges that are particularly pronounced with respect to some demographic groups. 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.[7]

Facial recognition errors can impact substantial traveller and community interests (e.g. by contributing to discriminatory traveller enhanced screening referral and irreversibly contributing to lasting loss of dignity by perpetuating racial prejudices), 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.[8] 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.[9]

Some facial recognition proposals would extend beyond border control objectives. For example, a Canadian pilot program testing a mobile device-based facial recognition 'passport' is ultimately envisioned to be a "*de facto* universal identification system".[10] Where 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.

[1] 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."

[2] 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."

[3] See discussion in Section 1.1.2, at pp 52-55, above.

[4] 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.

[5] 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; 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, p 6, above.

[6] *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."

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

[8] 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.

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

[10] *Alberta v Hutterian Brethren of Wilson County*, 2009 SCC 37, para 40. See Box 12, at p 95, above, for a description of the World Economic Forum's Known Traveller Digital Identity proposal and Canada's ongoing pilot.

Higher impact decision-making tools require border control officials to notify the public of its anticipated use, and provide an explanation of its components, of how its outcomes are incorporated into the broader decision-making process, and a description of the training data that was used in its generation.[553] Higher impact automated decisions must also be subject to human intervention before becoming final, and subject to expert peer-review.[554] The level of impact is determined in relation to the rights of individuals or communities, the health or well-being of individuals or communities, the economic interests of individuals, entities or communities, and the ongoing sustainability of an ecosystem.[555] An algorithmic decision-making impact assessment tool released by TBS as a means of implementing this Directive emphasizes the following relevant factors as indicative of higher impact:[556]

- The anticipated impact of the system on rights and freedoms of individuals and communities;
- Whether vulnerable or marginalized communities will be implicated by the system;
- The use of personal information by the system;
- Private sector involvement in collecting the data that trained the system;
- Whether the algorithmic process is opaque and difficult to explain or interpret to human decision-makers or impacted individuals;
- The analysis of unstructured data such as video and images;
- The duration of the impact and its reversibility; and
- Use will be in a context of intense public scrutiny due to broader systemic privacy concerns.

[553] 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.

[554] Treasury Board of Canada Secretariat, Directive on Automated Decision-Making, effective as of April 1, 2019, Section 6.2 and Appendix, sections 6.3.9 – 6.3.10 and Appendix C, "Human-in-the-Loop for Decisions".

[555] Treasury Board of Canada Secretariat, Directive on Automated Decision-Making, effective as of April 1, 2019, Section 6.2 and Appendix B.

[556] 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/.

Other relevant criteria include whether the system is interconnected with other technology systems, the reversibility and duration of any impact resulting from an automated decision, and whether data from connected devices will be relied upon.

Border Control Objectives Achieved Through Private Sector Instrumentality

While a comprehensive legal analysis of the use of facial recognition by border-related private sector entities is beyond the scope of this paper, the private sector frequently plays a central role in implementing public sector objectives at the border. In this context, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) plays a role in governing what information a private company can disclose to a border control agency. Private sector data processing obtained in violation of PIPEDA may be more likely to attract *Charter* protection when collected by the state. More generally, private sector conduct that occurs at the direction of the government can more generally be a factor in assessing the scope of constitutional protection.

PIPEDA generally prohibits private sector entities from collecting, using or disclosing personal information without consent. Organizations can imply consent in strictly defined circumstances.[557] Where implying consent, organizations need not explicitly bring a practice to an individual's attention, but may detail the practice in a privacy policy or related generalized notice. Private companies cannot imply consent where the collection, use or disclosure in question raises a residual risk of harm, where individuals would not reasonably expect the processing in question or where the personal data at issue is sensitive.[558] While some categories of information are generally considered sensitive, the analysis is contextual and dependent on the nature, purpose and recipients of an information exchange.[559]

Section 7 of PIPEDA exempts specific situations from PIPEDA's general consent obligation, including where the information was made publicly available under certain narrowly defined contexts,[560] and situations that contemplate a role for government agencies.[561]

[557] *Royal Bank of Canada v Trang*, 2016 SCC 50, para 23.

[558] Office of the Privacy Commissioner of Canada, Guidelines to Obtaining Meaningful Consent, May 2018. Risk of harm is defined as a material residual risk that bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage or loss of property might occur despite steps taken to minimize the likelihood that such harm could occur.

[559] *Royal Bank of Canada v Trang*, 2016 SCC 50, paras 36-37 and 49.

[560] *Wansink v TELUS Communications Inc*, 2007 FCA 21, paras 19-23; *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, paragraphs 7(1)(d), 7(2)(c.1) and 7(3)(h.1).

[561] *Wansink v TELUS Communications Inc*, 2007 FCA 21, paras 19-23; *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, paragraphs 7(1)(b) and (e), (2)(a) and (d), (3)(c), (c.1), (c.2).

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.[1] 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.[2]

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.[3] 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.[4]

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.[5]

Finally, implied consent is not available where sensitive data or high risk processing are a factor.[6] 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.[7]

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.[8] 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.[9] The limitless and systematic identification capability provided by Clearview is therefore disproportionate and hence inappropriate.[10]

---

[1] 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."; PIPEDA Report of Findings #2015-002, June 5, 2015.

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

[3] 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); 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.

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

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

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

[7] 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. See also: United States, Department of Homeland Security, Customs and Border Protection, "Privacy Impact Assessment: Publicly Available Social Media Monitoring and Situational Awareness Initiative", March 25, 2019, DHS/CBP/PIA-058, p 1: "CBP uses Internet-based Platforms, as well as government and commercially developed tools that provide a variety of methods for monitoring social media sites." Note that the program does not currently rely on facial recognition, but rather on key word searches.

[8] 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.

[9] 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.

[10] *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.

The collection, use and disclosure of publicly available information is generally subject to PIPEDA's privacy protections.[562] PIPEDA permits private companies to process publicly available personal information without consent only under narrow circumstances. The 'publicly available' character of personal information can also impact the form of consent individuals can reasonably expect in relation to its collect, use and disclosure.[563] The general premise is that personal information appearing in some types of explicitly itemized publications can be used without consent for the primary purposes that animated its publication.[564] While border control agencies will rarely have recourse to seek personal

[562] *Regulations Specifying Publicly Available Information*, SOR/2001-7; Order in Council, Regulations Specifying Publicly Available Information, PC 2000-1777, December 13, 2000, Regulatory Impact Analysis Statement:

> The basic premise underlying this Regulation is that the collection, use and disclosure of publicly available personal information for commercial purposes should be subject to the same fair information practices as are required by the Act for all other personal information.

This is consistent with Canadian law more broadly, which generally recognizes that privacy protections persist despite the public availability of information: *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62, para 27: "It goes without saying that by appearing in public, an individual does not automatically forfeit his or her interest in retaining control over the personal information which is thereby exposed. This is especially true given the developments in technology that make it possible for personal information to be recorded with ease, distributed to an almost infinite audience, and stored indefinitely."; *R v Jarvis*, 2019 SCC 10, para 37; Kristen Thomasen & Suzie Dunn, "R v Jarvis—Location, Equality, Technology: What is the Future of Privacy?", December 18, 2018, *Robson Crim Legal Blog*, https://docs.wixstatic.com/ugd/bab59a_f4e02851683142778d3211805317a4c9.pdf; Tamir Israel, "Digital Privacy in Emerging Contexts: Lessons from the SCC's Evolving Section 8 Jurisprudence", *The Winston Report*, Winter 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3335518.

[563] *Royal Bank of Canada v Trang*, 2016 SCC 50.

[564] Order in Council, Regulations Specifying Publicly Available Information, PC 2000-1777, December 13, 2000, Regulatory Impact Analysis Statement:

> As a rule, individuals are able to decide for themselves with whom they will share personal information and under what circumstances. However, some personal information enters into the public sphere through a variety of channels, often without the knowledge or consent of the individual. ... This personal in-formation is made public for a specific and primary purpose ...
>
> Privacy concerns relate to the manner in which the information is made publicly available, e.g., whether there are any controls or limitations placed on who may collect and use it and how (increasingly access is possible to an electronic record rather than to the traditional hard copy. Internet access is more common as well.). The fact that individuals have continuing expectations of privacy for some publicly available personal information is seldom ad-dressed. Another privacy issue is the growing use that commercial organizations make of this information for purposes that often have nothing to do with the primary purpose for which the information was made public, i.e., to contact individuals and offer them products or services. There is also an increasing tendency to collect and use publicly available information to create comprehensive personal profiles of the individual, including their consumption habits, lifestyles and personal histories for a variety of other purposes, including employment decisions. Many, if not most, of these secondary uses are presently carried out without the knowledge or consent of the individual. A final issue is that, with few rules to govern publicly available personal information, organizations have little incentive to consider obtaining consent from the individual.
>
> The Regulation is based on a recognition that some personal information is publicly available for a legitimate primary purpose, often with the individual's tacit agreement (e.g., the telephone directory, announcements). In these circumstances, it is reasonable to allow organizations to collect, use and disclose this information without adding the requirement to obtain consent. To require an organization to obtain consent to use this information for its primary purpose would not contribute to the protection of the individual's privacy, would add to the organization's costs and could frustrate some public policy purpose. However, it is also reason-able to insist that any purpose other than the primary one should be subject to the consent requirement. ... Using the criteria of consistency with the primary purpose or tacit consent as the basis for the Regulation of publicly available personal information strikes the appropriate balance between the individual's right of privacy and the business need for information.

See also: *Royal Bank of Canada v Trang*, 2016 SCC 50, paras 36-37 and 49: financial data is generally sensitive, but a bank can imply consent to disclose a mortgage discharge statement where mortgage information is legally mandated to be public for the primary purpose of informing would-be purchasers (including creditors) of any property encumbrance. However, the bank may only disclose this personal information where the recipient demonstrated the disclosure will be for the primary purpose that the information was legally published by establishing a legal interest in the property in question. *Royal Bank of*

information that is already publicly available from private companies, various automated decision-making tools rely on publicly available personal information in their creation and in their general operation.[565] Personal information obtained from public telephone directories, business directories, statutorily authorized registries or judicial decisions, however, may only be collected, used or disclosed for purposes directly related to those for which they appear in these respective publications.[566] Additionally, automated tools rarely rely solely on personal information that was voluntarily provided to the author of a traditional media publication such as a magazine, book or newspaper.[567]

Private entities such as airlines or private surveillance companies can rely on these exemptions to disclose personal customer information, but upon receiving a state agency request that is consistent with constitutionally protected reasonable expectations of privacy.[568] Reasonable expectations of privacy are more likely to be implicated where sensitive data or intrusive techniques are involved.[569]

PIPEDA can impact reasonable expectations of privacy more directly. Contractual clauses notifying individuals that their data might be disclosed to state agencies can impact how much privacy a customer can reasonably expect when a state agency asks a company to disclose that customer's data.[570] PIPEDA neutralizes the presence of these notifications by rendering these clauses unlawful—a customer would not reasonably expect a company to adopt an unlawful contractual clause.[571]

While the *Charter* does not typically apply to private action, laws such as PIPEDA protect constitutional values in private sector contexts and as a result are quasi-constitutional in nature.[572] PIPEDA can also

---

Canada v Trang, 2016 SCC 50, paras 36-37 and 49; and *AT v Globe24h.com*, 2017 FC 114, paras 75-76 and 78-79: "The CJC Model Policy discourages decisions that are published online to be indexed by search engines as this would prevent information from being available when the purpose of the search is not to find court records. ... The respondent's actions result in needless exposure of sensitive personal information of participants in the justice system via search engines."

[565] See, generally: 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).

[566] *Regulations Specifying Publicly Available Information*, SOR/2001-7, sections 1(a)-(d); Order in Council, Regulations Specifying Publicly Available Information, PC 2000-1777, December 13, 2000, Regulatory Impact Analysis Statement.

[567] *Regulations Specifying Publicly Available Information*, SOR/2001-7, sections 1(e); Order in Council, Regulations Specifying Publicly Available Information, PC 2000-1777, December 13, 2000, Regulatory Impact Analysis Statement. Note that the exception does include the electronic version of traditional media publications:

> As a rule, individuals are able to decide for themselves with whom they will share personal information and under what circumstances. However, some personal information enters into the public sphere through a variety of channels, often without the knowledge or consent of the individual. Examples include personal information that appears in telephone or other directories, public registries maintained by governments, public court records or that is published in the media. ... Several organizations questioned why the examples of publications "a magazine, book, or newspaper" were drawn from traditional rather than electronic media and whether "publication" included internet media. To clarify this point, the words "in printed or electronic form" have been added to the term "publication". ... Organizations should be able to infer from the context of most announcements and notices whether or not the individual in fact provided the information. If an organization is in doubt, it should not collect the information without consent. ... One organization suggested the Regulation is too restrictive and may interfere with freedom of expression, e.g., clipping services, indexes. However, these activities fall under the journalistic exclusion in the Act.

[568] *R v Spencer*, 2014 SCC 43.

[569] *R v Simmons* [1988] 2 SCR 495, paras 27-28 51 & 54; *R v Monney*, [1999] 1 SCR 652, para 44 and 48; *R v Hardy*, [1995] 103 CCC (3d) 289 (BCCA), paras 57-61. See also: *United States v Cotterman*, (2013) 709 F.3d 952 (US, 9th Circuit, *en banc*).

[570] *R v Gomboc*, 2010 SCC 55; *R v Chehil*, 2009 NSCA 111. Contrast: *R v Jones*, 2017 SCC 60, paras 42 and 45; *R v Orlandis-Hasburgo*, 2017 ONCA 64.

[571] *R v Spencer*, 2014 SCC 43; *R v Orlandis-Hasburgo*, 2017 ONCA 649, para 68-69, 97-104 and 111-115; *R v Jones*, 2017 SCC 60, paras 42 and 45.

[572] *Eastmond v Canadian Pacific Railway*, 2004 FC 852, para 100; *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2012 SCC 62, para 19 (finding Alberta's substantially similar 'Personal Information Protection Act' to be quasi-constitutional in nature); *Douez v*

bolster *Charter* protections. If a private company violates PIPEDA when seeking to address border control agency objectives, this can bolster the scope of *Charter* protection.[573] Private sector surveillance tools are also sometimes used in border control contexts.[574] Particularly where artificial intelligence tools are at issue, the creation or operation of these tools may be unlawful under PIPEDA. Artificial intelligence tools frequently rely on aggregating large volumes of data, and often this occurs without meeting consent obligations, in violation of PIPEDA.[575]

Finally, where state agencies rely on private companies to achieve specific public functions, this can impact the legality and constitutionality of government objectives more generally. It is particularly common for governments to rely on airlines to achieve various border control objectives. Where private companies seek out private information at the direction or request of border control agencies, this can trigger section 8 of the *Charter* even in the absence of explicit legislative obligations compelling airline compliance.[576] This is particularly so where there is considerable interaction between the private company and the border control agency, effectively rendering the private company an 'agent of the state'.[577] If legislative or regulatory obligations enlist airlines directly,[578] the *Charter* will apply to the legislation itself, and could also apply directly to airline decisions taken to achieve those legislative or regulatory obligations.[579] Generally speaking, the government cannot abrogate its *Charter* obligations by relying on a private company to achieve its border control objectives.[580]

Facebook Inc, 2017 SCC 33, paras 50, 59 and 104: (BC Privacy Act protects the quasi constitutional privacy rights of British Columbians): "Privacy legislation has been accorded quasi-constitutional status."; *Nammo v TransUnion of Canada Inc*, 2010 FC 1284; *AT v Globe24h.com*, 2017 FC 114, paras 93-100

[573] *R v Spencer*, 2014 SCC 43; *R v Jones*, 2017 SCC 60, paras 42 and 45; *R v Chehil*, 2009 NSCA 111, paras 26 and 28-29; *R v Orlandis-Hasburgo*, 2017 ONCA 649, para 111-112. Note that state agency conduct that violates other private rights can also impact the scope of *Charter* protection: *R v Le*, 2019 SCC 34, paras 44 and 136.

[574] See: 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. For a description and legal analysis of use of such tools by law enforcement agencies, 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).

[575] Office of the Privacy Commissioner of Canada, "Clearview AI Ceases Offering its Facial Recognition Technology in Canada", *Office of the Privacy Commissioner of Canada*, July 6, 2020, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/; Office of the Privacy Commissioner of Canada, "Commissioners Launch Joint Investigation into Clearview AI Amid Growing Concerns over Use of Facial Recognition Technology", February 21, 2020, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/; See also: *Patel v Facebook Inc*, Case No 18-15982 (9th Circuit, 2019) and discussion in Section 1.4, p 52, above and in 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), for more details.

[576] *R v Buhay*, 2003 SCC 30, paras 25-34; *R v Broyles*, [1991] 3 SCR 595; *R v Weir*, 2001 ABCA 181, paras 9-11.

[577] *R v Weir*, 2001 ABCA 181, paras 9-11; *R v Orlandis-Hasburgo*, 2017 ONCA 649, paras 21-36; *R v Marakah*, 2017 SCC 59, para 50; *R v Reeves*, 2018 SCC 56, para 46. See also: Daphne Gilbert, Ian R Kerr & Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers", (2007) 51(4) *Crim L Q* 469, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1302544.

[578] For example, see: *Exit Information Regulations*, SOR/2019-241, June 25, 2019.

[579] *Eldridge v British Columbia (Attorney General)*, ; *R v Buhay*, 2003 SCC 30, para 31 ("It may be that if the state were to abandon in whole or in part an essential public function to the private sector, even without an express delegation, the private activity could be assimilated to that of a state actor for *Charter* purposes.").

[580] Canada, Department of Justice, "Section 32(1)—Application of the Charter", *Charterpedia*, last updated June 17, 2019, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art321.html: "The Charter does not apply to non-governmental entities created by government for the purpose of legally enabling them to do things of their own choosing (such as private corporations, hospitals and universities) ... Governments cannot circumvent the Charter, however, simply by granting powers to non-governmental entities or by pursuing governmental initiatives through means other than the traditional mechanisms of government action."; Robert J Sharpe & Kent Roach, "The *Charter of Rights and Freedoms*", *6th Ed.* (Toronto: Irwin Law, 2017).

3.2.3 Judicial Review, Procedural Fairness & Rules of Evidence

Border control decisions are subject to substantive judicial review and procedural fairness obligations.[581] Where a border control determination implicated a traveller's life, liberty or security of the person, then procedural fairness obligations become elevated to constitutional stature and attract protection under section 7 of the *Charter* while additional principles of fundamental justice must also be respected.[582] The level of procedural safeguards that border control decisions will require is generally contingent on the significance of the decision and its potential impact on travellers' rights and interests, and the specific context of a given case.[583] The scope and rigour of substantive review will also depend on a range of factors, including the statutory context and the nature of the decision.[584]

In many border control contexts, laws will not trigger procedural fairness obligations or rigorous substantive review.[585] Border control officials owe no duty of procedural fairness with respect to routine border control screening, as the consequences for travellers are not sufficiently severe and because CBSA has the right to fully inspect all travellers.[586] More severe consequences, such as a risk of refoulement, attract procedural safeguard obligations that are fair and sufficient to protect implicated rights.[587] However, no specific procedural vehicle is guaranteed, whereas the bar is high for those seeking to demonstrate that a law or its application is grossly disproportionate, arbitrary or overbroad.[588]

Substantive fairness can also include a right to an impartial and independent decision-maker, the right to a fair hearing, the right to know the case one must meet, and the right to reasons justifying a

[581] 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.

[582] *Canada (Attorney General) v Bedford*, 2013 SCC 72, para 108-123; *Atawnah v Canada (Public Safety and Emergency Preparedness)*, 2015 FC 774, para 56, aff'd 2016 FCA 144.

[583] *Baker v Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817; *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65, paras 76-81; 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.

[584] *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65.

[585] For an overview of procedural fairness and judicial review considerations in the immigration context, with particular emphasis on the implications of automated systems, see: 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 47-54.

[586] *Dhillon v Canada (Attorney General)*, 2016 FC 456, paras 29-30, 37 and 41: "Referral to secondary examination as a result of the Previous Offender Process does not constitute an additional sanction, penalty or legal consequence. … While there is no doubt that the applicant subjectively views the inconvenience of frequent referrals for secondary examination as a significant negative consequence, that subjective view is not objectively sustainable in the context of port of entry examinations."

[587] *Singh v Minister of Employment and Immigration*, [1985] 1 SCR 177; *Atawnah v Canada (Public Safety and Emergency Preparedness)*, 2016 FCA 144, para 31; *Suresh v Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1, paras 115-119 ("deciding what procedural protections must be provided involves consideration of the following factors: (1) the nature of the decision made and the procedures followed in making it, that is, "the closeness of the administrative process to the judicial process"; (2) the role of the particular decision within the statutory scheme; (3) the importance of the decision to the individual affected; (4) the legitimate expectations of the person challenging the decision where undertakings were made concerning the procedure to be followed; and (5) the choice of procedure made by the agency itself").

[588] *Atawnah v Canada (Public Safety and Emergency Preparedness)*, 2016 FCA 144, para 27; *Charkaoui v Canada (Citizenship and Immmigration)*, 2007 SCC 9; *Ewert v Canada*, 2018 SCC 30, para 73.

decision.[589] As noted in a report by The Citizen Lab and the International Human Rights Program, automated decision-making tools can strain these procedural safeguards.[590] In many instances, the opacity of automated tools obscures the substantive basis of the decision and as a result border control officials may be hampered in their ability to meet their obligation to provide reasons and to inform travellers of the case they must meet if their rights are being assessed.[591]

Automated determinations can also supplant human judgement, undermining the right to an impartial and independent decision-maker.[592] Opaque mathematical determinations can lead to over-reliance by individual human decision-makers who are unaware of the factors relied upon by the automated tool in question and lack the technical capabilities to critique its outcomes.[593] Decision-makers are also precluded from fettering their own discretion, and must take into account the specific context and factors of each question to be resolved.[594] While it has been argued that some automated decisions may be no more than an application of 'institutional memory',[595] many automated decision-

[589] Canada, Department of Justice, "Section 7 – Live, Liberty and Security of the Person", *Charterpedia*, last updated June 17, 2019, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art7.html: "The following are procedural principles of fundamental justice that have been found to apply outside the criminal context: the right to a hearing before an independent and impartial tribunal (*Ruffo v. Conseil de la magistrature*, [1995] 4 S.C.R. 267 at paragraph 38; *Pearlman v. Manitoba Law Society Judicial Committee*, [1991] 2 S.C.R. 869, at 883; *Charkaoui* (2007), *supra*, at paragraphs 29, 32); the right to a fair hearing, including the right to State-funded counsel where circumstances require it to ensure an effective opportunity to present one's case (*G.(J.)*, *supra* at paragraphs 72-75 and 119; *Ruby, supra*, at paragraph 40); the opportunity to know the case one has to meet (*Chiarelli, supra*, at 745-46; *Suresh, supra* at paragraph 122; *May v. Ferndale Institution*, *supra*, at paragraph 92; *Charkaoui* (2007), *supra*, at paragraph 53), including, where the proceeding may have severe consequences, the disclosure of evidence (*Charkaoui* (2008) at paragraphs 56, 58; *Harkat, supra* at paragraphs 43, 57, 60); the opportunity to present evidence to challenge the validity of the state's evidence (*Suresh, supra* at paragraph 123; *Harkat, supra*, at paragraph 67); the right to a decision on the facts and the law (*Charkaoui* (2007), *supra*, paragraphs 29, 48); the right to written reasons that articulate and rationally sustain an administrative decision (*Suresh, supra*, at paragraph 126); and the right to protection against abuse of process (*Cobb, supra*, at paragraphs 52-53). The application of these principles is highly contextual, but it may be assumed that if they apply outside the criminal context, they apply with greater force in the criminal context."

[590] See: 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 47 *et seq*.

[591] *Canada (Minister of Employment and Immigration) v Chiarelli*, [1992] 1 SCR 711: individuals must be given "sufficient information to know the substance of the allegations against him, and to be able to respond."; *Charkaoui v Canada (Citizenship and Immigration)*, 2007 SCC 9, para 61: "the person must be given the necessary information, or a substantial substitute for that information must be found."

[592] 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,

[593] See: Jason Millar, "Five Ways a COVID-19 Contact-Tracing App Could Make Things Worse", *Policy Options*, April 15, 2020, https://policyoptions.irpp.org/magazines/april-2020/five-ways-a-covid-19-contact-tracing-app-could-make-things-worse/; Cosima Gretton, "The Dangers of AI in Health Care: Risk Homeostasis and Automation Bias", *Towards Data Science*, June 24, 2017, https://towardsdatascience.com/the-dangers-of-ai-in-health-care-risk-homeostasis-and-automation-bias-148477a9080f?gi=e7b5eb341e4a; Safiya Umoja Noble, "Algorithms of Oppression: How Search Engines Reinforce Racism", (New York: NYU Press, 2018) p 37, describes this deference in relation to algorithmic decision-making in the context of search engines: "… renderings are delivered to users through a set of steps (algorithms) implemented by programming code and then naturalized as "objective." One of the reasons this is seen as a neutral process is because algorithmic, scientific and mathematical solutions are evaluated through procedural and mechanistic practices …". See also discussion in Section 1.6, above.

[594] G. Régimbald & M. Estabrooks, "Administrative Law (2013 Reissue)", *Haslbury's Laws of Canada*, (Canada: LexisNexis Canada, 2013)(QL), Section IV 2(2)(b)(iii) Fettering Discretion, HAD-69. See also: *Canada (Attorney General) v Georgian College of Applied Arts and Technology*, 2003 FCA 199; *Grewal v Canada (Minister of Employment and Immigration)*, [1985] 2 FC 263 (FCA): "whether or not the explanation justifies the necessary extension must depend on the facts of the particular case and it would, in my opinion, be wrong to attempt to lay down rules which would fetter a discretionary power which Parliament has not fettered."

[595] *Dhillon v Canada (Attorney General)*, 2016 FC 456, para 40: "The Previous Offender Process essentially functions as part of CBSA's institutional memory. Its automation does not constitute a fettering of discretion because the process does not lead to automatic referrals to secondary examinations upon every attempted entry into Canada. Instead, the Previous Offender Process is designed to recognize future consistent compliance by decreasing the frequency of mandatory secondary examinations, presumably on the basis that compliance reflects a reduction in risk. This continued reduction in the frequency of automatic referrals through the Previous Offender Process demonstrates the latter's function as institutional memory: the longer Mr. Dhillon complies with the Act, the less likely that system will remember his Contravention at the time of Mr. Dhillon's entry into Canada."

making tools create sophisticated, multi-factor assessment processes that extend well beyond historic institutional criteria while the process of selecting specific criteria for assessment to the exclusion of others can, itself, be unreasonable, arbitrary or discriminatory.[596] These systems can have far-reaching implications if they become the *de facto* basis for decisions with serious impact in lieu of discretionary human decision-making.[597]

Some legal systems have embraced the use of biometric recognition as appropriate evidence of identity in judicial border-related processes. In the United Kingdom, for example, Eurodac matches have been held to provide sufficient evidence of identity to form a basis of refusal in migrant and asylum contexts.[598] Eurodac is a biometric border control system that has historically operated on the basis of automated fingerprint matching, but is being expanded to include facial recognition.[599] In its typical operation, Eurodac's automated fingerprint matches are supplemented with manual verification by a UK-based fingerprint expert.[600] Requiring human vetting of Eurodac matches mitigates to some degree any false positives that might result from shortcomings in the automated biometric matching process itself.[601]

However, it has also been held that where a Eurodac match & manual confirmation has occurred, these are 'determinative' and can only be overturned by "cogent evidence to the contrary."[602] Such deference extends not only to the matching process itself, but also to additional enrollment data, such as the time and place in which the biometric data was enrolled.[603] Further, impacted individuals are granted limited rights to challenge how the biometric data was enrolled or how the

[596] 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; Rashida Richardson, Jason Schultz & Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems and Justice", (2019) 94 *NYU L Rev Online* 192, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423; Sarah Myers West, Meredith Whitaker & Kate Crawford, "Discriminating Systems: Gender, Race, and Power in AI", April 2019, *AI Now Institute*; Safiya Umoja Noble, "Algorithms of Oppression", (NY: New York University Press, 2018); 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.

[597] 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.

[598] *RZ (Eurodac, Fingerprint Match, Admissible) Eritrea*, [2008] UKAIT 7 (UK Asylum & Immigration Trib); *YZ & Ors v Secretary of State for the Home Department*, [2011] EWHC 205 (UK QB, Admin), para 102: citing *RZ Eritrea*, with approval:

> … the Tribunal undertook a general assessment of the Eurodac system. It concluded that fingerprint evidence from the Eurodac system is admissible in evidence … generally as part of the examination of a claim to asylum. It also held (see [45]) that if there is a dispute as to a match, that must be a question of fact to be determined on the available evidence but, in the light of the evidence the Tribunal heard about the system and its accompanying safeguards, in its judgment "evidence of a match produced through the Eurodac and confirmed by [the Immigration Fingerprint Bureau in Lunar House] should be regarded as determinate of that issue in the absence of cogent evidence to the contrary". The Tribunal (at [50]) rejected the submission that there was any requirement for corroboration in respect of fingerprint evidence.

[599] European Union, Fundamental Rights Agency, "Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights", 2018; European Commission, Proposal for a Regulation on amending Regulation (EU) No 603/2013, COM(2016)272, https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-272-EN-F1-1.PDF.

[600] *RZ (Eurodac, Fingerprint Match, Admissible) Eritrea*, [2008] UKAIT 7 (UK Asylum & Immigration Trib).

[601] And where proof of this manual confirmation is absent, the credibility of a Eurodac match is more readily challenged: *Ahmadi v Secretary of State for the Home Department*, [2017] UKAITUR PA115102016 (UK Asylum & Immigration Trib), paras 20-21.

[602] *RZ (Eurodac, Fingerprint Match, Admissible) Eritrea*, [2008] UKAIT 7 (UK Asylum & Immigration Trib), para 45.

[603] *RZ (Eurodac, Fingerprint Match, Admissible) Eritrea*, [2008] UKAIT 7 (UK Asylum & Immigration Trib).

matching mechanism operates.[604] Finally, the fact of a Eurodac automated biometric match can continue to informally impact asylum decisions even after the underlying data has been deleted.[605] This is problematic given decision-makers' deference to opaque biometric matching processes which cannot be explained in a way that can be challenged using human logic. The UK Biometric Commissioner recently highlighted the problems that can result from such deference (in the criminal justice context):

> ... as systems develop their pattern-matching autonomously, it is no longer clear on what basis matching is being claimed and therefore difficult for courts to judge the veracity of evidential claims. Courts may accept matching claims if supported by expert endorsement or may require that it is verified by human judgement on the claimed matching. It is also possible that further technical development will allow machine learning systems to 'explain' how they have reached their judgements.[606]

This level of deference would be more problematic if applied to automated facial recognition systems, which are less accurate then automated fingerprinting but can still attract comparable levels of deference from human decision-makers.

In Canada, rules of evidence have recognized that some automated assessment and identification techniques can undermine the judicial fact-finding role and should be relied upon with caution or not at all. For example, in the criminal context, courts have rejected the submission of polygraph results because of the "human fallibility in assessing weight to be given to evidence cloaked under the mystique of science".[607] Human judgement has proven equally unreliable when called upon to weigh evidence from instruments held to be demonstrably precise and infallible.[608] Courts have permitted the evidentiary use of identification tools, but only with a substantial degree of caution. Facial recognition techniques raise similar challenges. When border control officials seek to identify a visa applicant or asylum seeker and query a facial recognition system, the system will typically provide 10-50 images of individuals who look similar to the traveller.[609] On the basis of this 'photo lineup', border control officials might

[604] *RZ (Eurodac, Fingerprint Match, Admissible) Eritrea*, [2008] UKAIT 7 (UK Asylum & Immigration Trib), para 45; *E v CIPO*, [2019] IEHC 39, paras 3 and 6.

[605] *E v CIPO*, [2019] IEHC 39, paras 4-5: A Eurodac match had been illegally retained longer than the statutory retention period and was relied upon by UK border control officials in their rejection of an asylum claim. A reconsideration of the asylum claim was ordered following the deletion of the Eurodac biometric data, but references to the fact the match had occurred were retained in the file. Despite this fact, UK border control officials claimed, and the court accepted, that the Eurodac match was not relied upon when affirming their rejection of E's asylum claim and ongoing knowledge of the Eurodac match was held not to have biased the UK border control official's final determination. See also: *Kamara v Secretary of State (Home Department)*, [2013] EWHC 959 (Admin), where the mere belief by UK border control agencies that a fingerprint match had occurred led to the detention of an asylum applicant.

[606] United Kingdom, Commissioner for the Retention and Use of Biometric Material, Annual Report 2018, June 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/812351/Biometrics_Commissioner_AR_2018_Print.pdf, para 22.

[607] *R v Béland*, [1987] 2 SCR 398, per La Forest, J, concurring, para 64, and per McIntyre, J, para 20.

[608] *R v St-Onge Lamoureux*, 2012 SCC 57, paras 28, 34-36 and 73.

[609] See descriptions of this mode of operation in Sections 1.2.2 and 1.3.1 at pp 26 and 34, above.

decide that the traveller is not who they claim to be.[610] Yet, in the criminal context, courts have recognized that photo lineups are an unreliable form of identification, and cautioned against their evidentiary use in the past.[611]

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.[1] 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.[2] Opacity regarding the underlying comparison mechanism and the 'scientific mystique' of automated biometric recognition create a presumption of accuracy that is 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.[3] Should this policy change,[4] 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.[5]

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.[6]

[1] 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; *Atawnah v Canada (Public Safety and Emergency Preparedness)*, 2016 FCA 144, para 31.

[2] 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."

[3] 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/.

[4] 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.

[5] For a critique of the European Union approach to fingerprint evidence in immigration contexts, see Section 1.6, above. 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."

[6] 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/.

[610] See Passport Canada, "Facial Recognition Application Project – Privacy Impact Assessment: Executive Summary", June 28, 2016, https://www.international.gc.ca/gac-amc/publications/atip-aiprp/assessments-evaluation/facial-faciale.aspx, and discussion at Section 1.2.2, p 28, above.

[611] *R v Hibbert*, 2002 SCC 39, paras 51-12; *R v* Phillips, 2018 ONCA 651, paras 44-48; R *v Faleh*, 2019 ABCA 441, paras 32-33 (trial judge was alive to the frailties of … eyewitness and photo lineup evidence); *R v Brown*, 2007 ONCA 71, paras 11-12 and 17; *R v Le (TD)*, 2011 MBCA 83, para 140; *R v Jones*, [2004] 193 OAC 56, para 11. See also: Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data", *Georgetown Law: Center on Privacy & Technology*, May 16, 2019, https://www.flawedfacedata.com/.

In other jurisdictions, the need for limits on evidentiary use of facial recognition matches has been recognized. Australia's government-wide Identity Matching Service (described in Box 13, above), recognizes as a guiding principle that facial recognition results should not be used as evidence of identity in court.[612] However, the Australian regime was criticized for not encoding this principle in the subsequent legislative regime introduced in support of its facial recognition solution.[613]

3.2.4 Equality Rights at the Border

Section 15(1) of the *Charter* recognizes the right to equal treatment, without discrimination on the basis of protected grounds. Section 15(1) of the *Charter* guarantees substantive equality, and should not be interpreted in an overly formalistic or technical manner.[614] Some courts have also suggested that severe discrimination such as racial profiling can offend the principles of fundamental justice, as protected by section 7 of the *Charter*.[615] Additionally, the *Canadian Human Rights Act* (CHRA) regulates discriminatory practices, including practices that differentiate adversely in the provision of a service or deny access to a service on the basis of a prohibited ground.[616]

To establish that a given practice is *prima facie* discriminatory in character, it must first be demonstrated that the practice distinguishes, excludes or prefers on the basis of a protected ground, particularly if the practice differentiates by perpetuating a prejudice or stereotype or otherwise contributes to discriminatory impact.[617] If *prima facie* discrimination is established on a balance of probabilities, the border control agency may any adverse treatment by demonstrating

---

[612] For example, paragraph 2.1(f) of the Australian Intergovernmental Agreement on Identity Matching Services (entered by Australian federal, state and territorial governments as a basis for legislative reforms) includes such a principle: "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." (Intergovernmental Agreement on Identity Matching Services, October 5, 2017, https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf).

[613] However, the proposal has been criticized for failing to encode this guiding principle in law: Government of Australia, Parliamentary Joint Committee on Intelligence and Security, Advisory Report on the Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-Matching Services) Bill 2019, Parliamentary Paper 458/2019, October 14, 2019, paras 2.68-2.69.

[614] *R v Kapp*, 2008 SCC 41; *Withler v Canada (Attorney General)*, 2011 SCC 12; and *Québec (Attorney General) v Alliance du personnel professionel et technique de la santé et des services sociaux*, 2018 SCC 17.

[615] *R v Smith*, [2004] 26 CR (6th) 375 (ONSC), paras 34 and 40.

[616] *Canadian Human Rights Act*, RSC 1985, c H-6, sections 4, 53 and 5.

[617] *Canada (Attorney General) v Davis*, 2017 FC 159, para 17; *Quebec (Commission des droits de la personne et des droits de la jeunesse) v Bombardier Inc (Bombardier Aerospace Training Center)*, 2015 SCC 39, para 35 see also paras 37-38 and 49; *O'Grady v* Bell, 2020 FC 535, para 47; *Moore v British Columbia (Education)*, 2012 SCC 61, para 33; *Kahkewistahaw First Nation v Taypotat*, 2015 SCC 30, paras 16-21; *Québec (Attorney General) v Alliance du personnel professionel et technique de la santé et des services sociaux*, 2018 SCC 17; and *Stewart v Elk Valley Coal Corp*, 2017 SCC 30, para 45.

See also: *Richards v Canada (Public Safety and Emergency Preparedness)*, 2007 FC 1100, paras 25 and 29 aff'd at 2008 FCA 341, paras 25, 28, 29 and 34; and *Feher v Canada (Public Safety and Emergency Preparedness)*, 2019 FC 335 (note that questions have been certified for appeal *ibid,* para 313); *YZ v Canada (Citizenship and Immigration)*, 2015 FC 892.

Note that while the approaches to determining discrimination under section 15 of the *Charter* and the *Canadian Human Rights Act* can inform each other, the two remain analytically distinct: *British Columbia (Public Service Employee Relations Commission) v BCGSEU*, [1999] 3 SCR 3, paras 47-49; *Fraser v Canada (Attorney General)*, 2018 FCA 223, para 44. Human rights statutes in general are generally interpreted consistently, barring legislative intent to the contrary: *Quebec (Commission des droits de la personne et des droits de la jeunesse) v Bombardier Inc (Bombardier Aerospace Training Center)*, 2015 SCC 39, para 31.

that it is justified under section 1 of the *Charter* or by establishing a '*bona fide*' justification under paragraph 15(1)(g) and sub-section 15(2) of the CHRA.[618]

Many border control activities can be challenged for failing to achieve substantive equality. While the CHRA does not apply to the mere enactment of a legislative provision,[619] many CBSA activities are 'services' subject to regulation under the CHRA if discriminatory in nature.[620] If an applicant can factually demonstrate they were singled out for an unusual level of scrutiny at a border control crossing on the basis of a protected ground, for example, then this might amount to a discriminatory practice within the meaning of the CHRA.[621] In addition, section 15 of the *Charter* applies to a broad range of government action, including "legislation, regulations, directions, policies, programs, activities and the actions of government agents carried out under lawful authority."[622] For example, border control laws denying procedural advantages to asylum seekers on the basis of prejudicial stereotypes associated with their country of origin have been found to constitute unjustifiable discrimination.[623]

The initial requirement for differential or adverse treatment is not an onerous hurdle.[624] Differential treatment need not be intentionally discriminatory, as neutral practices and policies can nonetheless operate in a manner that, in effect, perpetuates a stereotype or prejudice.[625]

---

[618] Note that the CHRA's '*bona fide* justification standard is distinct from the *Charter*'s section 1 proportionality assessment, in particular with respect to section 15(2) of the CHRA, which requires reasonable accommodation to the point of undue hardship if a discriminatory practice is to be justified: *Alberta v Hutterian Brethren of Wilson Colony*, 2009 SCC 37, paras 66 *et seq*.

[619] *Canada (Canadian Human Rights Commission) v Canada (Attorney General)*, 2018 SCC 31, paras 58 and 63; *Alberta v Hutterian Brethren of Wilson Colony*, 2009 SCC 37, paras 66 *et seq* (noting that the section 1 framework is more appropriate for justifying legislative actions of parliament than the justification framework adopted in some human rights instruments).

[620] *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.

For a useful taxonomy of immigration-related border control related points of administrative decision-making that may attract scrutiny on the basis of its discriminatory character can be found in: 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*, pp 23-28.

See also: *Abdi v Canada (Public Safety and Emergency Preparedness)*, 2018 FC 733 (a decision to refer an individual to an immigration admissibility hearing must be consistent with the *Charter* as it is discretionary and may lead to serious consequences). Note, however, that not all immigration decisions are discretionary to the same degree: *Cha v Canada (Minister of Citizenship and Immigration)*, 2006 FCA 126.

[621] *Richards v Canada (Public Safety and Emergency Preparedness)*, 2008 FCA 341, paras 28 and 32-34; *Canada (Attorney General) v Davis*, 2017 FC 159, paras 33 and 38.

[622] Canada, Department of Justice, "Charterpedia: Section 15 – Equality Rights", last modified June 17, 2019, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art15.html. See also: *Little Sisters Book and Art Emporium v Canada (Minister of Justice)*, 2000 SCC 69.

[623] *YZ v Canada (Citizenship and Immigration)*, 2015 FC 892, in general and specifically paras 118-120 (refusing a statutory appeal:

> The first question is whether the denial of an appeal to the RAD by DCO claimants creates a distinction based on an enumerated or analogous ground of discrimination. The Supreme Court has stated that "inherent in the word 'distinction' is the idea that the claimant is treated differently than others" (*Withler* at paragraph 62). … The differential treatment in paragraph 110(2)(d.1) of the *IRPA* is clearly a distinction on the basis of the national origin of a refugee claimant (*Canadian Doctors* at paragraphs 751-773). If the claimant comes from one of the countries designated under subsection 109.1(1) of the *IRPA*, his or her claim will be assessed without the potential benefit of or access to an appeal to the RAD, unlike claimants from non-DCO countries.

See also: *Feher v Canada (Public Safety and Emergency Preparedness)*, 2019 FC 335, (note that questions have been certified for appeal *ibid,* para 313), generally and specifically paras 27-32 (requiring asylum seekers from certain listed countries of origin to wait an additional 24 months before applying for an updated risk assessment prior to deportation violates section 15 of the *Charter*).

[624] *Québec (Attorney General) v Alliance du personnel professionel et technique de la santé et des services sociaux*, 2018 SCC 17, paras 26 and 71-73 and 83. However, it may be more difficult to establish this first step where government action is facially neutral: *Fraser v Canada (Attorney General)*, 2018 FCA 223, paras 40-42.

[625] *Quebec (Commission des droits de la personne et des droits de la jeunesse) v Bombardier Inc (Bombardier Aerospace Training Center)*, 2015 SCC 39, paras 40-42 (in

Additionally, prejudice need not be the sole basis for differential treatment in order for a practice to be discriminatory, it is sufficient to demonstrate that membership in a protected ground is a contributing factor.[626] Actions that are normally within the government's prerogative can be rendered unlawful or unconstitutional where these fail to meet the requirements of substantive equality.[627] For example, the government has no obligation to provide asylum seekers a re-evaluation of risk factors prior to deportation.[628] However, if a statutory scheme provides a right to pre-removal risk assessment, it cannot differentiate on the basis of stereotypes associated with national origin.[629] Similarly, border control agents may disproportionately target specific entities for enhanced scrutiny of imported materials, but may not do so in a manner that is systemically discriminatory without justification.[630]

Mathematically determined assessment criteria can be discriminatory in character even if applied systematically in a manner that, on average, is neutral. Mathematically developed employment qualification criteria may be discriminatory in character if the calibration pool used in their development is biased against members of protected groups or if the criteria impact members of protected groups in a disproportionate manner.[631] Additionally, the use of quantitative statistical assessment models in order to categorize individuals for more efficient border control processing can be unjustifiably discriminatory if it generally impacts on members of protected groups in proportions that are not mathematically accurate.[632] Where border control entities are obligated

---

the context of Quebec's provincial human rights instrument): "Not requiring proof of intention applies logically to the recognition of various forms of discrimination, since some discriminatory conduct involves multiple factors or is unconscious. The first element of discrimination is not problematic. The plaintiff must prove the existence of differential treatment, that is, that a decision, a measure or conduct "affects [him or her] differently from others to whom it may apply": *O'Malley*, at p. 551. This might be the case, for example, of obligations, penalties or restrictive conditions that are not imposed on others."; *Ontario Human Rights Commission v Simpsons-Sears*, [1985] 2 SCR 536, para 18; *Stewart v Elk Valley Coal Corp*, 2017 SCC 30, para 24; *Moore v British Columbia (Education)*, 2012 SCC 61, para 61.

[626] *Stewart v Elk Valley Coal Corp*, 2017 SCC 30, para 46 ("Second, I see no need to alter the settled view that the protected ground or characteristic need only be "a factor" in the decision. It was suggested in argument that adjectives should be added: the ground should be a "significant" factor, or a "material" factor. Little is gained by adding adjectives to the requirement that the impugned ground be "a factor" in the adverse treatment.")'; *Quebec (Commission des droits de la personne et des droits de la jeunesse) v Bombardier Inc (Bombardier Aerospace Training Center)*, 2015 SCC 39, paras 44-52.

[627] *Canada (Attorney General) v Davis*, 2017 FC 159 and *Canada (Attorney General) v Davis*, 2009 FC 1104, para 55, aff'd but not on this point, 2010 FCA 134. Whether the government exercises its legitimate prerogative in a differentiating manner is, however, a question of fact: *Richards v Canada (Public Safety and Emergency Preparedness)*, 2008 FCA 341, paras 29 and 34. See also: *Canadian Doctors for Refugee Care v Canada (Attorney General)*, 2014 FC 651, paras 740-742 (the government is not under any free-standing obligation to provide health care, but cannot offer health care in a manner that discriminates between asylum seekers based on country of origin).

[628] *Atawnah v Canada (Public Safety and Emergency Preparedness)*, 2016 FCA 144 (preventing asylum seekers from specific countries from seeking a pre-removal risk assessment for a period of 36 months following an initial risk assessment does not violate section 7 of the *Charter* and, moreover, requiring asylum seekers from listed countries to wait 36 months while other asylum seekers need only wait 12 months for a pre-removal risk assessment is not arbitrary).

[629] *Feher v Canada (Public Safety and Emergency Preparedness)*, 2019 FC 335, paras 29-32 and 257 (forcing asylum seekers from specifically listed countries to wait 36 months for a pre-removal risk assessment while other asylum seekers may seek a pre-removal risk assessment after only 12 months is differential treatment and, if conducted in a manner that perpetuates a stereotype, violates section 15's prohibition on discriminatory treatment).

[630] *Little Sisters Book and Art Emporium v Canada (Minister of Justice)*, 2000 SCC 69, para 120-121: "Targeting is not necessarily unconstitutional. The Customs Department is obliged to use its limited resources in the most cost-effective way. This might include targeting shipments that, on the basis of experience or other information, are more likely than others to contain prohibited goods. The evidence here, however, did not justify the targeting of Little Sisters and the three other lesbian and gay bookstores."

[631] *British Columbia (Public Service Employee Relations Commission) v BCGSEU*, (aerobic capacity testing criteria cannot be calibrated based on average performance levels that fail to take into account differences in aerobic capacity between men and women); *SGEU v Saskatchewan (Environment)*, 2018 SKCA 48 (fitness qualification criteria that is calibrated to exclude only 20% of woman and elderly male applicants is arbitrary, as some of these members of protected groups are likely on a balance of probabilities to be excluded despite being capable of doing the job).

[632] *Feher v Canada (Public Safety and Emergency Preparedness)*, 2019 FC 335, para 248.

to take into account the personal characteristics of individuals, even mathematically sound 'proxy' factors may be facially discriminatory if these impact detrimentally on members of protected groups.[633]

Discrimination that is systemic in nature can often be insidious and difficult to prove with direct evidence.[634] Racial profiling is a particularly insidious form of systemic discrimination.[635] Courts have recognized that travellers expect scrutiny at border crossings and are therefore less stigmatized by incursions that would be intrusive in other contexts. In justifying generalized intrusive search and detention, the Supreme Court of Canada found in *Simmons* that "No stigma is attached to being one of the thousands of travellers who are daily routinely checked in that manner upon entry to Canada and no constitutional issues are raised."[636] However, where members of protected groups are singled out in higher proportions this same scrutiny can exacerbate historical inequities and can be deeply humiliating.[637] For example, a recent study of racial profiling conducted by the Ontario Human Rights Commission summarized the stigmatizing impact that members of marginalized communities experience when crossing borders:

---

[633] *YZ v Canada (Citizenship and Immigration)*, 2015 FC 892, paras 123-126; *Feher v Canada (Public Safety and Emergency Preparedness)*, 2019 FC 335, para 249.

[634] *CN v Canada (Canadian Human Rights Commission)*, [1987] 1 SCR 1114; *Québec (Commission des droits de la personne et des droits de la jeunesse) v Bombardier Inc (Bombardier Aerospace Training Center)*, 2015 SCC 39, para 32.

[635] *Québec (Commission des droits de la personne et des droits de la jeunesse) v Bombardier Inc (Bombardier Aerospace Training Center)*, 2015 SCC 39, para 33:

> … The concept of racial profiling was originally developed in the context of proceedings brought against the police for abuse of power, but it has since been extended to other situations.
>
> > Racial profiling is any action taken by one or more people in authority with respect to a person or group of persons, for reasons of safety, security or public order, that is based on actual or presumed membership in a group defined by race, colour, ethnic or national origin or religion, without factual grounds or reasonable suspicion, that results in the person or group being exposed to differential treatment or scrutiny.
> >
> > Racial profiling includes any action by a person in a situation of authority who applies a measure in a disproportionate way to certain segments of the population on the basis, in particular, of their racial, ethnic, national or religious background, whether actual or presumed. [Emphasis added.]
>
> (Commission des droits de la personne et des droits de la jeunesse, *Racial Profiling: Context and Definition* (2005) (online), at p. 13; see also Ontario Human Rights Commission, *Policy and guidelines on racism and racial discrimination* (2005) (online), at p. 19.)

[636] *R v Simmons*, [1988] 2 SCR 495, para 27; *Dehghani v Canada (Minister of Employment and Immigration)*, [1993] 1 SCR 1053: "Another factor identified in *Simmons* as indicating that no detention of constitutional consequence occurs during routine questioning is the absence of stigma. Clearly, there is no stigma associated with a referral to a secondary examination. For instance, Canadian citizens who are not able to demonstrate their identity are often referred to a secondary examination for confirmation of their citizenship."; *R v Monney*, [1999] 1 SCR 652, para 38; *R v Jones*, [2006] 81 OR (3d) 481 (ONCA), para 33: "The Chief Justice's observation that those who are subject to routine questioning and searches suffer no "stigma" is germane to the self-incrimination analysis. The absence of any "stigma" attached to routine questioning and searches at the border tells me that where state action does not become more intrusive than routine questioning and searches, the relationship between the state and the individual cannot be characterized as either coercive or adversarial. The absence of coercion or an adversarial relationship suggests that the principle against self-incrimination does not demand the exclusion in subsequent proceedings of statements made during routine questioning and searches at the border."; *Dhillon v Canada (Attorney General)*, 2016 FC 456, paras 32 and 41: "This routine examination does not attract any stigma nor, as conceded by the applicant, does it amount to a detention in the Constitutional sense. ... While there is no doubt that the applicant subjectively views the inconvenience of frequent referrals for secondary examination as a significant negative consequence, that subjective view is not objectively sustainable in the context of port of entry examinations."

[637] As noted by the New York Southern District in its review of a 'stop and frisk' program carried out by the New York Police Department: "While it is true that any one stop is a limited intrusion in duration and deprivation of liberty, each stop is also a demeaning and humiliating experience. No one should live in fear of being stopped whenever he leaves his home to go about the activities of daily life. Those who are routinely subjected to stops are overwhelmingly people of color, and they are justifiably troubled to be singled out when many of them have done nothing to attract the unwanted attention. Some plaintiffs testified that stops make them feel unwelcome in some parts of the City, and distrustful of the police. This alienation cannot be good for the police, the community, or its leaders. Fostering trust and confidence between the police and the community would be an improvement for everyone." (*Floyd v City of New York*, (2013) 959 F.Supp.2d 540 (SDNY), remanded for appearance of impartiality: *Floyd v City of New York*, Case 13-3088 (2013, 2nd Circuit).

> We received many responses from South Asian, Muslim, Black and other racialized survey respondents about being racially profiled at airports and at border crossings.
>
> Respondents described being stopped, followed by air marshals, placed on "no fly" lists, having their names flagged or their identification questioned and not believed, without justification. We heard how these experiences made people feel humiliated and powerless, in part because they were often unable to get any information about why they were singled out. Not surprisingly, respondents reported that the stereotypes that contributed to their experiences of racial profiling are perceptions of Muslim, Brown and Arab people as Muslim terrorists.
>
> The vast majority of survey respondents reported being repeatedly selected for "random" screening and extra questioning, with many saying that it happened every or almost every time they travelled. Many said that this was in contrast to how they saw White travellers treated. Many said that their bags were searched, and some said that they were subjected to body searches. Respondents reported that they were asked inappropriate questions about their name, living situation in Canada, religious affiliation, and where their family is from. …
>
> 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."[638]

These subjective perceptions are premised on well-documented prejudices that often pervade and underlie security-related interactions between the state and members of marginalized groups.[639] These perceptions also inevitably form the context and lens through which many members of marginalized communities experience border control settings, and would tend to magnify the psychological stigma experienced by these individuals in border control interactions, impacting whether a particular interaction is experienced as 'routine' or not.[640]

---

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

[639] *R v Spence*, 2005 SCC 7, para 5 (in the context of jury selection): "The courts have acknowledged that racial prejudice against visible minorities is so notorious and indisputable that its existence will be admitted without any need of evidence. Judges have simply taken "judicial notice" of racial prejudice as a social fact not capable of reasonable dispute."); *R v Le*, 2019 SCC 34 in general and in particular para 83-84 and 97: "Evidence about race relations that may inform whether there has been a detention under s. 9, like all social context evidence, can be proved in legal proceedings by direct evidence, admissions, or by the taking of judicial notice. The realities of *Charter* litigation are that social context evidence is often of fundamental importance, but may be difficult to prove through testimony or exhibits … We do not hesitate to find that, even without these most recent reports, we have arrived at a place where the research now shows disproportionate policing of racialized and low-income communities."; *Ewert v Canada*, 2018 SCC 30, para 57 (in the context of assessment tools used by Correctional Services Canada and the need to address any bias in these tools with respect to first nation prisoners): "The mischief s. 4(g) was intended to remedy informs its interpretation. This mischief is, at least in part, the troubled relationship between Canada's criminal justice system and its Indigenous peoples. The alienation of Indigenous persons from the Canadian criminal justice system has been well documented. Although this Court has in the past had occasion to discuss this issue most extensively in the context of sentencing and of the interpretation and application of s. 718.2(e) of the *Criminal Code*, R.S.C. 1985, c. C-46, it is clear that the problems that contribute to this reality are not limited to the sentencing process."); *Campbell v Vancouver Police Board (No 4)*, 2019 BCHRT 275, para 112. Contrast: *Public Guardian for Nunavut v R*, 2019 NUCJ 7, para 39.

[640] *R v Le*, 2019 SCC 34, paras 97, 106 (within the context of section 9 of the *Charter*, the appropriate perspective is a reasonable person in the shoes of the claimant who is informed themselves about community perspectives on race relations and impacts the court's assessment of whether a 'detention' has occurred): "The documented history of the relations between police and racialized communities would have had an impact on the perceptions of a reasonable person in the shoes of the accused."; *R v Thompson*, 2020 ONCA 264, para 63 ("the appellant's status as a racialized Canadian in Brampton, one of the largest majority-racialized cities in Canada, is relevant to the perception of a reasonable person in his shoes."); *R v Grant*, 2009 SCC 32, para 32 ("the individual's particular circumstances and perceptions at the time may be relevant in assessing the reasonableness of any perceived power imbalance between the individual and the police"), per Binnie, J, concurring, para 154: "A growing body of evidence and opinion suggests that visible minorities and marginalized individuals are at particular risk from unjustified "low visibility" police interventions in their lives. … Courts cannot presume to be colour-blind in these situations."; *R v Golden*,

Racial profiling at the border perpetuates and reinforces these underlying stereotypes, and as such strikes at the heart of substantive equality rights.[641]

Nonetheless, racial profiling has been challenging to prove in border control contexts, for a few reasons. First, as automated or mathematical tools are increasingly incorporated into border control decision-making, frontline officials and some independent oversight bodies may find it difficult to assess the overall discriminatory impact of a given process.[642] Automation bias and enduring perceptions of neutrality imbue mathematical determinations with an authoritative deference that is difficult to dislodge.[643] However algorithmic systems, including automated facial recognition systems, frequently exhibit bias in ways that impact disproportionately on members of protected groups and perpetuate stereotypes.[644] Often these biases will arise because the automated system embeds historical biases hidden in training datasets that appear to be 'neutral'[645] whereas at other times bias will result because the circumstances of marginalized groups are not adequately reflected in training and testing datasets.[646] Further, where members of racial groups are singled out with greater frequency than others by an automated system, this can reinforce stereotypes—to border control officials who witness large volumes of racialized groups identified 'mathematically' for increased scrutiny may perceive that their internal, often subconscious, prejudices are confirmed.[647]

2001 SCC 83, para 83: "…even the most sensitively conducted strip search is highly intrusive. Furthermore, we believe it is important to note the submissions of the ACLC and the ALST that African Canadians and Aboriginal people are overrepresented in the criminal justice system and are therefore likely to represent a disproportionate number of those who are arrested by police and subjected to personal searches, including strip searches.... As a result, it is necessary to develop an appropriate framework governing strip searches in order to prevent unnecessary and unjustified strip searches before they occur."

[641] *Kahkewistahaw First Nation v Taypotat*, 2015 SCC 30, para 20; *Quebec (Attorney General) v A*, 2013 SCC 5, per Abella, J, (dissenting in result), para 332: "The root of s. 15 is our awareness that certain groups have been historically discriminated against, and that the perpetuation of such discrimination should be curtailed. If the state conduct widens the gap between the historically disadvantaged group and the rest of society rather than narrowing it, then it is discriminatory."

[642] For more details, see 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*.

[643] Jason Millar, "Five Ways a COVID-19 Contact-Tracing App Could Make Things Worse", *Policy Options*, April 15, 2020, https://policyoptions.irpp.org/magazines/april-2020/five-ways-a-covid-19-contact-tracing-app-could-make-things-worse/; Cosima Gretton, "The Dangers of AI in Health Care: Risk Homeostasis and Automation Bias", *Towards Data Science*, June 24, 2017, https://towardsdatascience.com/the-dangers-of-ai-in-health-care-risk-homeostasis-and-automation-bias-148477a9080f?gi=e7b5eb341e4a; Safiya Umoja Noble, "Algorithms of Oppression: How Search Engines Reinforce Racism", (New York: NYU Press, 2018).

[644] Rashida Richardson, Jason Schultz & Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems and Justice", (2019) 94 *NYU L Rev Online* 192, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423; Safiya Umoja Noble, "Algorithms of Oppression", (NY: New York University Press, 2018); Sarah Myers West, Meredith Whitaker & Kate Crawford, "Discriminating Systems: Gender, Race, and Power in AI", April 2019, *AI Now Institute*.

[645] For an example of how this form of automation of institutional memory can generally occur (but in a context where no discriminatory treatment is at issue) see: *Dhillon v Canada (Attorney General)*, 2016 FC 456, paras 5-11 and 40 (non-discretionary risk assessment for secondary screening referrals on the basis of past infractions amounts to an to an 'automation of institutional CBSA memory'). Courts have recognized the prejudicial impact that the "mystique of science" can have on decision-makers in other contexts as well: *R v Béland*, [1987] 2 SCR 398, para 64, per La Forest, J, concurring, in ruling polygraph tests inadmissible in jury trials, warned of the "human fallibility in assessing the proper weight to be given to evidence cloaked under the mystique of science." See also: Rashida Richardson, Jason Schultz & Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems and Justice", (2019) 94 *NYU L Rev Online* 192, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423.

[646] See, for example, 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.

[647] This type of disproportionate referral can reinforce the 'attitudinal problem of stereotyping' in the same ways in which under-representation of demographic groups in specific workforces can reinforce prejudicial perceptions that members of those groups are unable to do the work in question: *CN v Canada (Canadian Human Rights Commission)*, [1987] 1 SCR 1114. *R v Dudhi*, 2019 ONCA 665, para 71.

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.[1] 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.[2] 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.[3] 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.[4]

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.[5] 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.[6]

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.

---

[1] 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.

[2] *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.

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

[4] 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.

[5] *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.

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

Second, the standard of proof for profiling has been difficult to establish because membership in a protected group is not always statistically tracked by CBSA,[648] while individual impressions and observations of discriminatory practice are an insufficient evidentiary basis, even when uncontested.[649]

Finally, because border control officials are often granted wide latitude when subjecting travellers to scrutiny, there will typically be sufficient legitimate justification even where unconscious racial profiling remains a contributing factor.[650] In many contexts, there is no obligation to justify border control decisions, and as such it becomes difficult to demonstrate whether racial profiling was a factor in the decision or not.[651]

Despite these challenges in documentation, practices that subject travellers to differential treatment on the basis of racial bias discriminate unjustly and should not be permitted.

[648] *Canada (Attorney General) v Bougachouch*, 2014 FCA 63, paras 35-36.

[649] See, for example: *Canada (Attorney General) v Bougachouch*, 2014 FCA 63, paras 8 and 30-34.

[650] *Richards v Canada (Public Safety and Emergency Preparedness)*, 2008 FCA 341 (as border control agents may subject *anyone* to secondary screening doing is on the basis of membership in a protected group might not amount to differential treatment); *R v Dudhi*, 2019 ONCA 665, paras 57-66.

[651] *Dhillon v Canada (Attorney General)*, 2016 FC 456; *Quebec (Commission des droits de la personne et des droits de la jeunesse) v Bombardier Inc (Bombardier Aerospace Training Center)*, 2015 SCC 39, para 88 ("It cannot be presumed solely on the basis of a social context of discrimination against a group that a specific decision against a member of that group is necessarily based on a prohibited ground under the *Charter*."), paras 80 and 97 ("Because Bombardier's decision to deny Mr. Latif's request for training was based *solely* on [US] DOJ's refusal to issue him a security clearance, it is common ground that proof of a connection between the U.S. authorities' decision and a prohibited ground of discrimination would have satisfied the requirements of the second element of the test ... Finally, the Commission faults Bombardier for failing to check with the Canadian authorities or to ask the U.S. authorities to explain the reasons for their refusal. In this regard, it should be noted that Mr. Latif himself did not receive any explanation."); *Ewert v Canada*, 2018 SCC 30, para 79. For a contrasting approach, see footnote 639, above.

3.3 Legislative Models: Lawful Authority & Limitation

Border control-specific legislative instruments can interact with facial recognition in various ways. Some legislative frameworks are framed in a manner that precludes the use of facial recognition, either by express intention or otherwise. In other contexts, human rights obligations might require express legislative authorization before facial recognition border control systems can be adopted or expanded. Border control related legislative frameworks also vary with respect to the degree to which safeguards and accuracy obligations are required or expressly encoded. This section describes a number of these, selected in an attempt to demonstrate the variety of lawful authority relied upon by other jurisdictions when instituting facial recognition at border control junctures. Select examples of different legislative approaches from Australia, the European Union, the United States and Canada are included.

Australia

Adoption of facial recognition measures in border control contexts has frequently been preceded by legislative or regulatory authorization. However, as Australia has no enforceable human rights instrument, explicit lawful authority is more of a convention than a legal requirement.[652]

In 2006, Australia amended the *Migration Act 1958*, redefining immigration 'clearance authority' to include both 'clearance officers' and 'authorised systems', allowing travellers to verify their passports without human intervention.[653] In 2018, the *Migration Regulations 1994* were amended, allowing travellers to submit their facial images to authorised systems as adequate evidence of their identity, permitting automated facial recognition without reliance on passports and paving the way for contactless (and passport-less) immigration clearance.[654]

By contrast, in 2016, Australia repurposed its citizenship facial image database into a generalized law enforcement facial recognition capacity, granting the Australian Federal Police access to a centralized facial verification service based on this image repository.[655] No underlying statutory instrument authorized this expansion. More recently, legislation has been introduced that would

[652] While Australia is a signatory to foundational human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, its domestic human rights framework does not impose any constitutional human rights obligations. Domestic legislation requires that government action be consistent with Australia's international human rights commitments, and specific additional rights are encoded in the *Privacy Act 1988*. Legislative instruments must include a human rights impact statement. Generally speaking, incursions on human rights, including the right to privacy, must be prescribed by law, however this requirement is not enforceable. For an overview, see: Australian Government, Australian Law Reform Commission, "Traditional Rights and Freedoms—Encroachments by Commonwealth Laws", December 2015, ALRC Report 129, https://www.alrc.gov.au/wp-content/uploads/2019/08/alrc_129_final_report_.pdf, Section 2: Rights and Freedoms in Context.

[653] *Migration Amendment (Border Integrity) Bill 2006*.

[654] *Migration Amendment (Seamless Traveller) Regulations 2018*, https://www.legislation.gov.au/Details/F2018L01538; *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text.

[655] Australia, Hon. Michael Keenan, Minister for Justice, "New Face Verification Service to Tackle Identity Crime", *Media Release*, November 16, 2016, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/4938075/upload_binary/4938075.pdf;fileType=application%2Fpdf#search=%22media/pressrel/4938075%22.

provide a statutory framework for this capability, while significantly expanding its scope (see Box 13 for a more complete description).[656] If passed, the framework would realize an inter-governmental agreement by authorizing facial recognition across a broad variety of federal, state and private-sector agencies through an 'interoperability hub'.[657] This 'hub' would permit participating agencies to biometrically query any database of facial images held by any other participating agency, in pursuit of wide-ranging public policy objectives, including to "prevent identity crime, support law enforcement, uphold national security, promote road safety, enhance community safety and improve service deliver."[658] The Bill envisions the creation and eventual incorporation of a facial recognition-enabled driver's license database, however passport facial image repositories will be included, and likely to provide a robust and complete source of facial identification.[659]

While the proposed legislation would provide a framework for the envisioned facial recognition capability, most of the privacy safeguards and limitations on its use would arise from privacy impact assessments and other non-binding agreements.[660] In part due to this lack of legislated limitations, a parliamentary committee concluded it had "serious issues" with the Bill, noting that:

> The Committee accepts that it is not the Government's intent to set up the identity-matching services scheme without privacy safeguards in place. However, few privacy safeguards are currently set out in the IMS Bill. Rather, they are detailed in the IGA, in the Explanatory Memorandum and in proposed Participation Agreement and Access Policies. None of these materials have the force or protection of legislation.[661]

Despite this general lack, some core elements of the facial recognition system are encoded in the legislation. For example, the legislation explicitly defines the technical matching mechanisms it authorizes, and strictly limits how more invasive facial recognition capabilities [1:N] as opposed to less invasive facial recognition capabilities [1:1].[662] The Bill remains under legislative consideration.

---

[656] Parliament of Australia, Parliament Library, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019: Bills Digest", August 26, 2019, Bills Digest No 21, 2019-20, https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6875141/upload_binary/6875141.pdf.

[657] Parliament of Australia, Parliament Library, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019: Bills Digest", August 26, 2019, Bills Digest No 21, 2019-20, https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6875141/upload_binary/6875141.pdf.

[658] Parliament of Australia, Parliament Library, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019: Bills Digest", August 26, 2019, Bills Digest No 21, 2019-20, https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6875141/upload_binary/6875141.pdf, p 5.

[659] Australian Passports Amendment (Identity-Matching Services) Bill 2019, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6386_ems_b063b85b-0541-488e-9e01-fcccdafe5f3f/upload_pdf/713752.pdf;fileType=application%2Fpdf.

[660] Australia, Parliamentary Joint Committee on Intelligence and Security, Advisory Report on the Identity Matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019, October 2019, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019/Report, para 2.47-2.48.

[661] Australia, Parliamentary Joint Committee on Intelligence and Security, Advisory Report on the Identity Matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019, October 2019, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019/Report, para 5.11.

[662] See Box 13 and Section 2.5, pp 98-102, above for more details.

A related legislative proposal would amend the *Australian Passports Act* in order to automate various passport-related decisions deemed 'low-risk', including decisions to collect more personal information in order to process passport applications and decisions regarding the issuance of passports.[663] Facial recognition is anticipated to play a central role in these low-risk automated decision-making processes. In reviewing the Bill, a parliamentary committee has recommended that the Bill be amended so that only automated decisions leading to neutral or beneficial outcomes will have legal impact.[664]

United States

United States Customs and Border Protection (CBP) is legally required to collect biometric information from foreign nationals as they enter and depart the country.[665]

CBP has been criticized for extending its facial recognition program beyond its statutory authority. In particular, border control agencies have been criticized for expanding facial recognition to United States citizens on international flights when their legislative mandate is limited to collecting biometric data of foreign nationals.[666] CBP appears to justify the application of its program to United States citizens on the basis of consent.[667] However, consent has proven difficult to exercise and it remains unclear if most eligible travellers are aware that opting out of facial recognition is an option.[668]

---

[663] Australian Passports Amendment (Identity-Matching Services) Bill 2019, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6386_ems_b063b85b-0541-488e-9e01-fcccdafe5f3f/upload_pdf/713752.pdf;fileType=application%2Fpdf, para 8: "the Bill will also incorporate scope for the Minister to automate other decisions under the Passports Act. The intention is that these be low-risk decisions that a computer can make within objective parameters, such as decisions to collect personal information for processing passport applications using the FVS and decisions to issue passports to people whose biographical data and facial images exactly match information in previous passport applications."

[664] Australia, Parliamentary Joint Committee on Intelligence and Security, Advisory Report on the Identity Matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019, October 2019, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019/Report.

[665] United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, pp 2-3.

[666] 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:

> Under the current law, CBP is permitted to obtain biographic and biometric information of foreign nationals through the Biometric Exit Program. In 2018, CBP expanded this pilot program to include facial recognition scans of individuals boarding certain international flights. Considering that the legal authority which CBP cites to carry out this program expressly limits the collection of biometric data to "foreign nationals", we were stunned to learn of reports that the agency has partnered with the Transportation Security Administration and commercial airlines to use facial recognition technology on American citizens. It remains unclear under what authority CBP is carrying out this program on Americans.

See also: 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.

[667] 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. See also: United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, pp 13 and 38: "While regulations limit CBP's collection of biometric information to certain in-scope foreign nationals entering and exiting the United States, CBP's biometric entry-exit capabilities may also capture biometric data (facial images) from exempt foreign nationals and U.S. citizens. However, exempt foreign nationals and U.S. citizens are routinely able to "opt out" of using this technology to verify identity and can instead choose a manual check of documentation for identity verification."

[668] Allie Funk, "I Opted Out of Facial Recognition at the Airport—It Wasn't Easy", July 2, 2019, *WIRED*, https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/.

Additionally, under the United States *Administrative Procedure Act*,[669] government agencies must undergo a public consultation process when adopting new legal rules that substantively impact the rights or interests of individuals.[670] CBP has been criticized for failing to engage in a regulatory approval process while testing and deploying facial recognition systems.[671] The lack of a formalized rule has permitted US border control agencies to repeatedly alter the scope and nature of alternative mechanisms available to travellers who do not wish to submit to facial recognition upon entering or leaving the United States.[672]

In some instances, private sector tools have been relied upon by individual United States border control agents to carry out facial recognition searches without any clear legislative or even any institutional framework in place. Clearview AI is a commercial facial recognition vendor that offers its services to investigative state and other agencies through an online portal (see Box 17 for more details).[673] United States Immigration and Customs Enforcement (ICE) agents conducting immigration enforcement and removal investigations have reportedly used the tool in the absence of a formal institutional arrangement between ICE and Clearview AI.[674] In February 2020, it was also reported that almost 280 individual United States Customs and Border Protection (CBP) accounts were registered with Clearview AI and had carried out close to 7,500 searches.[675] CBP did not enter into an institutional arrangement with Clearview AI, and confirmed that the searches were not carried out in connection with its primary formal facial recognition program.[676] In other contexts, law enforcement agencies have confirmed that

[669] Encoded at 5 USC 500 *et seq*.

[670] *Electronic Privacy Information Center v Department of Homeland Security*, (2011) 653 F.3d 1 (US DC CirC); Todd Garvey, "A Brief Overview of Rulemaking and Judicial Review", March 27, 2017, *Congressional Research Service*.

[671] 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*, pp 7-8.

[672] Electronic Information Privacy Center, "EPIC v CBP (Biometric Entry/Exit Program), *EPIC.org*, last modified April 2020, https://epic.org/foia/dhs/cbp/biometric-entry-exit/; 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 8 ("although DHS has said that face scans may be optional for some American citizens, it is unclear whether this is made known to American travelers.") and footnote 42 (indicating that the ability to opt-out may be contingent on specific agreements between United States Customs and Border Protection and particular airlines, and concluding that: "It is not possible to evaluate the specific opt-in/opt-out procedures set forth in the referenced agreements, because the text of these agreements has not been made public.").

[673] Kashmir Hill, "The Secretive Company that Might End Privacy as We Know It", *New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[674] The agency does have a formal arrangement (adopted as a paid pilot) with respect to its child exploitation unit: 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: "A spokesperson for ICE told BuzzFeed News that HSI began a paid pilot program in June 2019 through its Child Exploitation Investigations Unit and noted that a formal contract has not yet been signed. ICE's use of facial recognition technology is primarily used by Homeland Security Investigations (HSI) special agents investigating child exploitation and other cybercrime cases," the spokesperson said. "ICE Enforcement and Removal Operations (ERO) officers have also occasionally used the technology, as task force officers with HSI and the Department of Justice, and through training, on human trafficking investigations."

[675] 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.

[676] 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: "In total, those accounts have run almost 7,500 searches, the most of any federal agency that did not have some type of paid relationship. A spokesperson for CBP said Clearview was not used for the agency's biometric entry-exit programs and declined further comment."

adoption and use of the tool has occurred on largely an ad hoc basis, often without awareness at the institutional level.[677]

Procurement and operation of border control facial recognition systems is also guided by Department of Homeland Security administrative obligations. For major acquisition programs, this includes administrative obligations to establish clear performance requirements and conduct pilot field testing in order to determine whether facial recognition systems meet those requirements when operating in a real-world environment.[678] The field tests include accuracy ratings and operational effectiveness quotas and measurements—for example, CBP expects its facial recognition system to capture facial images for 97% of in-scope travellers exiting the United States, and error thresholds comprising FNIR of 90% and FPIR of 0.1%.[679] It is not clear to what degree these obligations apply to acquisition programs that are adopted informally by individual agents on a large scale, such as CBP and ICE agents' use of Clearview AI. In addition, the *E-Government Act of 2002* requires border control agencies to conduct and, to the extent practicable, publish full Privacy Impact Assessments describing the anticipated impact of the technology.[680]

United Kingdom

The United Kingdom has adopted general-purpose protections governing biometrics in its data protection law, which recognizes biometric data as 'special category' data, requiring additional protection.[681] The United Kingdom also remains subject to the European Convention on Human Rights, discussed in the following section. In the law enforcement context, an appellate court has held that this biometric regulation regime was not sufficiently precise to curtail the more intrusive nature of facial recognition technologies and hence cannot form the basis for lawful authority on its own.[682]

The United Kingdom has amended its border control regulatory framework to explicitly facilitate automated processing of foreign nationals through the use of facial recognition-enabled automated

[677] 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.

[678] United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, pp 19-20: "As a major acquisition program, CBP and the Biometric Entry-Exit Program are required to follow DHS acquisition policy and guidance to test and deploy air exit capabilities." See also: Department of Homeland Security, Acquisition Management Directive 102-01 and Instructional Manual 201-01-001.

[679] United States, Government Accountability Office, "Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues", September 2020, GAO-20-568, pp 51 and 52.

[680] *E-Government Act of 2002*, Pub L 107-347, Title II, December 17, 2002, 116 Stat 2910, (codified at 44 USC 3501, notes), section 208(b)(1)(B)(iii): "(B) … each agency shall … (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." Indeed, CBP has published multiple full and un-redacted privacy impact assessments for border control facial recognition systems: https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service.

[681] European Union, Regulation 2016/679 (General Data Protection Regulation), Article 9; United Kingdom, *Data Protection Act 2018*, sections 10-11.

[682] *R (Bridges) v Chief Constable of South Wales Police*, [2020] EWCA Civ 1058, para 91.

ePassport gates.[683] However, these regulations do not impose any specific conditions regarding facial recognition accuracy or use.

European Union

The European Union will generally premise EU-wide biometric border control initiatives with some form of statutory instrument. This results partially from the lack of generalized EU-wide authority to compel biometric recognition at the national level, and due to a requirement for lawful authority where fundamental rights are impacted by biometrics.

Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the European Union *Charter of Fundamental Rights* enshrine the rights to privacy and data protection. The creation and use of facial recognition capabilities in border control settings implicates these rights, and is considered to be intrusive.[684] Given the uniquely identifiable nature of biometrics, even the ephemeral use of facial recognition systems triggers CFR protections,[685] and lawful authorization is generally required as a precondition for the adoption of a facial recognition system.[686] Facial recognition concerns are at times addressed by limiting the scope of lawful authority provided by EU-wide legal instruments. Concerns arising from centralization of a facial recognition system, for example, can be mitigated by requiring additional lawful authority as a pre-condition to centralization.[687]

---

[683] United Kingdom, The Immigration (Leave to Enter and Remain)(Amendment) Order 2019, February 18, 2019, SI 2019/298, https://www.legislation.gov.uk/uksi/2019/298/pdfs/uksi_20190298_en.pdf; United Kingdom, The Immigration (Leave to Enter and Remain)(Amendment) Order 2010, March 25, 2010, SI 2010/957.

[684] European Data Protection Supervisor, Opinion 06/2016, Opinion on the Second EU Smart Borders Package, September 21, 2016, para 16: "Biometric data are of a peculiar nature and considered more delicate as they are unequivocally linked to one individual, whose body is made "readable". The EDPS takes note of the need to use biometrics in order to ensure higher assurance of the identity of third country nationals crossing the EU borders. Nonetheless, due to their very nature, processing of biometric data implies a more serious interference and therefore requires ensuring a higher level of data protection."; *R (Bridges) v Chief Constable of South Wales Police*, [2019] EWHC 2341, 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).

[685] Case 291/12, *Schwartz v Bochum*, October 17, 2013, (Court of Justice of the European Union, 4th Chamber)(with respect to fingerprints), paras 26-30 and 49; *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 13-14, 67-68, 78 and 80-85: "fingerprints objectively contain unique information about the individual concerned, allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and the retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant."); *R (Bridges) v Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin), para 59: "It is sufficient if biometric data is captured, stored and processed, even momentarily. 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.

[686] Case 291/12, *Schwartz v Bochum*, October 17, 2013, (Court of Justice of the European Union, 4th Chamber), paras 35 and 58-61; *S and Marper v United Kingdom*, App Nos 30562/04 and 30566/04, (ECtHR Grand Chamber, 2008), para 99 (ultimately choosing not to decide the matter on the ground of legality, however); *R (Bridges) v Chief Constable of South Wales Police*, [2020] EWCA Civ 1058 (in relation to overt, rather than covert, facial recognition in the criminal context), para 91.

[687] Case 291/12, *Schwartz v Bochum*, October 17, 2013, (Court of Justice of the European Union, 4th Chamber), para 61; European Union, Regulation 2252/2004, December 13, 2004, Article 1(2) "Passports and travel documents shall include a storage medium which shall contain a facial image."; European Union, Regulation No 444/2009, *amending Council Regulation No 2252/2004*, May 28, 2009, recital 5: Regulation (EC) No 2252/2004 requires biometric data to be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. This is without prejudice to any other use or storage of these data in accordance with national legislation of Member States. Regulation (EC) No 2252/2004 does not provide a legal base for setting up or maintaining databases for storage of those data in Member States, which is strictly a matter of national law." See also:

> The EDPS stresses that each large scale IT system operates on the basis of a specific legal basis in which the architecture of the system is clearly defined, including the centralisation or the decentralisation of the system. The EDPS also recalls the hierarchy of legal acts in the EU defined in

Specific elements of a facial recognition system may require independent legal authorization under EU law. The EU is currently undergoing an interoperability initiative that would facilitate biometric-based recognition across seven large-scale border control-related databases (six of these databases already exist, and a seventh will be created).[688] Bringing about this centralization and interoperability could not be accomplished without significant new legislative authorization.[689] Once implemented, the detrimental impact on fundamental rights that would result from creating a centralized, interoperable biometric search capability across multiple border control systems may not be justified, despite finding a basis in clear lawful authority.

EU facial recognition authorization frameworks will typically include detailed safeguards. In 2017, for example, the European Union adopted a regulation mandating facial recognition of foreign nationals upon exit and entry with the primary intention of identifying individuals who stay within the EU longer than authorized.[690] The regulation stipulates that the biometric Exit and Entry System will only start operation once regulatory specifications for image quality and minimum performance thresholds "including minimum specifications … in particular in terms of False Positive Identification Rate, False Negative Identification Rate and Failure to Enrol Rate" are in place.[691] The EU's border control system interoperability initiative will also provide minimum quality and accuracy standards, as well as an obligation to monitor and periodically report on data quality and querying accuracy in its implementing legislation.[692]

> the Treaty on the Functioning of the European Union28: crucial changes especially to the architecture of an existing IT system which is defined in its legal basis, cannot be introduced by a delegation agreement and not even by delegating or implementing acts of the Commission. Such a change of the architecture can be only done by a change of the legislative basis, preceded by appropriate impact assessment and feasibility studies which clearly show the necessity and proportionality of a possible centralisation. Such an agreement can also raise doubts as to its legal certainty, transparency, its impact on the functioning of the whole system and possible changes in responsibilities. The delegation agreement should not be used in any way to circumvent democratic scrutiny which is a part of a legislative process. Consequently from the legal point of view, the architecture of the system cannot be changed by a delegation agreement between eu-LISA and a group of Member States.

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

[688] European Commission, Twentieth Progress Report Towards an Effective and Genuine Security Union, COM(2019)552, October 20, 2019, pp 4-5.

[689] European Data Protection Supervisor, Opinion 9/2017, proposal for a Regulation on the eu-LISA, October 9, 2017, para 14: "The EDPS stresses that each large scale IT system operates on the basis of a specific legal basis in which the architecture of the system is clearly defined, including the centralization or the decentralisation of the system. ... from the legal point of view, the architecture of the system cannot be changed by a delegation agreement between eu-LISA and a group of Member States."; Council of Europe, High Level Expert Group on Information Systems and Interoperability, Final Report, May 8, 2017, p 12: "Establishing a data warehouse probably requires amendment of the legal instruments establishing the databases concerned."

[690] European Union, Regulation 2017/2226, Entry/Exit System (EES), November 30, 2017.

[691] European Union, Regulation 2017/2226, Entry/Exit System (EES), November 30, 2017, Articles 66(1)(a) and 36(b) and (g):

> 36 The Commission shall adopt the implementing acts necessary for the development and technical implementation of the EES Central System, … in particular measures for: ... (b) the specifications for the quality, resolution and use of the facial image for biometric verification and identification in the EES, including where taken live or extracted electronically from the eMRTD; ... (g) performance requirements, including the minimum specifications for technical equipment and requirements regarding the biometric performance of the EES, in particular in terms of the required False Positive Identification Rate, False Negative Identification Rate and Failure To Enrol Rate;"

[692] European Union, Regulations 2019/817 and 2019/818, establishing a framework for interoperability, May 20, 2019, Articles 13(3) and 37:

> 1. Without prejudice to Member States' responsibilities with regard to the quality of data entered into the systems, eu-LISA shall establish automated data quality control mechanisms and procedures on the data stored in [implicated border control systems]. 2. eu-LISA shall implement mechanisms for evaluating the accuracy of the shared BMS, common data quality indicators and the minimum quality standards for storage of data in the [implicated border control systems]. ... 3. eu-LISA shall provide regular reports on the automated data quality control mechanisms and procedures and the common data quality indicators to the Member States. eu-LISA shall also provide a regular report to the Commission covering the issues encountered and the Member States concerned. ... 4. The details of the automated data quality control

Canada

Most border control-related biometric recognition measures in Canada have been adopted within an explicit legislative and regulatory context. However, exceptions to this general practice suggest that the Canadian government does not view prior legislative authorization as a mandatory pre-requisite to the use of facial recognition in border control contexts. In particular, in the context of whether a rights infringing practice is 'prescribed by law' and capable of justified, courts have opined that "[g]overnments should not be free to use a broad delegated authority to transform a limited-purpose licensing scheme into a *de facto* universal identification system beyond the reach of legislative oversight."[693]

In 2004, Canada amended the primary regulation governing the vetting and issuance of passports (the *Canadian Passport Order*), to explicitly authorize the conversion of passport facial images into biometric templates in passport application vetting, and to include ICAO-compliant facial images into Canadian passports.[694] While Canada made no use of ICAO-compliant passport images for facial recognition at border crossings at the time, this regulatory change enabled Canadian travellers to interact with passport-based facial recognition border control systems in other states.

Prior to 2013, the collection and use of biometrics for Immigration-related purposes was largely conducted under discretionary authorities set out in the *Immigration and Refugee Protection Act*.[695] In 2012-13, through IRPA amendments and implementing regulations, the Temporary Resident Biometric Project was legally formalized, creating a framework for the systematic collection of biometric information in non-enforcement contexts for foreign nationals seeking a temporary resident visa, study permit or work permit.[696] In 2015, the IRPA was amended to expand the dedicated

> mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data in the [implicated border control systems], in particular regarding biometric data, shall be laid down in implementing acts.

[693] *Alberta v Hutterian Brethren of Wilson Colony*, 2009 SCC 37, para 40, (the use of subordinate regulation as lawful authority to establish an identification scheme will generally be sufficient to ensure the government action is 'prescribed by law' when justifying rights-incursions under section 1 of the *Charter*, but justifying wide-ranging identification systems that extend beyond the legislative context from which they emerge might require legislative reform). See also: *Little Sisters Book and Art Emporium v Canada (Minister of Justice)*, 2000 SCC 69, paras 138 (compliance with *Charter* rights can be achieved by legislation, regulation, government directive or agency practice) and 141 ("Violative conduct by government officials that is not authorized by statute is not "prescribed by law" and cannot therefore be justified under s. 1. The equality rights issues therefore proceed directly to the remedy phase of the analysis."); *Multani v Commission scolaire Marguerite-Bourgeoys*, 2006 SCC 6, para 22 ("when...delegated power is not exercised in accordance with the enabling legislation, a decision ... is not a limit 'prescribed by law'"); *PS v Ontario*, 2014 ONCA 900, paras 182-183; *R v Welsh*, 2013 ONCA 190, para 80: "Section 1 requires that the limit be "prescribed by law". At issue here is a police investigative technique that rests on nothing more precise than the general legal duty of the police to investigate crime. The Crown does not contend that there is a law that authorizes or permits the police to use the investigative technique under scrutiny. Where the actions of a government agent are not specifically authorized or prescribed by law, s. 1 does not apply. A general duty of that nature does not amount to a limit "prescribed by law" within the meaning of s. 1."

[694] Canadian Passport Order, SI/81-86, PC 1981-1472, section 8.1, adopted in Order Amending the Canadian Passport Order, SI/2004-113, PC 2004-951, September 1, 2004: http://www.gazette.gc.ca/rp-pr/p2/2004/2004-09-22/pdf/g2-13819.pdf, Explanatory Note:

> Section 8.1 of the Order authorizes the Passport Office to convert a passport applicant's photograph into a biometric template that would be used as part of the facial recognition program to confirm the applicant's identity, including nationality, in order to determine their entitlement to obtain and possess a Canadian passport. Furthermore, in accordance with passport security specifications established by the International Civil Aviation Organization for a globally interoperable system governing the use of travel documents, the Passport Office will issue passports embedded with integrated circuit chips containing digital biometric information about the bearers.

[695] *Regulations Amending the Immigration and Refugee Protection Regulations*, SOR/2018-128, PC 2018-844, June 22, 2018, Regulatory Impact Analysis Statement.

[696] *Protecting Canada's Immigration System Act*, SC 2012, c 17, particularly clause 6; Library of Parliament, "Bill C-31: An Act to Amend the Immigration and

biometrics framework beyond temporary residents.[697] Under the amended Act, regulations can specify procedures for the collection, creation and use of biometric information.[698] To date, implementing regulations have expanded the biometric project to encompass all temporary permit applicants, permanent resident applicants and refugee protection claimants, subject to some itemized exceptions (such as individuals younger than 14 years of age and some applicants over 79 years of age).[699] For covered applicants or claimants, the regulations currently require collection of facial images and fingerprints,[700] and permit the creation of fingerprint and facial biometric templates.[701] The IRPA provisions explicitly authorize use of biometric information for verification purposes alone, but permit this verification process to extend beyond the application process.[702] The implementing regulations currently authorize border control agents or automated screening mechanisms to require biometric verification each time such a claimant or applicant enters Canada.[703]

In 2017, CBSA began employing facial recognition-enabled Primary Inspection Kiosks in order to automate identification objectives in customs and in processing known travellers.[704] The Primary Inspection Kiosks are used to process all travellers seeking entry into Canada, including citizens. The

---

Refugee Act, the Balanced Refugee Reform Act, the Marine Transportation Security Act and the Department of Citizenship and Immigration Act", Publication No 41-1-C31-E, revised June 4, 2012, sections 2.4 – 2.4.1: "Bill C-31 introduces one entirely new element to non-refugee-related aspects of Canada's immigration policy: the use of biometrics for temporary resident visa applications. … Although fingerprints have been collected from refugee claimants and from individuals arrested for contravening the IRPA in Canada, clause 6 introduces the collection of biometrics in a non enforcement context by adding section 11.1 to the Act."; Immigration, Refugees and Citizenship Canada, Temporary Residents Biometrics Project (TRBP), Privacy Impact Assessment – Summary, last modified December 27, 2012, https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/access-information-privacy/privacy-impact-assessment/temporary-resident-biometrics-project-2012.html. By regulation, the Temporary Resident Biomterics Project was limited in application to foreign nationals from 29 itemized countries and one territory: *Regulations Amending the Immigration and Refugee Protection Regulations*, SOR/2018-128, PC 2018-844, June 22, 2018, Regulatory Impact Analysis Statement.

[697] *Economic Action Plan 2015 Act, No 1*, SC 2015, c 35, Division 15. The IRPA was also amended to clarify lawful authority to administer the act by electronic means, including through the use of automated decision-making systems

[698] *Immigration and Refugee Protection Act*, SC 2011, c 27, sections 10.01 and 10.02 ("10.01 A person who makes a claim, application or request under this Act must follow the procedures set out in the regulations for the collection and verification of biometric information...").

[699] *Immigration and Refugee Protection Regulations*, SOR/2002-227, *as amended*, paragraphs 12.2(1)(a)-(b):) 12.2 (1) Section 10.01 of the Act does not apply to (a) a person who is under the age of 14; (b) a person who is over the age of 79, unless that person makes a claim in Canada for refugee protection").

[700] *Immigration and Refugee Protection Regulations*, SOR/2002-227, *as amended*, section 12.3(b).

[701] *Immigration and Refugee Protection Regulations*, SOR/2002-227, *as amended*, section 12.4.

[702] *Immigration and Refugee Protection Act*, SC 2011, c 27, sections 10.01: "A person who makes a claim, application or request under this Act must follow the procedures set out in the regulations for the collection and verification of biometric information, including procedures for the collection of further biometric information for verification purposes after a person's claim, application or request is allowed or accepted."

[703] *Immigration and Refugee Protection Regulations*, SOR/2002-227, *as amended*, section 12.5: "For the purposes of section 10.01 of the Act, the procedure for the verification of biometric information to be followed by a person ... referred to in any of paragraphs 12.1(a) to (m) is that, on seeking to enter Canada and when directed by an officer or by alternative means of examination referred to in paragraph 38(b), the person shall provide the information listed in subparagraphs 12.3(b)(i) and (ii) by means of an electronic device made available for that purpose, in order to verify the biometric information that they provided under paragraph 12.3(b)."

Note that this does not appear to preclude other forms of biometric recognition, such as biometric comparison to avoid duplicative applications or detect criminality, during the application assessment process rather than upon verifying a permanent resident or other applicant's identity upon entry into Canada (see: *Regulations Amending the Immigration and Refugee Protection Regulations*, SOR/2018-128, PC 2018-844, June 22, 2018, Regulatory Impact Analysis Statement: "Under the TRBP, between September 2013 and August 2017, IRCC collected biometric information from approximately 1 213 733 applicants, resulting in matches to 2 011 previous asylum claimants, 186 161 previous immigration applicants, 720 Canadian criminal records, and 134 individuals who possessed both a Canadian criminal record and a previous asylum claim.")

Note that under section 38(b) of the *Immigration and Refugee Protection Regulations* permits screening by means of automated systems.

[704] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html; Canada Border Services Agency, "NEXUS – Privacy Impact Assessment", Executive Summary, last modified January 14, 2020, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/nexus-eng.html.

CBSA has not publicly identified its lawful authority for including this biometric recognition capability. CBSA appears to be relying on its general lawful authority for compelling trusted and untrusted travellers to present themselves at customs upon entering Canada, rather than an explicit legal instrument for facial recognition.[705] Further, the public component of CBSA's privacy impact assessment for these kiosks does not acknowledge any additional privacy and accuracy impact that results from automated facial recognition, appearing to conflate the collection of a biographic facial image with the use of a biometric facial image for automated recognition.[706]

Finally, the Known Traveller Digital Identity program described in Box 12, above, is being piloted in Canadian airports. The program as envisioned relies on voluntary participation, and as such does not rely on any specific legislative or regulatory authority. If fully implemented, supporting regulations might be enacted to justify the program's border control-related elements.[707] It is not clear how this lawful authority will interact with the program's broader ambition to create a universal digital identification capacity.[708]

Adopting facial recognition absent a clear legislative framework undermines the transparency of the system and fails to impose the safeguards necessary to ensure the system operates in an accurate and prescribed manner. For example, it remains unclear whether the CBSA's PIK system is optional to travellers.[709] By contrast, comparable programs in the United Kingdom, the United States and Australia have expressly encoded and clearly defined voluntariness into their biometric programs.[710]

---

[705] *Canada Border Services Agency Act*, sub-section 5(1); *Customs Act*, RSC 1985, c 1, sections 11 and 11.1; *Presentation of Persons (2003) Regulations*, SOR/2003-323. By contrast, paragraph 11(a) of the *Presentation of Persons (Customs) Regulations* authorizes travellers arriving into Canada by commercial aircraft to present themselves by means of an electronic device. However, these do not expressly address the use of automated biometric recognition systems. Paragraph 6.3 of the *Presentation of Persons (Customs) Regulations* authorize the collection of iris images from travellers enrolled in NEXUS, and the use of these iris images for biometric recognition of trusted travellers entering Canada under a NEXUS authorization.

[706] Canada Border Services Agency, "Primary Inspection Kiosk – Privacy Impact Assessment: Executive Summary", March 14, 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html: "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, and will increase the integrity of data collection and the security of data transmission." The publicly available portion of the NEXUS privacy impact assessment indicates that the full PIA will "explain in more detail" the transition from Iris-based NEXUS biometric recognition to fully automated facial recognition: Canada Border Services Agency, "NEXUS – Privacy Impact Assessment", Executive Summary, last modified January 14, 2020, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/nexus-eng.html.

[707] The NEXUS program, for example, is a similar 'trusted traveller' program which operates on an 'opt-in' basis. NEXUS program participants are authorized to present themselves by alternative means when entering Canada by section 6.1 of the *Presentation of Persons (2003) Regulations*, SOR/2003-323.

[708] 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.

[709] In public statements, the CBSA has suggested that travellers do not have any choice in submitting to facial recognition where PIKs have been implemented:

> **Do I have to use a Primary Inspection Kiosk?**
>
> You are asked to use the kiosks where they are available as this allows us to provide you the best service. If you are ineligible or unable to use a kiosk, you will make your declaration to a border services officer when you arrive.

Canada Border Services Agency, "Primary Inspection Kiosks – Frequently Asked Questions", *cbsa.asfc.gc.ca*, last modified February 13, 2010: https://www.cbsa-asfc.gc.ca/travel-voyage/pik-bip-eng.html. The public version of CBSA's Privacy Impact Assessments are equally silent on the question of voluntariness.

[710] United Kingdom, *The Immigration (Leave to Enter and Remain)(Amendment) Order 2019*, SI 2019/298, February 18, 2019, Explanatory Memorandum; United Kingdom, *The Immigration (Leave to Enter and Remain)(Amendment) Order 2010*, SI 2010/957, March 24, 2010, Explanatory Memorandum, para 8.1: "use of any automated gate scheme is entirely voluntary."; Australia, *Migration Amendment (Seamless Traveller) Regulations 2018*,

The lack of a clear legislative framework also bypasses the opportunity to impose conditions regarding transparency and accuracy, such as those directly incorporated into some European Union frameworks.[711] While the accuracy of the CBSA's program is subject to review under the *Privacy Act*,[712] the CBSA has, to date, indicated in public comments that it will not disclose accuracy ratings for its PIKs.[713]

In some Canadian border control contexts, legislative instruments have taken active steps to preclude biometric recognition in the absence of express legislative amendment. For example, in granting the CBSA a discretionary authority to collect information from travellers exiting Canada, a closed list of biographic data elements was encoded into section 92 of the *Customs Act*,[714] precluding the collection of biometrics including facial templates.[715]

Canada is a participant in the Five Country Conference (FCC or "Migration 5"), a border arrangement between agencies in Canada, the United States, the United Kingdom, Australia and New Zealand (also members of the Five Eyes signals intelligence alliance). The FCC has established a High Value Data Sharing (HVDS) Protocol creating a framework for bilateral automated biometric querying between FCC members.[716] The Protocol does not impose specifications for automated biometric recognition, but does facilitate automated exchange of fingerprints and it is left to recipient states to determine whether

---

https://www.legislation.gov.au/Details/F2018L01538; Australia, *Migration Amendment (Seamless Traveller) Regulations 2018*, Explanatory Statement, Attachment B, Statement of Compatibility with Human Rights, https://www.legislation.gov.au/Details/F2018L01538/Explanatory%20Statement/Text: "Contactless Processing maintains the current requirements on travellers, other than not requiring the presentation of a passport where previously collected passport information is available. … travellers will also retain the option of choosing manual processing, with the physical identity document, by a clearance officer if preferred."

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

[712] *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.

[713] 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.

[714] *An Act to Amend the Customs Act*, SC 2018, c 30, clause 2; Library of Parliament, Bill C-21: An Act to Amend the Customs Act: Legislative Summary, Publication No 42-1-C21-E, October 31, 2018, https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/42-1/c21-e.pdf, p 6.

[715] *Exit Information Regulations*, Regulatory Impact Analysis Statement, Part I, 153(11) *Canada Gazette*, March 16, 2019, https://cippic.ca/uploads/ExitInformationRegulations-SOR2019_241.pdf:

> Risk: The scope of the Entry/Exit Initiative could inadvertently be expanded to include additional personal information beyond what is strictly necessary to manage travel history information (biometric information, licence plates, passenger name record data, etc.).
>
> Mitigation: New legislative authorities have been enacted to ensure that the collection of personal information is limited by a statutory framework, namely, the data elements outlined in sections 92 and 93 of the Customs Act. The collection of any additional personal information is not currently in scope, nor are there any plans to collect this information in the immediate future.

[716] Immigration, Refugees and Citizenship Canada, "Four Country Conference High Value Data Sharing Protocol—Privacy Impact Assessment", Last updated August 21, 2009, https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/access-information-privacy/privacy-impact-assessment/four-country-conference.html; New Zealand, Department of Labour – Immigration New Zealand, "Exchange of Information with Australia as Part of the Five Country Conference High Value Data Sharing Protocol", August 2010, https://www.immigration.govt.nz/documents/about-us/fcc-pia-new-zealand-and-australian-department-of-immigration-and-citizenship-aug-2010.pdf, p 5.

to use manual or automate matching when responding to requests.[717] The program was initially limited to 3,000 refugee and immigration enforcement-related automated queries per year between each participating FCC country.[718] Queries are not intended to directly target FCC member country nationals, but may do so incidentally.[719] Canada's implementation of this mechanism will return a 'no match' response to any query that matches a Canadian citizen or, for requests unrelated to refugee cases, a permanent resident.[720] No clear safeguards are included to ensure the 3,000 query limits are respected, or to report on matching accuracy. Canada's participation in the data sharing protocol was recently expanded as part of a broader initiative to expand fingerprint and facial biometrics in immigration processing.[721] No steps to include facial recognition in this system have been announced to date.

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.

[717] Immigration, Refugees and Citizenship Canada, "Four Country Conference High Value Data Sharing Protocol—Privacy Impact Assessment", Last updated August 21, 2009, https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/access-information-privacy/privacy-impact-assessment/four-country-conference.html; New Zealand, Department of Labour – Immigration New Zealand, "Exchange of Information with Australia as Part of the Five Country Conference High Value Data Sharing Protocol", August 2010, https://www.immigration.govt.nz/documents/about-us/fcc-pia-new-zealand-and-australian-department-of-immigration-and-citizenship-aug-2010.pdf; Canada, *Regulations Amending the Immigration and Refugee Protection Regulations*, SOR/2017-79, enacting section 315.38: "A query in respect of a person must be made by submitting to another party either the person's fingerprints accompanied by a unique transaction number or the unique transaction number assigned to a previous query received in respect of the person."

[718] Immigration, Refugees and Citizenship Canada, "Four Country Conference High Value Data Sharing Protocol—Privacy Impact Assessment", Last updated August 21, 2009, https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/access-information-privacy/privacy-impact-assessment/four-country-conference.html.

[719] Canada, *Regulations Amending the Immigration and Refugee Protection Regulations*, SOR/2017-79, Regulatory Impact Statement PC 2017-462, May 5, 2017; New Zealand, Department of Labour – Immigration New Zealand, "Exchange of Information with Australia as Part of the Five Country Conference High Value Data Sharing Protocol", August 2010, https://www.immigration.govt.nz/documents/about-us/fcc-pia-new-zealand-and-australian-department-of-immigration-and-citizenship-aug-2010.pdf, p 5.

[720] Immigration, Refugees and Citizenship Canada, "Regulations for Automated Biometric-Based Information Sharing with Australia, New Zealand and the United Kingdom—Privacy Impact Assessment", Last updated June 1, 2018, https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/access-information-privacy/privacy-impact-assessment/automated-biometric-information-sharing-australia-new-zealand-uk.html; Canada, *Regulations Amending the Immigration and Refugee Protection Regulations*, SOR/2017-79, Regulatory Impact Statement PC 2017-462, May 5, 2017: "The Regulations specify that information will be shared on third-country nationals, including asylum claimants and overseas refugee resettlement applicants. The Regulations also specify that only in the case of asylum or resettlement queries from Australia, New Zealand, or the United Kingdom will information on permanent residents of Canada be disclosed on an automated basis. The Regulations also specify that information on Canadian citizens will not be disclosed."

[721] *Regulations Amending the Immigration and Refugee Protection Regulations*, SOR/2018-128, PC 2018-844, June 22, 2018, Regulatory Impact Analysis Statement.

Section 4. Observations & Conclusions

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 also 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]

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 & 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.

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]

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]

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. [Sections 1.1.1 and 1.6]

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]

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]

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 identity management tool for public and private sector administrative purposes. [Sections 1.3.2, 1.6, 2.4, 2.5 & 2.6][Box 12]

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 most 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. [pp 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 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.

FIN.