National Security and Intelligence Review Agency

Office de surveillance des activités en matière de sécurité nationale et de renseignement

STUDY OF THE GOVERNMENT OF CANADA'S USE OF BIOMETRICS IN THE BORDER CONTINUUM

NSIRA // Review 20 - 08

Table of Contents

1. EXECUTIVE SUMMARY 3

List of Acronyms 5

Glossary of Terms 8

2. AUTHORITIES 9

3. INTRODUCTION 9

Background 9

The Study 11

Scope 11

Criteria 12

Methodology and Information Requirements 13

The Report 13

4. BIOMETRICS *PAST* 14

9/11 14

ePassport 16

Temporary Resident Biometrics Program (TRBP) (2009-2018) 17

Beyond the Border (2011) and Immigration Information Sharing (IIS) (2013-2016) 18

Information-Sharing Pilot between CBSA and IRCC/CIC (2013-2016) 19

Research into Facial Recognition 21

Pilot and Research on Operational Video-based Evaluation of Infrastructure and Technology: Face Recognition in Video (PROVE-IT: FRiV) (2011-2013) 21

Faces on the Move (FOTM) (2014-2017) 21

FASTER-PrivBio Project (2015-2017) 27

Biometrics Expansion Project (2015-2020) 28

Assessing Biometrics Past 29

5. BIOMETRICS *PRESENT* 30

Immigration Program 31

Assessing the Immigration Program 38

Passport Program 42

Assessing the Passport Program 48

Arriving into Canada 51

Primary Inspection Kiosks (PIKs) 51

NEXUS 55

6. BIOMETRICS *FUTURE* 56
7. OBSERVATIONS 65
1. Biometrics and National Security 65
2. The Steady-State Activities 67
3. Expanding Use of Biometrics over Time 68
4. Pilot Projects 69
5. Evolving Legal and Societal Norms 70
6. The Dual-Use of Biometrics 71
7. Technical Systems 74
8. Visibility into Algorithms 75
9. Preventing Bias and Discrimination 75
8. Conclusion 77
Annex A. Technical Note: Immigration and Passport Program Systems 79
Immigration Program 80
Passport Program 83
Departmental Responsibilities and System Interconnectivity 84

1. EXECUTIVE SUMMARY

The Government of Canada (GoC) uses biometrics to identify individuals with a level of confidence beyond what is possible absent such techniques.

Biometrics play a fundamental role in the border continuum, which includes the screening of foreign nationals seeking admission to Canada and the identification of passengers travelling internationally by air. In the course of this study, the National Security and Intelligence Review Agency (NSIRA) examined activities conducted by the Canadian Border Services Agency (CBSA), Immigration, Refugees, and Citizenship Canada (IRCC), and Transport Canada (TC). The study also extended to the Royal Canadian Mounted Police (RCMP), which plays a supporting role in one of the major IRCC-led programs in this area.

Biometrics are sensitive personal information. The identification of persons by virtue of their biological characteristics raises privacy and human rights concerns. There is public apprehension about the government's use of biometric analysis, as reflected in discussions regarding the use of facial recognition technology and, relatedly, its possible disparate impact on marginalized groups. At the same time, identifying individuals entering the country – and consequently determining whether they have a right to enter, or what risks they might pose – serves a national security function. In this way, the use of biometrics requires an assessment of the balance between privacy and security.

This report informs, contextualizes, and contributes to this conversation by presenting NSIRA's foundational study of the GoC's biometric activities in the border continuum.

The study identified a set of observations linked to nine overarching themes:

1. *Biometrics and National Security.* The centrality of national security as a justification for biometric activities has waned over time relative to other objectives, such as identity management and traveller facilitation. This makes it challenging to assess biometric activities *in general* as national security activities. Future NSIRA reviews may focus more narrowly on biometric activities that directly engage national security.
2. *The Steady-State Activities.* The steady-state biometric activities in the border continuum are generally well-supported by current legal authorities and are consistent with international practice.
3. *Expanding Use of Biometrics over Time.* The use of biometrics in the border continuum has significantly expanded over the last three decades, and is likely to continue expanding in the future. This trajectory is driven partly by advancing technological capabilities, partly by evolving challenges in identity management. It is reflected in other jurisdictions around the world. Exploiting the possibilities created by

technological developments and keeping pace with other jurisdictions cannot justify the expanded use of biometrics in their own right. New biometric activities must be justified according to the necessity and proportionality of collecting and using biometrics for particular, intended objectives.

4. *Pilot Projects.* Pilot projects and initiatives raise more concerns than do steady-state activities, as they risk being implemented on an experimental basis, without sufficient legal analysis or policy development. These projects represent an area of continued interest for NSIRA. Despite the temporary or experimental nature of a project, NSIRA expects that departments will conduct the analysis necessary to ensure that legal authority is in place for the conduct of the activity, and that the attendant collection, use, retention and disclosure of personal information is well-governed by policy.

5. *Evolving Legal and Societal Norms.* The public debate surrounding legal authorities questions whether existing standards and protections are sufficient for regulating biometric activities or whether new standards and protections are required. The border is, comparatively, a space in which greater intrusiveness is considered reasonable – but the boundaries of those justifications are not limitless, and will require careful calibration moving forward.

6. *The Dual-Use of Biometrics.* NSIRA observed several instances of possible dual-use of biometric information in the activities examined in this report. Even where they pose demonstrable benefits, new uses of biometrics must be carefully considered to ensure their reasonableness and proportionality. In addition, all new uses must be justified and well-authorized in law. The principle of "purpose limitation" may be a way of guarding against unjustified dual-use in the context of biometric activities.

7. *Technical Systems.* There is significant overlap between the technical systems and databases used across the steady-state biometric activities. The overall architecture of this system – biometric collection, transmission, and storage in the course of the GoC's activities in the border continuum – is complex, though not necessarily problematic.

8. *Visibility into Algorithms.* Departments and agencies have limited visibility into how the algorithms they use for biometric analysis operate. Each department and agency did, however, demonstrate that performance metrics are known and tested, and that custom thresholds are used when appropriate.

9. *Preventing Bias and Discrimination.* IRCC and CBSA have conducted preliminary analyses to explore how their biometric activities may impact diverse groups of people, though the implementation of possible mitigation strategies was not always

apparent. In some contexts, technological advancements have helped to reduce, but not eliminate, differential impacts. More work remains in terms of mitigating differential impacts on segments of the population. At the same time, the departments and agencies under review have demonstrated their awareness of possible systemic inequalities and their commitment to addressing them.

These observations are intended to contribute to Canadians' understanding of the complex and evolving use of biometrics in the border continuum, and to shape how NSIRA as an organization engages with this area in future work.

Public debate about the government's application of biometric technology will continue to evolve, driving change in the legal and regulatory frameworks associated with such activities. As such, continued scrutiny from NSIRA is warranted, particularly in those instances where the collection and use of biometric information is justified by explicit reference to national security outcomes.

List of Acronyms

AFIS – Automated Fingerprint Identification System

BEP – Biometrics Expansion Project

BSO – Border Service Officer

BTD – Biometrics Transformation Directorate

CBP – US Customs and Border Protection

CBSA – Canada Border Services Agency

CI – Central Index

CIBIDS – Canadian Immigration Biometric Identification System

CIC – Citizenship and Immigration Canada

CJIMS – Criminal Justice Information Management Service

COSMOS – Consular Management and Operations System

CoT – Chain-of-Trust

CSIS – Canadian Security Intelligence Service

CPIC – Canadian Police Information Centre

CPO – Canadian Passport Order

CTOB – Chief Transformation Officer Branch

DOJ – Department of Justice

DTC – Digital Travel Credentials

DRDC – Defence Research and Development Canada

EFCD – Electronic Fingerprint Capture Device

eTA – Electronic Travel Authorization

EURODAC – European Asylum Dactyloscopy Database

FOSS – Field Operations Support System

FOTM – Faces-on-the-Move

FRS – Facial Recognition Solution

GBA+ – Gender-Based Analysis Plus

GCMS – Global Case Management System

GoC – Government of Canada

IAPI – Interactive Advanced Passenger Information

IATA – International Air Transport Association

IBAS – Interdiction and Border Alert System

ICAO – International Civil Airline Organization

ICES – Integrated Customs Enforcement System

IIS – Immigration Information Sharing

INTERPOL – International Criminal Police Organization

IRCC – Immigration, Refugees, and Citizenship Canada

IRIS – Integrated Retrieval Information System

IRPA – Immigration and Refugee Protection Act

IRPR – Immigration and Refugee Protection Regulations

KTDI – Known Traveller Digital Identity

LBFC – Land Border Face Capture

M5 – Migration 5 group

NCIC – National Criminal Information Centre

NIST – National Institute of Standards and Technology

NPP – Notice of Proposed Procurement

NSIRA – National Security and Intelligence Review Agency

NSP – National Security Policy

NTWG – New Technology Working Group

OBIM – Office of Biometrics and Identity Management

OGD – Other Government Department

OPC – Office of the Privacy Commissioner

PIA – Privacy Impact Assessment

PIK – Primary Inspection Kiosk

PKI – Public Key Infrastructure

PMP – Passport Management Program

POE – Port(s) of Entry

PPMI – Passport Program Modernization Initiative

PROVE-IT:FRiV – Pilot and Research on Operational Video-based Evaluation of Infrastructure and Technology: Face Recognition in Video

RCMP – Royal Canadian Mounted Police

RTIDS – Real Time Identification System

SCIDA – Security of Canada Information Act

SFV – Systematic Fingerprint Verification

SL – Passport System Lookout

SLTD – Stolen, Lost Travel Document (INTERPOL)

TBID – Travelers Biometric Identification Determination System

TC – Transport Canada

TRBP – Temporary Resident Biometrics Program

VAC – Visa Application Centre

WEF – World Economic Forum

Glossary of Terms

Algorithm. A set of rules or calculations applied to data that generate an interpretable or reportable result.

Automation/Automated Decision-Making. Automated decision-making is the process of making a decision by automated means without any human involvement.

Biometric. The measurement and analysis of biological characteristics, such as fingerprints, iris patterns, retinas, DNA, and hand or face geometry, and to the analysis of certain behavioural characteristics, such as voice, gait or typing rhythm.

Biometric Data Subject. An individual whose individualized biometric data is within the biometric system.

Biometric Information. Biometric information refers to biometric data records (data record containing biometric data such as a biometric sample or aggregation of biometric samples at any stage of processing).

Biometric Template. Set of stored biometric features comparable directly to prove biometric features.

Enrolment. Act of creating and storing a data record attributed to a biometric data subject, containing non-biometric data and associated with one or more biometric samples, biometric templates, or biometric models attributed to a biometric data subjects and used as the object of biometric comparison.

Facial Recognition. Automated recognition of individuals based on their facial characteristics.

False-Negative. Failure to associate a biometric probe and a biometric reference belonging to the same biometric data subject.

False-Positive. Incorrect association between a biometric probe and a biometric reference from different biometric data subjects.

Identity Management. The set of principles, practices, policies, processes and procedures used to realize an organization's mandate and its objectives related to identity.

One-to-one verification. Process in which biometric probe(s) from one biometric data subject is compared to biometric reference(s) from one biometric data subject to produce a comparison score.

One-to-many identification. Process in which biometric probe(s) from one biometric data subject is compared against the biometric references of more than one biometric data subject to return a set of comparison scores.

Biometric probe. A biometric sample or biometric feature set input to an algorithm for biometric comparison to a biometric reference(s).

2. AUTHORITIES

The National Security Review Agency (NSIRA) conducted this study under section 8(1)(b) of the *National Security and Intelligence Review Agency Act*.

3. INTRODUCTION

Background

1. Biometrics enhance the government's ability to know who you are. The measurement and analysis of unique biological characteristics – including, *inter alia*, fingerprints, iris patterns, and facial features – facilitates the identification of individuals to a level of confidence beyond what is possible absent the use of such techniques. Biometrics can be layered with traditional identifiers – such as name, date of birth, place of birth, gender etc. – to enhance the government's identification process.
2. Knowing who you are – including verifying that you are who you claim to be – has benefits for national security. At the border, in particular, questions about identity are paramount: who has the right to enter the country, who does not, and who might pose a threat to the security of Canada and Canadians?
3. At the same time, the identification of persons by virtue of their biological characteristics raises acute privacy and human rights concerns. Biometrics are intrinsically personal information, and are largely immutable (i.e., they cannot be easily changed, as can passwords or other identifiers). There is public apprehension about the government's use of biometric analysis, as reflected in discussions regarding the use of facial recognition technology and, relatedly, its possible disparate impact on marginalized groups.[1] As biometric technology is increasingly integrated into

[1] Tamir Israel, "Facial Recognition at a Crossroads: Transformation at Our Borders and Beyond," Ottawa: CIPPIC, September 2020. Accessed 13 August 2021. https://cippic.ca/uploads/FR_Transforming_Borders.pdf; Petra Molnar, "Technological Testing Grounds: Migration Management Experiment and Reflections from the Ground Up," EDRi/Refugee Law Lab, 2020. Accessed 13 August 2021. https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf; Hilary Beaumont, "When

public spaces, it will be important for government and for Canadians to consider the associated calibration of security, privacy, and human rights.

4. This report informs, contextualizes, and contributes to this conversation by presenting NSIRA's foundational study of the Government of Canada (GoC)'s biometric activities in the border continuum[2], with a focus on activities relating to the screening of foreign nationals seeking admission to Canada and the identification of passengers travelling internationally by air.[3] The immediate objective of the study was to map the biometric activities occurring in this space. This includes examining the collection, retention, use, and disclosure of biometric information, as well as the legal authorities under which said activities occur. The baseline for an informed public discussion is accurate information about which activities are being pursued by the GoC and whether/how they are authorized in law.

5. The study also considered the reasonableness and necessity of these activities, studying the accuracy and reliability of biometrics, including the possibility of discrimination on the basis of identity factors like race and gender; the proportionality of their collection, retention, use and disclosure; and the transparency with which the GoC discusses its use of biometrics and their contribution to national security.

6. NSIRA's ability to look across departments and agencies and to make both specific and general observations – to examine the forest as well as the trees – was particularly valuable in assessing a wide and growing biometric landscape.

7. In addition to informing an important public conversation, the report's broad treatment of biometric activities in the border continuum advances NSIRA's work in two ways. First, it identifies several more narrow areas of interest or concern, to which NSIRA may return in future targeted reviews. Second, it defines a set of criteria against which NSIRA may review the GoC's use of biometrics in national security and intelligence activities – both within and beyond the border continuum.

Border Security Crosses a Line," *The Walrus*, March/April 2020. Accessed 13 August 2021. https://thewalrus.ca/when-border-security-crosses-a-line/.

[2] The term "border continuum" is used here to refer to the activities and processes associated with the international movement of individuals, including foreign nationals coming to Canada (immigration applicants, refugees, and asylum claimants) and Canadian citizens and permanent residents travelling internationally with Canadian-issued travel documents (e.g. passports).

[3] Accordingly, our analysis did not extend to matters of in-land enforcement of border legislation, although we note the CBSA's use of voice recognition in this space. As an alternative to presenting at a CBSA in-land office, individuals may choose to have their voice recorded and verified over the phone using voice recognition. GPS data can then confirm the individual's location, and therefore compliance with applicable immigration requirements. CBSA briefing to NSIRA, 22 October 2020.

The Study

Scope

8. The border is distinct from other public settings. There are security imperatives that arise when individuals cross sovereign boundaries, such that the state is justified in taking measures not permissible in other contexts.[4] While privacy rights and civil liberties do not disappear, expectations of privacy and of free movement are significantly lower. In considering the GoC's biometric activities, therefore, it was practical to separate the border continuum from other settings; what might be overly intrusive in the latter may be justified in the former. Further, the border can serve as a testing ground for new biometric techniques and technologies, which then spread to other areas.[5] If there are public concerns about biometric technology more generally, the border may serve as a harbinger of things to come and ought to be scrutinized accordingly.

9. In this study, we examine the collection, retention, use, and disclosure of biometric information and evaluate, where applicable, said activities against the criteria outlined below. We reviewed relevant policy and legal frameworks as communicated by departments and agencies, to inform our assessment of reasonableness and necessity, and to establish foundational knowledge that will inform future compliance assessments in the biometrics space. Our assessment of reasonableness and necessity was conducted at a high-level, reflecting on the themes, trends and issues manifest in considering the GoC's biometric activities in the border continuum as a whole. We did not conduct independent verification or audit of the claims or activities themselves.

10. In the course of this study, NSIRA examined activities conducted by the Canada Border Services Agency (CBSA), Immigration, Refugees, and Citizenship Canada (IRCC), and Transport Canada (TC). The study also extended to the Royal Canadian Mounted Police (RCMP), which plays a supporting role in one of the major IRCC-led programs in the border continuum.

11. NSIRA also surveyed the history, and possible future, of biometric activities in the border continuum. The biometric landscape is not static, nor are practices in traveler facilitation and border security. Much of the public concern regarding biometrics (in particular over something like facial recognition technology) has to do with what lays just over the horizon, rather than simply any activity currently taking place. To this end, discussion of past activities, programs, and pilot projects illustrate the expansion of biometrics that has culminated in the present moment.

---

[4] For a discussion of why the border is unique in case law see paragraphs 22-28 of R. v. Simmons, 1988 CanLII 12 (SCC), [1988] 2 SCR 495. Accessed 18 August 2021. https://www.canlii.org/en/ca/scc/doc/1988/1988canlii12/1988canlii12.html?resultIndex=2.

[5] See Molnar, "Technological Testing Grounds."

Similarly, several pilot projects and initiatives known to be in development serve as examples of what may be to come. This wider lens contextualizes present activities and thus helps fulfill the broader objectives of the study.

Criteria

12. A set of basic criteria guided NSIRA's assessment of the GoC's present biometric activities in the border continuum:

    - *Compliance*. NSIRA examined the legislative and policy framework governing departments' and agencies' collection and use of biometrics. It examined the enabling legislation's compliance with the *Canadian Charter of Rights and Freedoms* and *Privacy Act*; considered the safeguards and features of the departments' or agencies' enabling statutes and regulations as applies to their biometric programs; and reviewed applicable departmental and Treasury Board policies.
    - *Proportionality*. Proportionality, in this context, weighs the government's objectives in using biometrics against any impacts on individuals' privacy or human rights. Generally speaking, NSIRA expects that any intrusions on the rights and freedoms of individuals be readily justifiable and offer important benefits to pressing and substantial objectives.
    - *Accuracy*. Because biometrics are fundamentally designed to identify individuals, it is important that they do so accurately, such that they can effectively contribute to the government's objectives in a given activity/program. Biometric analysis (including the use of algorithms) is subject to error rates and false-matches that can have significant consequences for individuals. Relatedly, algorithms used for biometric analysis are susceptible to demographic performance variables which could give rise to bias or discrimination.
    - *Transparency*. In light of the GoC's *National Security Transparency Commitment* of 2017, this criterion generally assessed the public transparency of biometric activities in the border continuum. It emphasized the availability of information regarding the type of biometrics collected and the connection of biometrics to GoC priorities, including national security.
    - *Data Security*. Given the sensitive nature of biometric information, protection of said data throughout the so-called "privacy lifecycle" (collection, storage, transmission, and destruction) is particularly important. As such, NSIRA assessed the policy frameworks of the activities under review for data security protections, such as encryption, access limitations, and privacy-by-design principles.

13. Collectively, these criteria informed NSIRA's assessment of the lawfulness, reasonableness and necessity of the departments' exercise of their powers as concerns the use of biometrics in

Canada's border continuum. Our observations highlight potential issues and areas of concern, which may serve as a basis for subsequent in-depth review of particular activities.

Methodology and Information Requirements

14. NSIRA received information from departments and agencies in the form of briefings, written responses, and documents. The latter included policies, procedures, project reports, technical studies, operational bulletins, manuals, correspondence, websites, and relevant legal opinions.

15. In addition to information obtained from departments and agencies, the nature of the study – dealing with a broad category of information widely used and heavily scrutinized across the globe – meant that a significant volume of open-source research was pertinent. As such, NSIRA examined media reports (both domestic and international), industry reports, academic research, think tank reports, government reports/documents from other jurisdictions, and inter-governmental and non-governmental organization research on biometrics and related technology. What emerged was a sense of the common standards, themes, risks, and even lexicon associated with biometrics, all of which helped inform NSIRA's observations regarding the GoC's biometric activities in the border continuum.

The Report

16. The body of the report is organized into three descriptive sections, presented in chronological order:

    - *Biometrics Past:* a discussion of the history and evolution of the use of biometrics in the border continuum, including relevant pilot projects and key expansions along the way;
    - *Biometrics Present:* a description of current, steady-state biometric activities; and,
    - *Biometrics Future:* a discussion of the role biometrics are likely to play in the border continuum moving forward, based on present trajectories.

17. The concluding section unpacks overarching themes and observations pertinent to the study objectives outlined above. While some of these observations are specific to a particular program or activity, others apply horizontally across various aspects of the study. The mélange reflects both the nature of a foundational study and the unique, crosscutting mandate that NSIRA enjoys. Our observations are intended to contribute to Canadians' understanding of the complex and evolving use of biometrics in the border continuum, and to shape how NSIRA as an organization engages with this area in future work.

4. BIOMETRICS *PAST*

18. IRCC began collecting fingerprints from asylum claimants and deportees in 1993,[6] partly as a consequence of the rise in global migration volumes following the end of the Cold War. Canada received 37,000 refugee protection claims in 1992, up from just a few thousand annually for the balance of the 1980s.[7] The resulting pressure on the system led, in part, to the introduction of Bill C-86 in June 1992, which included several provisions designed to enhance the efficiency and integrity of Canada's immigration and refugee system, among them the fingerprinting of asylum claimants and deportees.[8] This provision generated public criticism, with the government eventually amending it to include the deletion of fingerprints if/when an individual became a Canadian citizen.[9] Ultimately, the purpose of the collection was to introduce processing efficiency into the system and to enhance both fraud detection and fraud deterrence through rigorous identity management.[10]

19. Over the subsequent years, the collection and use of biometrics in the border continuum has steadily expanded, such that nearly everyone entering Canada by air – whether a foreign national or Canadian citizen – now has their biometric information collected and/or analyzed in some way. How did we get from there to here? The present section addresses this question by describing the evolution of the GoC's activities over time, highlighting key moments, programs, and projects that animate it along the way.

9/11

20. The terrorist attacks of September 11, 2001, dramatically altered Canada's national security landscape. The 2001 budget reflected the new priorities of the day, with $7.7 billion over five

---

[6] IRCC, "Evaluation of the Biometrics (Steady State) and Canada-United States Immigration Information Sharing (IIS) Initiatives," October 2019, p. 1. [NSIRA_202002_005, p. 1.]

[7] Ninette Kelley and Michael J. Trebilcock, *The Making of the Mosaic: A History of Canadian Immigration Policy.* (Toronto: Toronto University Press, 2010), p. 381.

[8] Valerie Knowles, *Strangers at Our Gates: Canadian Immigration and Immigration Policy, 1540-2015.* (Toronto: Dundurn Press, 2016), p. 239. National security considerations were also present in the bill; for a discussion, see Sharryn J. Aiken, "Of Gods and Monsters: National Security and Canadian Refugee Policy," *Revue Quebecoise de droit international*. 2001. 14 (2). Accessed 19 August 2021. https://www.sqdi.org/wp-content/uploads/14.2_-_aiken.pdf.

[9] *Strangers at Our Gates,* p. 240.

[10] *Strangers at Our Gates,* p. 239. For example, an individual could not submit multiple applications under multiple names, or resubmit under a different name if a previous application had been rejected.

years allocated to security measures, including $1 billion to immigration screening and enforcement and $1.2 billion to border security initiatives.[11]

21. These outlays came on the heels of explicit recommendations from a parliamentary committee to, among other things, "modernize border management to accommodate future security and trade needs" and "test and implement [...] advanced technologies in [...] border processing operations."[12] The latter recommendation included the suggestion that "biometric technology in the form of fingerprint or retina scanners could [...] be considered to identify individuals [...] crossing the border."[13] The report also called for the reactivation and full implementation of the NEXUS program, which had been a cross-border travel pilot project between the US and Canada launched in November 2000 but suspended in the wake of the attacks.

22. The central plank of post-9/11 US-Canada border security cooperation, however, was the *Smart Border Declaration*, signed on December 12, 2001. Accompanied by a 30-point Action Plan, the declaration guided US and Canadian efforts to enhance border security. The very first item on the Action Plan was the introduction of "biometric identifiers", calling for the two countries to "develop on an urgent basis common biometric identifiers in documentation such as permanent resident cards, NEXUS, and other travel documents to ensure greater security."[14] Also of note were the provisions to expand information sharing in the visa and refugee/asylum context.[15]

23. The two countries explicitly framed the *Smart Border Action Plan* as an effort to "develop a zone of confidence against terrorist activity"[16]. In the US, the *Final Report of the National Commission on Terrorist Attacks Upon the United States* (more widely known as the "9/11 Commission Report") expressed this logic, calling for a "biometric screening system" that would encompass the entire border continuum, from passport and immigration application to arrival at ports of

---

[11] Department of Finance Canada, *The Budget Plan 2001: Supplementary Information and Notices of Ways and Means Motions Included*, Ottawa, 2001. Accessed 1 September 2021. https://www.budget.gc.ca/pdfarch/budget01/pdf/bpe.pdf.

[12] House of Commons Canada, *Towards a Secure and Trade-Efficient Border: Report of the Standing Committee on Foreign Affairs and International Trade,* Ottawa, pp. xi-x. Accessed 1 September 2021.

https://www.ourcommons.ca/DocumentViewer/en/37-1/FAIT/report-13/.

[13] House of Commons Canada, *Towards a Secure,* p. 15.

[14] Legislation Online, "U.S. and Canada Smart Border Declaration (2001). Accessed 1 September 2021. https://www.legislationline.org/documents/id/7543.

[15] Legislation Online, "U.S. and Canada Smart Border."

[16] Office of Homeland Security, "Action Plan for Creating a Secure and Smart Border," 12 December 2001. Accessed 13 September 2021. https://georgewbush-whitehouse.archives.gov/news/releases/2001/12/20011212-6.html.

entry, along with information sharing between jurisdictions.[17] Canada's 2004 *National Security Policy* (NSP) similarly foregrounded biometrics in its chapter on border security.[18] The NSP noted that Canada would "work toward a broader use of biometrics" and "examine how to use biometrics in [its] border and immigration systems to enhance the design and issuance processes of travel and proof-of-status documents and to validate the identity of travellers at [Canada's] ports of entry."[19] For both countries, biometrics were seen as a means of identifying possible terrorists crossing the border. 9/11 had fused border security to national security, turning identity management – hitherto primarily associated with efficiencies and fraud – into a national security priority.

24. In Canada, the NSP set the basic outline of the GoC's current steady-state biometric activities: facial recognition in the issuance and use of travel documents (Passport Program) and fingerprints and the validation of identity at ports of entry (Immigration Program). We return to these in Section 5.

25. In the balance of this section, we briefly describe the key biometric activities and programs adopted in the years following 9/11.

ePassport

26. Though standard in the document for decades, passport photographs were not considered "biometrics" until passports became machine-readable. The 2003 International Civil Aviation Organization (ICAO) guidelines on ePassports, also commonly referred to as "biometric passports," therefore mark the introduction of biometric identifiers to the document on the international stage. Canada committed to the ePassport in 2004, though actual implementation unfolded in stages over subsequent years, with the full rollout occurring in 2013. Hundreds of

[17] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, Washington, 2004. Accessed 1 September 2021. http://govinfo.library.unt.edu/911/report/911Report.pdf. The report also articulates an important shift in how these issues were viewed, noting that "[i]n the decade before September 11, 2001, border security – encompassing travel, entry, and immigration – was not seen as a national security matter," but that following the attacks ""travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack" (pp. 383-84).

[18] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, Ottawa, April 2004, p. 41. Accessed 19 July 2021. https://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

[19] Privy Council Office, *Securing an Open Society*, p. 45.

other jurisdictions adopted the ePassport during this period,[20] gradually establishing it as an international recommended practice for official travel documents. Canada's current iteration of the ePassport is discussed in paragraphs 95-112, below.

27. In addition to the "smart chip" embedded in the ePassport and containing the facial photograph, the government also pursued facial recognition in the passport application/issuance process. The first Privacy Impact Assessment (PIA) for what was then known as the "Facial Recognition Project" was crafted in 2003, though full implementation under the guise of the "Facial Recognition Solution" (FRS) did not occur until 2010. The system used facial recognition to help assess entitlement to a Canadian passport or other official Canadian travel document.[21] The specific objectives of the program were: to detect fraud, support the authentication of identity, and prevent passport issuance to ineligible applicants.[22] We discuss the current iteration of the FRS, which is a key component of the steady-state Passport Program, in paragraphs 95-112, below.

Temporary Resident Biometrics Program (TRBP) (2009-2018)

28. The "Temporary Resident Biometrics Program" (TRBP) – initiated in 2009[23] and operational by 2013 – marked a significant expansion of the collection of biometrics in the immigration context. Under the TRBP, biometrics (fingerprints and a digital photograph) were collected by IRCC (then-Citizenship and Immigration Canada [CIC]) as part of temporary resident applications[24] from 30 nationalities.[25] The fingerprints were screened "against fingerprint records of known criminals, past refugee claimants, persons previously deported, and previous immigration applicants" held

---

[20] Globally, 60% of passports issued in 2009 were ePassports. By 2013, at least 100 countries had adopted some version of the document. See Government of Canada, "History of the ePassport," May 13, 2014. Accessed 1 September 2021. https://www.canada.ca/en/news/archive/2014/05/history-epassport.html.

[21] E.g. Certificates of Identity or Refugee Travel Documents for non-Canadians.

[22] Passport Canada, "PIA Facial Recognition Project 2011", p. ii. [IRCC RFI #2 Documents]

[23] Budget 2008 allocated $26 million over two years to the project, intending to "enhance the integrity and efficiency of the border by preventing criminals from entering Canada, and facilitating the processing of legitimate applicants." Department of Finance Canada, "The Budget Plan 2008," February 26, 2008. Accessed 18 August 2021. https://www.budget.gc.ca/2008/pdf/plan-eng.pdf, p. 187. See also Government of Canada, "Biometrics Expansion Project: Project Charter," Project Delivery Office, July 20, 2018, p. 2. [NSIRA_202002_033, p. 2.]

[24] Temporary resident applications include visitor (tourist) visas, work permits, and study permits.

[25] The list included: Afghanistan, Albania, Algeria, Bangladesh, Burma (Myanmar), Cambodia, Colombia, Democratic Republic of Congo, Egypt, Eritrea, Haiti, Iran, Iraq, Jamaica, Jordan, Laos, Lebanon, Libya, Nigeria, Pakistan, Saudi Arabia, Somalia, South Sudan, Sudan, Sri Lanka, Syria, Tunisia, Vietnam, Yemen, and the Palestinian Authority. See IRCC, "Evaluation of the Biometrics (Steady State), p. 35. [NSIRA_202002_005, p. 35.]

by the GoC.[26] Once the application was approved and the applicant arrived in Canada, the CBSA verified[27] the biometrics ensuring that the person presenting was the same individual that had applied. In 2014, biometrics collection was expanded beyond temporary resident applications to include overseas refugee and resettlement applications.[28]

29. According to the GoC, biometrics were adopted as a means to access more complete and accurate information, so as to inform admissibility decisions made under the *Immigration and Refugees Protection Act* (IRPA)[29] regarding temporary resident applicants.[30] The TRBP's use of biometrics therefore supported identity management goals, with national security – the identification of individuals who might pose a security threat – constituting a supporting feature of the larger program.

Beyond the Border (2011) and Immigration Information Sharing (IIS) (2013-2016)

30. In 2011, Canada and the US issued the joint declaration *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness* and its accompanying "Beyond the Border Action Plan". The plan made a commitment to increase information sharing between the two countries.[31] Canada and the US had shared immigration information on a case-by-case, *ad hoc* basis since 2003, but the process was labour intensive and consequently limited in volume.

---

[26] Government of Canada, "Biometrics Expansion Project: Project Charter," Project Delivery Office, July 20, 2018, p. 2. [NSIRA_202002_033, p. 2.]

[27] On a discretionary basis at select POE.

[28] "CBSA, "Biometrics Expansion Transition," March 4, 2020, p. 2. [NSIRA_202002_009, p. 2.] Technically, this expansion was not part of the TRBP, which dealt with temporary resident applicants only. Collection from overseas refugee and resettlement applications occurred under separate, discretionary authorities. Taken together, however, the collection of biometrics from deportees and asylum claimants, from temporary resident applicants as part of the TRBP, and from refugee and overseas resettlement applicants, constituted the biometrics steady-state at that moment in time.

[29] Under the IRPA, which came into force in 2002 and is still in effect today, individuals can be found inadmissible for entry into Canada for reasons of security (s34), human or international rights violations (s35), criminality (s36 and s37), health (s38), financial insufficiency (s39), misrepresentation (s40), non-compliance (s41), or because of an inadmissible family member (s42).

[30] Government of Canada, "Temporary Resident Biometrics Project (TRBP) summary," December 27, 2020. Accessed 21 July 2021. https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/access-information-privacy/privacy-impact-assessment/temporary-resident-biometrics-project-2012.html

[31] The White House, "United States-Canada Beyond the Border: A Shared Vision Perimeter Security and Economic Competitiveness," December 2011. Accessed 21 July 2021. https://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf, p. iii.

31. The resulting program was the Immigration Information Sharing (IIS) initiative, which made it possible for Canadian and American authorities to systematically exchange immigration information on the basis of a biometric match between their respective immigration databases – a capability that became fully operational in August 2015.[32] For example, all biometric-required applicants to Canada[33] had their fingerprints systematically checked against US fingerprint holdings at the time of enrolment.[34] In the event of a match, the US returned relevant immigration information (e.g. biographical information to confirm identity, the outcome of any previous immigration applications, etc.) to IRCC, to help inform decisions about admissibility. The arrangement was reciprocal, meaning the US similarly queried Canadian immigration fingerprint holdings, with Canada returning immigration information in the event of a match. As characterized by a 2015 implementation report, this capability helped to "counter identity fraud, strengthen identity management and provide valuable information to inform respective admissibility determinations."[35]

32. The IIS was, in many ways, the natural extension of TRBP. Whereas TRBP made it possible to screen an applicant's biometrics against domestic databases, IIS extended this capability to US databases, thereby increasing the range of information obtainable through biometric querying.

Information-Sharing Pilot between CBSA and IRCC/CIC (2013-2016)

33. Beginning in 2013, a two-phase pilot project between CBSA and IRCC/CIC explored the benefits of leveraging facial recognition through information sharing. The impetus for the project was the experimental querying of 72 photographs of individuals wanted by the CBSA against IRCC/CIC's passport database. The querying was intended to verify whether any passports had been issued to individuals subject to CBSA warrants for arrest under the *IRPA* (under genuine or false identities), thus helping protect the integrity of the passport system, while also facilitating

---

[32] IRCC, "Evaluation of the Biometrics (Steady State)…"p. 3. [NSIRA_202002_005, p. 3]; see also Public Safety Canada, "2015 Beyond the Border Implementation Report," September 29, 2016. Accessed 21 July 2021. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2015-bynd-brdr-mplmntn/index-en.aspx. The IIS initiative also included information-sharing on the basis of biographical information.

[33] At the time, these were temporary resident applicants from 30 nationalities, as per the TRBP, as well as resettled refugee applicants and asylum claimants.

[34] Under the TRBP approximately 400,000 queries were sent per year. Government of Canada, "Biometrics Expansion Project: Project Charter," p. 3. [NSIRA_202002_033, p. 3.]

[35] "2015 Beyond the Border Implementation Report," September 29, 2016. Accessed 21 July 2021. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2015-bynd-brdr-mplmntn/index-en.aspx

enforcement of the *IRPA*. The CBSA and IRCC rely on sections 7, 8(2)(a) and 8(2)(e) of the *Privacy Act* for the use and disclosure of this information.[36]

34. Using facial recognition, the one-to-many identification of these 72 individuals identified three individuals who had fraudulently acquired travel documents. On the strength of these results, the organizations drafted a Memorandum of Understanding (MOU) in December 2013 to share photographs of 1,000 individuals wanted on active CBSA warrants and ran a one-to-many identification against the passport database using facial recognition. This time, 15 individuals were found to have submitted fraudulent passport applications.[37]

35. In 2015, another round of the project was initiated under a subsequent MOU, raising the number of queries to 3,000 individuals. Also expanded was the scope of information that could be returned as a result of a positive match. Whereas the 2013 MOU only authorized the sharing of information related to document fraud, the 2015 MOU authorized the sharing of any derogatory information[38] relevant to the enforcement of the *IRPA*.[39] Appendix III of the Information Sharing Annex to the 2017 IRCC-CBSA MOU established this information sharing on a permanent basis.[40]

---

[36] IRCC and CBSA, "Information Sharing Annex: IRCC-CBSA Memorandum of Understanding," 2017, p. 156. Annex covers both immigration and customs information. [NSIRA_202004_156, p. 12]. Information-disclosures from the CBSA to the IRCC may rely on s. 8(2)(a) of the *Privacy Act* (consistent use), s. 5 of *SCIDA,* or, in the case of customs information: s.107(5)(j) of the *Customs Act,* which authorizes the CBSA to disclose information collected for the purpose of the *Customs Act* or *Customs Tariff* to IRCC for the purposes of administering or enforcing the *Citizenship Act,* the *IRPA*, or the law of Canada respecting passports and other travel documents (see also para 5 of Appendix III). The IRCC, in turn, may rely on s.8(2)(a) of the *Privacy Act* as well (consistent use) or s. 8(2)(e) of the *Privacy Act* where the disclosure is made to three branches of the CBSA (the Inland Enforcement Division; the Intelligence and Targeting Operations Directorate; and Criminal Investigations Division). These branches are the CBSA units specified as eligible "investigative bodies" for the purposes of s. 8(2)(e) in Schedule II of the *Privacy Regulations*.

[37] CBSA, "CBSA – Citizenship and Immigration Canada Information Exchange on Individuals Wanted Under the Immigration and Refugee Protection Act," N.D.,

[38] In this context, derogatory information is information that may indicate a contravention of the relevant legislation.

[39] CBSA, "CBSA – Citizenship and Immigration Canada Information Exchange," p. 2. [NSIRA_202002_065, p. 2.]

[40] IRCC and CBSA, "Information Sharing Annex: IRCC-CBSA Memorandum of Understanding," p. 12. [NSIRA_202004_156, p. 12.]

Research into Facial Recognition

36. In addition to the expansion, refinement, and leveraging of biometric activities associated with passports and immigration, the GoC explored additional uses of biometrics, including facial recognition, through research into emerging technologies and pilot initiatives, testing possible applications in the border continuum.

Pilot and Research on Operational Video-based Evaluation of Infrastructure and Technology: Face Recognition in Video (PROVE-IT: FRiV) (2011-2013)

37. In 2011, CBSA led[41] the "Pilot and Research on Operational Video-based Evaluation of Infrastructure and Technology: Face Recognition in Video" (PROVE-IT: FRiV) project. PROVE-IT: FRiV examined, in a lab setting, the possible use of live-capture facial recognition in a controlled environment, such as an airport.[42] Researchers evaluated commercial products and tools available for this purpose, and determined that "face-based surveillance" was ready for live use in "in semi-constrained environments."[43]

Faces on the Move (FOTM) (2014-2017)

38. Building on the findings and results of PROVE-IT: FRiV, CBSA launched the "Faces on the Move" (FOTM) pilot project in 2014.[44] FOTM involved the live video capture of the facial images of travellers as they passed through Toronto Pearson International Airport Terminal 3 for a six-month period between June 2016 and November 2016.

---

[41] Along with École de technologie supérieure [ETS] and supported by multiple partners including the RCMP, Defence Research and Development Canada (DRDC), Transport Canada, the Department of Foreign Affairs and International Trade (DFAIT), the Pricy Council Office (PCO), the University of Ottawa, the FBI (US), the Home Office (UK), and the National Institute of Standards and Technology (NIST).

[42] CBSA, "PROVE-IT: FriV: Framework and Outcomes," April 2014. Accessed 22 July 2021. https://www.nist.gov/document/14-nist-friv-gorodnichy-ppdf.

[43] Face4 Systems Inc., "Canada Border Services Agency Faces-on-the-Move Demonstration Project: High-Level Architecture," N.D., p. 1. [NSIRA_202002_070, p. 1.] The results of the PROVE-IT (FRiV) project were reported in 2014 at the "International Biometrics Performance Conference" hosted by the National Institute of Standards and Technology (NIST). See NIST, "IBPC 2014 Presentations," December 5, 2016. Accessed 22 July 2021. https://www.nist.gov/itl/iad/image-group/ibpc-2014-presentations.

[44] The industry partner for the project was Face4 Systems Inc., a private technology firm headquartered in Ottawa, Canada. École de technologie supérieure (ETS) provided oversight of test methodology and analysis.

39. Project-specific video cameras were installed to capture facial images in the immigration arrivals area, primary inspection, and toward the exit following primary processing.[45] Facial images were checked in real time using facial recognition against two image databases: a "control" watchlist comprised of 65 CBSA volunteers, and an "operational" watchlist of 4,860 previously deported individuals, generated by CBSA. The CBSA volunteers conducted over 1,200 test walkthroughs over the course of the six-month demonstration. At the same time, approximately 15,000 to 20,000 travellers per day were screened against the operational watchlist, of which forty-seven were correctly detected by the system.[46] All records of personal information were to be destroyed at the end of the project, save those that served an administrative purpose, which would be retained for two years following the date of their last use in keeping with section 6(1) of the *Privacy Act* and section 4(1)(a) of the *Privacy Regulations.*[47]

40. The immediate purpose of FOTM was to raise the technology readiness level of facial recognition to the point of being ready for live, real-time implementation in a controlled environment.[48] Further objectives included the establishment of privacy and security protocols governing the deployment of facial recognition and the development of Canadian industry offerings in the facial recognition space through partnership with CBSA and access to the CBSA's operational environment (i.e. the border). Longer-term strategic goals included promoting the "efficient flow of people across Canada's borders" and addressing "evolving threats to public safety at or before the border…while respecting Canadian values including the right to privacy."[49] Ultimately, FOTM was couched as a building block toward future applications of facial recognition in the border

---

[45] Face4 Systems Inc., "Face4 Final Report for CSSP Project CSSP – 2014…," p. 25. [NSIRA_202002_072, p. 25.]

[46] There were additionally twenty-five on-line adjudication errors, and the overall adjudication error rate was 0.34%. [NSIRA_202002_070, p. 57.] On-line adjudication errors refer to the incorrect confirmation of a watchlist hit by a human operator in real time in the airport. Off-line adjudication, by contrast, happened outside of the live operational environment, without the attendant time pressure. While the system generated multiple false positive matches per day, human adjudication was required to confirm any matches flagged by the system. Adjudication errors are therefore more consequential than false positive matches, with the latter being a known and necessary product of the relevant technology (the relative sensitivity of the match threshold will generate more or less false positive/negative matches) while the former is the actual failure of the system as a whole, including human operators.

[47] CBSA, "Privacy Impact Assessment (PIA) Executive Summary: Archived – Faces on the Move: Multi-camera screening," July 22, 2016. Accessed 23 July 2021. https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/fotm-eng.html; Privacy Act, RSC 1985, c P-21; Privacy Regulations, SOR/83-508.

[48] Face4 Systems Inc., "Canada Border Services Agency Faces-on-the-Move Demonstration Project: Test Plan," N.D., p. 1. [NSIRA_202002_069, p. 1.] Face4 Systems Inc., "Face4 Final Report For CSSP Project CSSP – 2014 – CP – 2000, Faces-on-the-Move Multi-Camera Watchlist Screening," March 31, 2017, p. 12. [NSIRA_202002_072, p. 12.]

[49] Face4 Systems Inc., "Faces-on-the-Move Demonstration Project: Concept of Operations (CONOPS)," N.D., p. 1. [NSIRA_202002_068, p. 1.]

continuum and "similar security scenarios (transportation facilities, shopping malls, stadiums, mass public events)."[50] The lessons from FOTM were to inform a "roadmap" for the use of "science and technology […] for face surveillance, specifically at the border."[51]

41. According to the project's final report, FOTM experienced several policy challenges, "including concept of operation, deployment constraints, public notification, data security, data retention/purging rules, and legality of enforcement based on face recognition and privacy issues."[52] These and other challenges were likely to "influence face surveillance future deployments and/or technology road maps." Nonetheless, it recognized that the combination of advancing capabilities and relaxing public resistance to facial recognition technology "will drive the need for continual investment in both the science and the application of face recognition based surveillance."[53]

42. Prior to the demonstration period, a PIA conducted for FOTM in consultation with the OPC had brought additional issues to light.[54] This resulted in certain changes to the project, including dropping plans to use watchlist photographs from multiple government agencies and foregoing plans to advise enforcement agencies of a previously deported person's presence if the individual was not intercepted by the CBSA before leaving the port of entry.[55] The consultants' final report for the project "recognized that should facial recognition be deployed for long-term, operational use, the PIA would have to be redone and updated to identify potential ongoing risks that did not affect the short-term FOTM project."[56] Furthermore, CBSA recognized that, were FOTM to become a permanent program, the use of facial recognition would require an update to its *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology,* and to the

[50] Face4 Systems Inc., "Face4 Final Report For CSSP Project CSSP – 2014…," p. 11. [NSIRA_202002_072, p. 11.]

[51] Face4 Systems Inc., "Faces-on-the-Move Demonstration Project: Test Plan," pg. 1. [NSIRA_202002_069, p. 1.]

[52] Face4 Systems Inc., "Face4 Final Report For CSSP Project CSSP – 2014…," p. 71. [NSIRA_202002_072, p. 71.]

[53] Face4 Systems Inc., "Face4 Final Report For CSSP Project CSSP – 2014…," p. 72. [NSIRA_202002_072, p. 72.]

[54] CBSA, "Privacy Impact Assessment (PIA) Executive Summary: Archived – Faces on the Move: Multi-camera screening," July 22, 2016. Accessed 22 July 2021. https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/fotm-eng.html.

[55] Face4 Systems Inc., "Face4 Final Report For CSSP Project CSSP – 2014…," p. 21. [NSIRA_202002_072, p. 21.]

[56] Face4 Systems Inc., "Face4 Final Report For CSSP Project CSSP – 2014…," p. 21. [NSIRA_202002_072, p. 21.]

description of the related CBSA Personal Information Bank[57] (PIB), PPU 1104, which did not include "biometric information."[58]

43. Indeed, public signage and notice about the cameras was limited during the demonstration period. Signage at Terminal 3 of Toronto Pearson's International airport stated that "[t]his area is under video surveillance," but made no mention of facial recognition.[59] Similarly, the November 19, 2012, version of the CBSA's Privacy Notice on Video Monitoring and Recording, referred to in the PIA for FOTM, discloses that "[c]ameras may [...] monitor the movement of travelers and goods from one point of CBSA operation to another, for example, from primary to secondary,"[60] but does not provide notice of a facial recognition capability.[61] These lacunae in the notice provisions appear to have been acknowledged in the final report on FOTM, however, which notes that the machine learning component "may require an extension to the current [privacy and security] protocols."[62]

44. To date, FOTM or similar use of facial recognition has not been adopted as an ongoing activity. Other operational priorities, including the deployment of Primary Inspection Kiosks (PIKs) at select airports,[63] took precedence at the time the project was completed, and CBSA has not

---

[57] The OPC defines PIBs as "descriptions of personal information under the control of a government institution that is organized and retrievable by an individual's name or by a number, symbol or other element that identifies that individual. The personal information described in a PIB has been used, is being used or is available for an administrative purpose. The PIB describes how personal information is collected, used, disclosed, retained and/or disposed of in the administration of a government institution's program or activity." Office of the Privacy Commissioner, "OPC sources of federal government and employee information," October 24, 2019. Accessed 20 August 2021. https://www.priv.gc.ca/en/about-the-opc/opc-access-to-information-and-privacy/infosource/.

[58] CBSA, "Information about Programs and Information Holdings," October 2, 2019. Accessed 28 September 2021. https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html.

[59] The full text of the notice was: "This area is under video surveillance. Recordings may be used and shared in accordance with applicable federal legislation. For more information on the CBA's use of these recordings, please ask to speak with a supervisor or visit www.cbsa-asfc.gc.ca." CBSA, "Faces on the Move: Multi-Camera Screening – Privacy Impact Assessment (PIA)," January 14, 2016. Accessed 15 September 2021. https://www.theglobeandmail.com/files/editorial/News/0627-nw-na-facial-recognition/CBSA_FOTM_PIA.pdf, p. 23.

[60] Face4 Systems Inc., "Faces on the Move: Multi-Camera Screening," p. 7.

[61] CBSA, "Privacy Impact Assessment (PIA) Executive Summary: Archived – Faces on the Move: Multi-camera screening,"

[62] The final report on FOTM notes: "The privacy and security protocols for surveillance cameras are well established for notification, viewing, use, storage and deletion. *The addition of machine aided identification may require an extension to the current protocols.*" (emphasis added) [NSIRA_202002_072, p. 2.]

[63] PIKs also involve the use of biometrics, and are discussed in paragraphs 125-137 of this report.

indicated plans to revive FOTM.[64] The technology for FOTM was removed from the airport at the end of the pilot.[65]

45. The CBSA relied on its powers of examination under sections 15-18 of *IRPA* to authorize the FOTM project, explaining that "[t]hese sections require all persons seeking entry to Canada to submit to an examination of their persons and documents" and "allow for the presentation of photographic evidence of an applicant's identity."[66] Indeed, section 15(3) of *IRPA* authorizes "an officer [to] … examine any person carried by [a means of transportation bringing persons to Canada]," and to examine "any record or document respecting that person."[67] Section 16 of *IRPA* further specifies that "[a] person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must *produce* [at this examination] a visa and all relevant evidence and documents that the officer reasonably requires."[68] In the case of a foreign national, this evidence includes "photographic and fingerprint evidence."[69] The CBSA did not request legal assessment from the Department of Justice (DOJ) as to whether these authorities would support the FOTM pilot program.[70]

46. The CBSA's reliance on these general powers of examination to conduct facial recognition on travelers as they make their way to the point of processing is of concern to NSIRA. The legislative authorities relied on by the CBSA presume an overt interaction between the traveler and CBSA officials, and the knowing presentation by travelers of their individual documents, fingerprints and photographs during their examination. NSIRA is not satisfied that sections 15-18 of the *IRPA* provide clear authority for the collection of travellers' facial biometrics, particularly prior to – and away from – the point of formal examination. NSIRA is of the opinion that further legal advice would be required in order to ensure that the use of facial recognition in Canadian airports (or elsewhere at the border) is well-founded in the CBSA's legislative authorities.

47. Moreover, with respect to the pilot's compliance with section 8 of the *Charter*, the CBSA explained that a legal opinion from the Department of Justice (DOJ) was not required because "no information [was] being collected above and beyond the CBSA's current use of CCTV

---

[64] CBSA written response to NSIRA, 4 February 2021, "Annex 6 – Innovation Projects & VRP," p. 3.

[65] CBSA written response to NSIRA, 1 October 2021.

[66] CBSA written response to NSIRA, 4 February 2021, "Annex 6 – Innovation Projects & VRP," p. 3.

[67] *IRPA,* s. 15(3); see also general obligation to present one-self for examination at s. 18(1).

[68] *IRPA,* s. 16(1).

[69] *IRPA*, s. 16(2)(b).

[70] CBSA written response to NSIRA, 4 February 2021, "Annex 6 – Innovation Projects & VRP," p. 3.

technology."[71] The pilot used "the existing surveillance infrastructure" and "did not introduce any additional (audio or video) at ports of entry."[72] As such, the CBSA was of the opinion that FOTM did not engage privacy or other concerns that would necessitate legal consultation.[73]

48. As described in paragraph 39, however, project documents indicate that new cameras *were* installed for the demonstration period. Moreover, these arguments under-value the effects of facial recognition technology on individuals' privacy. The important fact is not the installation or absence of new cameras, but rather their ability to conduct facial recognition. This new aspect of what is being collected arguably changes the subject-matter of the search. As the OPC has recommended, PIAs (and, in NSIRA's view, assessments of lawful authority) should be renewed when new technologies are used, in order to ensure that the subject-matter of the search – and its privacy implications – are well-understood.[74] Notices should also be updated to ensure that the use of facial recognition is clearly made known to the public, unless operational imperatives justify a lower degree of transparency.

49. The deployment of such technology, whether on a short-term or long-term basis, must be carefully studied and be fully supported by legal authority and a sound policy framework. The FOTM demonstrated genuine benefits for the execution of the CBSA's duties at the border, specifically the identification of individuals of concern. Individuals previously deported for inadmissibility are known to attempt re-entry into Canada under assumed or false identities. The 47 "real hits" during the six-month demonstration window of FOTM attest to this fact. As noted in other contexts, of course, national security is one among many interests supported through better identity management. Further, findings of inadmissibility on security grounds (s. 34 of the *IRPA*) constitute a comparatively small portion of overall inadmissibility decisions.[75] At the same time, rare events can have extreme consequences. National security cases are, by their nature, infrequent but serious.

---

[71] CBSA written response to NSIRA, 4 February 2021, "Annex 6 – Innovation Projects & VRP," p. 3.

[72] CBSA written response to NSIRA, 4 February 2021, "Annex 6 – Innovation Projects & VRP," p. 3.

[73] CBSA written response to NSIRA, 4 February 2021, "Annex 6 – Innovation Projects & VRP," p. 3.

[74] See paragraphs 36-38 of Office of the Privacy Commissioner, "Police Use of Facial Recognition Technology in Canada and the way forward," June 10, 2021. Accessed 13 September 2021. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

[75] For example, s. 34 allegations made up 2.74% (11 of 402) of inadmissibility hearings before the Immigration Review Board (IRB) between January-March 2021. For 2020, the number was 4.26% (44 of 1,034). See Immigration and Refugee Board of Canada, "Admissibility Hearings Finalized by Type of Allegation," August 30, 2021. Accessed 15 September 2021. https://irb.gc.ca/en/statistics/hearings/Pages/AdmHAlle.aspx

FASTER-PrivBio Project (2015-2017)

50. FASTER-PrivBio was a 'proof of concept' project that developed a prototype mobile application that facilitated the application and approval of electronic travel authorizations (eTAs).[76] It was led by IRCC in conjunction with CBSA and other partners (including the University of Ottawa and Ryerson University). The application captured a digital photograph (selfie), extracted the digital photograph contained in the ePassport chip, compared the two using facial recognition (one-to-one comparison), and validated the authenticity of the travel document. Upon successful enrolment, the application would then create a 'client token' facilitating movement through the travel continuum for low-risk travellers.[77] The project incorporated a 'Privacy-by-Design' framework, with a specific emphasis on addressing the privacy concerns raised by the use of biometrics.[78]

51. Two basic security benefits were envisioned: first, the facilitation of low-risk travellers would allow resources and attention to be applied elsewhere, including toward higher-risk travellers in manual processing. Second, the application would automatically check enrolled travellers against CBSA, IRCC and other applicable (e.g. International Criminal Police Organization [INTERPOL]) biographic watchlists, thereby identifying individuals of concern.[79] This latter function, however, would largely replicate existing screening in the eTA process.

---

[76] An eTA is an entry requirement for visa-exempt foreign nationals travelling to Canada by air. Visitors apply online prior to arrival in Canada by providing certain biographical information and answering several screening questions. Once approved, the eTA is linked to the travellers passport.

[77] Alex Stoianov, "Technical Report 4: FasterPriv Bio: The Policy Analysis," Ryerson University, February 2017, p. 26. [NSIRA_202002_082, p. 26.] The closeout report for the project noted that the "mobile App should…provide more convenience for…travellers" allowing them to "pass through the border more quickly, efficiently, and conveniently." Defence Research and Development Canada (DRDC), "FASTER-PrivBio Project Summary Report," October 2018. Accessed 20 August 2021. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc331/p808727_A1b.pdf, p. 9.

[78] "Technical Report 3: FasterPriv Bio: The Privacy Analysis: A Case Study in Privacy by Design," Ryerson University, March 2017. [NSIRA_202002_080.] The key privacy feature was the 'decentralization' of biometric storage. Rather than collecting and storing the facial image in a centralized database, the image was retained by the user and verified when necessary using an anonymized template. Decentralized biometric storage is generally considered preferable from a privacy perspective, because it lowers the risk from data breaches.

[79] Canadian Security and Safety Program, "CSSP-2015-CP-2114: FasterPriv Bio," N.D., p. 1. [NSIRA_202002_085, p. 1.] The proof-of-concept demonstrated the ability of the mobile application to replicate the screening performed in the standard ETA process, the querying of new, biometric-specific databases was not included or considered in the project. See "Technical Report 3: FasterPriv Bio: The Privacy Analysis,"[NSIRA_202002_080.]

52. The project closed in 2017 having successfully demonstrated its intended deliverables.[80] Its key takeaways included the viability of mobile (smartphone-based) biometric credentials (including adequate data security protections, according to project participants), compatibility with ePassports and related IRCC systems and infrastructure, and the robust identity verifications possible through such a system.[81] The next phase of the project was to work toward live implementation, set to occur under the "Chain-of-Trust" (CoT) initiative. CoT development continues at present and is covered in Section 6, paragraphs 151-155, below.

Biometrics Expansion Project (2015-2020)

53. Initiated in 2015, the Biometrics Expansion Project (BEP), as its name suggests, marked another significant increase in the collection of biometrics in the immigration stream. Building on the TRBP, the BEP expanded the collection of biometrics to all persons (unless exempted) making a claim, application or request under the IRPA.[82] The BEP incorporated the IIS initiative and extended automated immigration information sharing, including through biometric querying, to other international partners in the Migration 5 (M5) group, which comprises the immigration agencies of the United States, Australia, New Zealand, and the United Kingdom.[83] The BEP also broadened the capacity for fingerprint verification at Canadian ports of entry (POE) through the introduction of automated Systematic Fingerprint Verification (SFV) at eight international

---

[80] DRDC, "FASTER-PrivBio Project Summary Report," p. 9.

[81] DRDC, "FASTER-PrivBio Project Summary Report," p. 9.

[82] For the full list of visa-exempt countries, see Schedule 1.1 of the IRPR, available at: https://laws-lois.justice.gc.ca/PDF/SOR-2002-227.pdf Accessed 17 August 2021. See also Government of Canada, "Entry Requirements by country/territory," November 29, 2019. Accessed 17 August 2021. https://www.canada.ca/en/immigration-refugees-citizenship/services/visit-canada/entry-requirements-country.html#visaExempt.

[83] The Migration 5 (M5) group has evolved from a consultative forum to an action-oriented body focused on collaboration on joint initiatives and information exchange to achieve improvements in security, service, and savings. The M5 is supported by a permanent secretariat which is housed in and fully resourced by New Zealand. Canada is represented in the M5 by both IRCC and CBSA.

airports (see paragraph 73) and the addition of discretionary fingerprint verification at secondary inspection at an additional 11 airports and 40 land POE.[85]

54. The BEP closed in 2020 and the biometric activities it established were transferred to steady-state operations. As such, the activities described here are addressed in Section 5, paragraphs 63-94, below.

Assessing Biometrics Past

55. This section surveyed the development of biometric activities in the border continuum over the past several decades, highlighting key moments, programs, and pilots along the way. Taken collectively, several themes emerge.

56. First, the GoC's collection and use of biometrics has steadily expanded. In the immigration context, for example, what began with deportees and asylum claimants in 1993 culminated in 2018 with all persons (unless exempted[86]) making a claim, application or request under *IRPA*.

57. Second, the commitments and priorities established in the wake of the 9/11 attacks spurred the adoption of biometrics in the early part of the millennium, setting the foundation for the basic architecture of biometric activities in the border continuum today. In this context, the rationale for biometric adoption was national security. Identifying individuals meant possibly identifying terrorists.

58. Third, identifying individuals is also (and increasingly) about broader identity management. For CBSA and IRCC, biometrics contribute to overall organizational goals, not just national security objectives. As the immediacy of 9/11 receded, broader identity management became a relatively larger part of the rationale for collecting and using biometrics. This shift reflected a more balanced logic for biometric adoption, embracing their overall utility rather than emphasizing the smaller – though important – national security subset.

59. Fourth, as biometric activities have expanded, so too has the overlap and/or shared responsibility between organizations in their design and implementation: between government

[85] IRCC, "Biometrics Expansion Project: Project Close Out Report," July 16 2020, p. 1. [NSIRA_202002_027, p. 1.]

[86] For a list of exemptions see footnote 91.

departments/agencies (e.g. IRCC and CBSA); between jurisdictions (e.g. Canada and the US, and Canada and other international partners); and between the public and private sector (as the GoC engages industry partners). Such closer cooperation may have implications for individuals' privacy rights, for possible future uses of biometrics, and also underscores the importance of sound data security across these various institutions.

60. Fifth, traveller facilitation has emerged as another force behind biometric adoption, to improve efficiency at the border and to reflect evolving societal norms about the use of technology. As the FASTER-PrivBIO project suggests, the development of new biometric activities takes for granted traveller familiarity with digital devices. At the same time, individuals are likely to be more comfortable adopting relatively intrusive technologies when they do so voluntarily and consensually.[87] This tension – between expectations of convenience and expectations of privacy – is likely to shape public dialogue over biometrics moving forward.

61. Sixth, and related to the above, the expansion of biometrics has coincided with a growing emphasis on privacy and privacy protections. Many of the pilots and projects described in this section explicitly addressed such concerns, including by adopting so-called "Privacy-by-Design" principles, which are intended to proactively protect personal information.[88] This dynamic reflects the development, over time, of the wider understanding (whether on the part of government, industry, the legal community, or academia) as to the particular risks associated with the collection and use of biometrics. Some applications of biometric analysis – for example the facial recognition used in the FOTM project – carry more risks than others, and ought to be scrutinized accordingly.

5. BIOMETRICS *PRESENT*

62. This section focuses on the GoC's steady-state biometric activities in the border continuum. The balance of the section examines the role of biometrics in the Immigration and Passport programs, respectively. For each, we examine how biometrics serve program objectives (noting, as relevant, their collection, use, retention, and disclosure) and consider the criteria outlined in Section 3. The end of the section examines the process of "arriving into Canada", which includes the analysis of

[87] For example, a survey by the International Air Transport Association (IATA) in 2019 "found that 70% of passengers are willing to share additional personal information including their biometric identifiers to speed up processes at the airport." IATA, "Global Passenger Survey (2019)", Accessed 3 October 2021. https://www.iata.org/en/pressroom/pr/2019-10-16-01/.

[88] See for example the principles outlined in Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," January 2011. Accessed 20 August 2021. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

traveller and NEXUS member biometrics by automated kiosks at Canadian airports. Throughout, we highlight the relevant national security considerations.

Immigration Program

63. IRCC is responsible for screening the admissibility of potential permanent and temporary residents coming to Canada.[89] As part of this process (hereafter the "Immigration Program"), IRCC employs biometrics, in cooperation with CBSA and the RCMP. As IRCC characterized it to NSIRA, for biometrics in the Immigration Program: "IRCC collects, the RCMP stores, and the CBSA verifies."[90]

64. IRCC collects (all ten) fingerprints and a digital photograph in support of applications for temporary resident visas or status, work permits, study permits, temporary resident permits, and permanent residency, and in support of refugee and asylum claims.[91] The collected biometrics are stored in two databases: photographs are stored in the IRCC's Global Case Management System (GCMS) and fingerprints are stored in the RCMP's Automated Fingerprint Identification System (AFIS).[92] The digital photograph, while ICAO compliant, is not used for facial recognition

---

[89] Government of Canada, "IRCC: Mandate and Role," March 10, 2020. Accessed 17 August 2021. https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/departmental-plan-2020-2021/mandate-role.html.

[90] IRCC written response to NSIRA, 20 November 2020, p. 5.

[91] There are some exemptions to the requirement to provide biometrics. Exemptions include applications from: Canadian citizens, registered Indians and persons who already have permanent resident status in Canada; Visa-exempt visitors making an application for an electronic travel authorization (eTA); Foreign nationals under the age of 14 or over the age of 79 (there is no upper age limit for in-Canada asylum claimants); US nationals making an application for a work, study or temporary resident permit; Her Majesty the Queen in right of Canada and any member of the Royal Family making an application for a work, study or temporary resident permit; Foreign nationals that hold a valid US entry visa and are transiting through Canada for less than 48 hours directly to or from the US; Cabinet ministers and accredited diplomats and officials of foreign countries (and their family members) coming to Canada in the course of official duties; and heads of state and heads of government coming to Canada for a temporary purpose on official or non-official business. IRCC written response to NSIRA, 20 November 2020, p. 2. The COVID-19 pandemic has affected biometrics collection, including suspensions of the need to provide biometrics in certain contexts, though all such changes are to be temporary. For example, in-Canada TR applicants are temporarily exempt from providing biometrics and permanent residency applications may use biometrics previously collected (if collection occurred in the past 10 years). See Government of Canada, "Coronavirus disease (COVID-19): Biometrics," June 1, 2021. Accessed 28 July 2021. https://www.canada.ca/en/immigration-refugees-citizenship/services/coronavirus-covid19/biometrics.html.

[92] AFIS is a subsystem of the RCMP's Real Time Identification System (RTIDS), which facilitates the electronic storage and processing of criminal, refugee, immigration, and civil/employee fingerprints. RCMP written response to NSIRA, 31 May 2021, pp. 11.

and may not be of sufficient quality for that type of analysis. As such, we focus primarily on fingerprints in our description and analysis of activities.

65. Biometrics are collected and enrolled at multiple service points, both in Canada and abroad, with the vast majority (approximately 90%) occurring at Visa Application Centres (VACs). VACs are commercial service suppliers, managed by private companies, contracted by IRCC to deliver biometric enrolment overseas.

66. The collection phase is a sensitive juncture given the personal nature of biometric information. The primary concerns here relate to privacy and the security of biometric data. Media reports have highlighted concerns about VACs, questioning whether adequate privacy protection can be maintained given the central role of private contractors based outside of Canada.[93] Possible links between the subcontractor administering Canada's VAC in Beijing and Chinese security forces have also been scrutinized.[94] Foreign governments have an interest in knowing who is applying to come to Canada - the information can be leveraged to monitor, suppress, harass, coerce, threaten or otherwise harm an individual. The possible interception or theft of biometric data is especially concerning, given its possible use in monitoring, surveillance, and identification.

67. IRCC has taken steps to ensure the flow of biometric information (including collection and transmission) at VACs is controlled. Contracts with VAC providers stipulate that they must abide by Canadian privacy laws.[95] IRCC further states that oversight of VAC contractors occurs through audits and site reviews, conducted by Canadian officials, at VAC locations.[96] All biometric information collected outside of Canada is said to be encrypted before being transmitted back to IRCC servers located in Canada (photographs in GCMS) and to the RCMP (fingerprints in the AFIS). Once successfully transmitted, IRCC states that the information is deleted from the point of collection.[97]

68. Given the nature of operating in certain foreign jurisdictions, however, there remain challenges to securing the information provided by applicants at VACs. Some VACs are located in countries with

---

[93] See Andrew Russell and Max Hartshorn, "Canada paid nearly $200M to visa company previously based in a tax haven and linked to China," *Global News,* February 3, 2021. Accessed 14 August 2021. https://globalnews.ca/news/7563381/canada-visa-application-firm-tax-haven-ties-china/

[94] See Nathan Vanderklippe and Steven Chase, "Canada's visa application centre in Beijing run by Chinese police," *Globe and Mail,* February 8, 2021. Accessed 13 August 2021. https://www.theglobeandmail.com/world/article-canadas-visa-application-centre-in-beijing-run-by-chinese-police/

[95] Public Works and Government Services Canada, "RFP - Visa Application Centre Global Contract Renewal - Immigration Biometrics," p. 23 [IRCC RFI #2 Documents].

[96] IRCC written response to NSIRA, 1 October 2021.

[97] IRCC written response to NSIRA, 20 November 2020, p. 8.

national interests inimical to those of Canada – the national security consequences of security breaches at these VACs may therefore be particularly acute. While the scope of the present study precluded in-depth examination of the security arrangements at VACs, NSIRA may wish to revisit the issue at a later date.

69. In the border continuum, Canada leverages (or uses) the collected biometrics in three ways: for screening at enrolment (with any returned information informing decisions about an application), for verification upon arrival at a Canadian POE, and for ongoing assessment of admissibility (or immigration status) once an individual is present in Canada.

70. Screening at enrolment is automatic, and includes both domestic (Canadian) and foreign databases. For enrolment, IRCC or CBSA[98] submits the collected fingerprints to the RCMP. Fingerprints and biographic information are then compared against the RCMP's criminal and immigration fingerprint repositories (the latter includes fingerprints collected as part of previous applications). Fingerprints are also queried against the immigration databases of Canada's M5 partners.[99]

71. Information returned from domestic and foreign screening informs decisions on admissibility – including possible inadmissibility on *IRPA* s. 34 security grounds.[100] Biometric immigration information sharing with the M5 partners includes sharing of derogatory alert codes. Information that indicates a potential national security concern may be referred to the Public Safety portfolio (including CSIS and CBSA) for additional security screening. While foreign screening also occurs using biographical information[101], biometrics confer the additional advantage of identifying

---

[98] Visa-exempt individuals may apply for study and work permits upon arrival at a POE in which case CBSA is responsible for the collection and enrolment of biometrics.

[99] IRCC, "PIA - Migration Five Information Sharing Regulations," N.D. [IRCC RFI #2 Documents].

[100] Section 34 reads: "A permanent resident or a foreign national is inadmissible on security grounds for: (a) engaging in an act of espionage that is against Canada or that is contrary to Canada's interests; (b) engaging in or instigating the subversion by force of any government; (b.1) engaging in an act of subversion against a democratic government, institution or process as they are understood in Canada; (c) engaging in terrorism; (d) being a danger to the security of Canada; (e) engaging in acts of violence that would or might endanger the lives or safety of persons in Canada; or (f) being a member of an organization that there are reasonable grounds to believe engages, has engaged or will engage in acts referred to in paragraph (a), (b), (b.1) or (c). Available at: https://laws-lois.justice.gc.ca/eng/acts/i-2.5/section-34.html. Accessed 17 August 2021.

[101] Biographical screening against foreign databases occurs outside of, and in addition to, the fingerprint screening process. The RCMP's involvement in this context is limited to the anonymous querying of fingerprints with M5 partners.

matches to previous applications associated with different names and/or with discrepant biographical information.

72. Following the screening process, biometrics are used by the CBSA to verify the identity of enrolled foreign nationals arriving at a Canadian POE. This ensures – to a level of confidence beyond what is generally possible absent the use of biometric information – that the individual granted a visa or permit is the same individual entering Canada.

73. The mode of verification varies between POE. At eight international airports, Systematic Fingerprint Verification (SFV) occurs through Primary Inspection Kiosks (PIKs). PIKs are automated kiosks used to process travellers through customs and immigration at major Canadian airports (for more on the PIK see paragraphs 125-137, below). The PIK captures fingerprints and transmits biometrics to the RCMP for one-to-one matching against the traveller's reference fingerprint in the RCMP database.[103] Where SFV is not available, Border Services Officers (BSOs) verify identity by comparing the traveller's enrolled photograph with the individual presenting in front of them, while fingerprint verification occurs on a discretionary basis at secondary inspection using CBSA's LiveScan device.[104]

74. Biometrics are also used to assess ongoing admissibility. That is, they serve as a means to connect individuals to information that could affect their immigration status and/or future immigration applications (for example interaction with law enforcement that might indicate inadmissibility).

75. The retention period for biometrics collected is partially contingent on the application's outcome. For both temporary resident[105] and permanent resident applications refused on the grounds of

[103] In addition to the captured fingerprints, the PIK sends a unique reference number created at enrollment so that the correct fingerprint record can be extracted for matching purposes. The results of the one-to-one matching are typically returned within five seconds.

[104] LiveScan is a device used to electronically capture and transmit fingerprints. The system includes both hardware and a software interface that allows for the transmission of information.

[105] These include temporary resident visas, study permits, work permits, and temporary resident permits.

what the IRCC considers "serious inadmissibility" (sections 34-37 of the *IRPA*), biometrics are retained until the individual's 100th birthday.

76. This extended retention period provides security benefits as biometrics can help identify an individual should they submit a subsequent application at any (realistic) point in the future, even if submitted under a different name. Extended retention also makes such identification possible for domestic and/or foreign partners with querying access to the immigration database. Should the individual receive a record suspension, criminal rehabilitation, or ministerial relief, the retention period reverts to the typical 15 years from the date of biometric enrolment. This caveat is important, as it realigns the retention of an individual's biometrics beyond the resolution of the underlying circumstances which warranted the extended retention.

77. At the end of the retention period, biometric information is disposed of by IRCC according to disposition authorizations issued by Library and Archives Canada. With respect to fingerprints held by the RCMP, an automated electronic purge transaction request is transmitted by IRCC and a confirmation of the purge returned.[106]

78. In 2021, IRCC discovered a privacy breach related to the retention of immigration fingerprints and photographs beyond their prescribed retention period. The information belonged to individuals who attained Canadian citizenship meaning that, according to IRCC biometric retention policy, fingerprints and photographs associated with their immigration file should have been deleted. IRCC notified the OPC in February 2021 about the issue, and notified affected clients, by email, in March 2021.[107] A public notification was placed on the IRCC website.[108]

79. The disclosure of biometric information raises privacy considerations and calls for attentive consideration of their subsequent use. Given that biometrics are personal information, the current legal framework requires that the GoC only use them for the purposes for which they were obtained (namely, determining an individual's admissibility to enter, or remain in, Canada); for a use consistent with that purpose; or as otherwise authorized by law.

80. The automated querying that occurs between Canada and its M5 partners involves an anonymous biometric (fingerprint) search, with no identifying biographic information included; if a match is detected, relevant immigration information is returned; if there is no match, the

---

[106] IRCC written response to NSIRA, 20 November 2020, p. 10.

[107] Of note, the retention of some clients' information led to that information being disclosed to law enforcement agencies. "Bio Purge Privacy Breach information provided to CIMM June 2 2021," p. 3 [IRCC RFI #2 Documents]

[108] IRCC, "Bio Purge Privacy Breach information provided to CIMM June 2 2021," [IRCC RFI #2 Documents]. For the public notification see Government of Canada, "Email/letter sent to clients to inform of retention of biometric information," March 19, 2021. Accessed 5 August 2021. https://www.canada.ca/en/immigration-refugees-citizenship/news/notices/email-letter-sent-retention-biometrics-information.html

receiving country sends a nil result. In either case, the receiving country is required to purge and not retain the fingerprint.[109] The system is designed, ultimately, with the intention that no biographic and/or immigration information is exchanged unless both parties already possess the biometric in their databases – an important privacy protection measure. Further, the automated agreements specify that any information exchanged will pertain to third-party nationals only; that is, Canada will not send or receive information on Canadian citizens or, with the exception of asylum claims, permanent residents.

81. Less frequent case-by-case (or *ad hoc*) exchanges may result in the actual exchange of underlying biometric information (whether photographs or fingerprints) if the information is deemed, by the requesting party, relevant to enforcing that party's immigration and citizenship laws.[110] Such exchanges are subject to caveats regarding use, onward disclosure, and retention, which apply to any information disclosed (not just biometrics), but which are not legally binding on the participants.[111] IRCC further indicated that *ad hoc* exchanges of biometric information may also occur with international partners beyond the M5, "with either the consent of the individual to whom the information pertains, or pursuant to section 8(2)(a) [i.e. the consistent use provision] of the *Privacy Act.*"[112]

82. The primary sources of authority for the collection, use, and disclosure of biometric information in the Immigration Program are the *IRPA* and the *Immigration and Refugee Protection Regulations (IRPR)*. Specifically, s. 10.01 of the *IRPA* authorizes the collection of biometrics for the purposes of enrollment and verification pursuant to an application under the Act. Under s. 10.02 of *IRPA,* the Minister may issue regulations respecting the implementation of these processes, through the *IRPR*. The *Regulations* specify to whom the biometrics requirements apply, the type of biometrics at issue, and guide their collection, processing and verification.[113] Section 16(1) of the *IRPA* requires that individuals making an application under the Act submit truthfully to examination and produce "relevant evidence and documents" while 16(2), which applies only to foreign nationals, specifies that such evidence includes "photographic and fingerprint evidence".

---

[109] Each bilateral agreement specifies that retention of this kind is improper, with "Quality Assurance" activities intended to monitor and ensure that it does not occur. IRCC written response to NSIRA, 3 August 2021, p. 3.

[110] The agreements are available at: Government of Canada, "IRCC: Agreements with other departments and governments," March 27, 2018. Accessed 17 August 2021. https://www.canada.ca/en/immigration-refugees-citizenship/corporate/mandate/policies-operational-instructions-agreements/agreements.html.

[111] In this context, then, fingerprints and facial photographs are grouped with other personal information (e.g. name, date of birth, address, medical information, travel history etc.) and not, as in the automated exchanges, leveraged for identification purposes (connecting information across databases).

[112] IRCC written response to NSIRA, 20 November 2020, p. 13.

[113] See esp. Part 2, Division 2.1.

IRCC also cites s. 4 of the *Privacy Act* as authorizing their collection of biometrics, given that the information relates "directly to the administration of [IRCC's] immigration programs." They note further that, consistent with s. 7 of the *Privacy Act,* biometrics "will only be used for the purposes for which it was collected, or for a use consistent with that purpose."[114]

83. In terms of the IRCC's disclosure of biometrics to international allies, s. 7 of the *IRPA* authorizes the Minister, with the approval of the Governor in Council, to enter into an agreement(s) with the government of a foreign state(s), for the purposes of the *IRPA*. Multiple such agreements are part of the *IRPR*, which cover Canada's information sharing activities with each M5 partner including:[115] the 'Agreement between the Government of Canada and the Government of the United States of America for the Sharing of Visa and Immigration Information';[116] the 'Annex Regarding the Sharing of Information on Asylum and Refugee Status Claims to the Statement of Mutual Understanding'; and the bilateral automated exchange arrangements with the Governments of Australia, New Zealand and the United Kingdom.[117] These agreements provide for the disclosure of biographic and biometric data between the parties to the extent "necessary, relevant and proportionate to achieve [the administration and enforcement of the parties' citizenship and immigration laws]."[118] Provisions in each agreement also govern the destruction of the information, the correction of previously disclosed information, and grant the Minister a discretion to refuse to disclose information detrimental to Canada's national interests.[119]

84. Such disclosures would also be consistent with s. 8(2)(f) of the *Privacy Act,* which allows for the disclosure of personal information under an agreement or arrangement between the Government of Canada and a foreign state, for the purpose of administering or enforcing its laws.[120] *Ad hoc* exchanges with partners beyond the M5 are conducted pursuant to the consistent use provisions of s. 8(2)(a) of the *Privacy Act.*

85. Canadian law enforcement may also access fingerprints collected by IRCC during the immigration application process for law enforcement purposes. Section 13.11 of the *IRPR* allows the RCMP to use – or disclose to other law enforcement agencies in Canada – any biometric information and specified, related personal information for the purpose of establishing or verifying a person's

---

[114] IRCC written response to NSIRA, 20 November 2020, p. 12.

[115] Section 150.1(1)(b) of the *IRPA* authorizes the Minister to enact regulations concerning the disclosure of information for the purposes of national security, the defence of Canada or the conduct of international affairs.

[116] *IRPR,* Part 19.1, Division 1.

[117] *IPRR*, Part 19.1, Division 3.

[118] See esp. Division 1, ss 315.22 – 315.25; Division 3, ss. 315.37-315.39.

[119] Division 1, s. 315.25(4), 315.26, 315.27; Division 3, s. 315.41(3), 315.42, 315.43.

[120] IRCC written response to NSIRA, 20 November 2020, p. 13.

identity in order to prevent, investigate or prosecute an offence.[121] This information may also be used to establish or verify the identity of a person whose identity cannot reasonably be otherwise established or verified because of a physical or mental condition or because of their death.[122] In other words, when law enforcement agencies submit fingerprints collected in the course of its duties to the RCMP -- or the RCMP itself verifies a fingerprint -- both criminal *and* immigration repositories, containing the fingerprints of foreign nationals and permanent residents, are included in the search.[123] Section 13.11(2) of the *IRPR* allows the following personal information to be used or disclosed: the individual's fingerprints and the date on which they were taken; their surname and first name; their other names and aliases, if any, their date of birth, their gender, and any file number associated with the biometric information or related personal information.

Assessing the Immigration Program

86. Biometrics facilitate identity management in the Immigration Program. First, the enrolment of biometrics ties an application to an individual. Second, biometric querying screens applicants against domestic and foreign databases, with the information returned as part of these queries informing decision-making regarding their admissibility into Canada. Third, biometrics are verified upon arrival at a Canadian POE to ensure that the individual presenting is the one to whom a visa or permit has been granted. Finally, biometrics are retained for a specified period (varying between application streams) so as to both assess continuing admissibility (status) under the *IRPA* and allow foreign nationals to submit subsequent applications without having to re-enrol their biometrics.[124]

87. National security benefits are a consequence of robust identity management. National security is a component of, rather than the sole impetus behind, the use of biometrics. Enrolling biometrics at the application stage serves as a potential deterrent to individuals who might otherwise apply

---

[121] *IRPR,* s. 13.11(1)(a); RCMP written response to NSIRA, 31 May 2021, pp. 5. See also section 150.1(1)(d) of the *IRPA* which authorizes the Minister to enact regulations concerning "the retention, use, disclosure and disposal by the RCMP of biometric information and any related personal information that is collected under [IRPA] and provided to it for the enforcement of any law of Canada or of a province." The *IRPR* does not currently regulate the retention and disposal of fingerprints collected by the IRCC in the course of its duties; see instead the discussion of retention policies and the requirements of the *Library & Archives Act* at paragraph 78.

[122] *IRPR,* 13.11(1)(b).

[123] This includes latent fingerprints collected in the course of criminal investigations. RCMP written response to NSIRA, 22 June 2021, p. 9. RCMP written response to NSIRA, 1 October 2021,

[124] Temporary resident applications operate under the "1-in-10 policy", meaning that biometrics are valid for a period of ten years and can be re-used (including for screening and verification purposes) for new or subsequent applications within that time frame. Permanent residency applications, by contrast, require biometric collection and enrolment for each new application.

for *mala fide* purposes. Biometric screening of domestic and foreign databases helps identify individuals who are inadmissible (including, potentially, for reasons of national security). Verifying biometrics upon arrival ensures that the individual authorized to enter and not an individual posing as that person is the individual who does enter. The retention of biometrics which includes the retention of biometrics tied to applications denied for reasons of national security allows for the ongoing assessment of admissibility under the *IRPA* (including s. 34) and facilitatesthe reciprocal querying of foreign databases. Without biometrics, such exchanges would rely on biographical information, which is more susceptible to fraud and/or error.[125]

88. Unique to each individual and easily captured by digital technology, fingerprints are generally regarded as accurate and reliable means of identification.[126] However, both CBSA and IRCC noted potential concerns in relation to Gender Based Analysis Plus (GBA+), which is an analytical process designed to assess how diverse groups of people may experience policies, programs and initiatives.[127] Specifically, some groups have more difficulty than others having their fingerprints captured, including individuals working in certain trades (which may indicate lower socio-economic status) and women (due to a biological difference in finger ridges).[128] Mitigation strategies at the collection stage included training for operators, and operational guidelines as well as a regulatory provision (R12.8 of the *IRPR*) that allow the application process to continue if fingerprint capture is not possible.[129]

89. Similarly, research has shown that fingerprint-matching algorithms – such as those used during SFV – may be less accurate for certain ethnic, gender, age, and socio-economic groups.[130]

---

[125] CIC and CBSA, "PIA - Canada-U.S. Systematic Biometric Information Sharing," p. 11. [IRCC RFI#2 Documents].

[126] Fingerprints have been used by law enforcement since the 19th century. They are not, however, infallible; see for example Jennifer Mnookin, et al. "Error rates for latent fingerprinting as a function of visual complexity and cognitive difficulty," May 2016. Accessed 1 August 2021. https://www.ojp.gov/pdffiles1/nij/grants/249890.pdf.

[127] For further detail on GBA+ see Government of Canada, "What is Gender-based Analysis Plus," April 14, 2021. Accessed 30 August 2021. https://women-gender-equality.canada.ca/en/gender-based-analysis-plus/what-gender-based-analysis-plus.html.

[128] IRCC, "Triage – Biometrics Expansion – March 2017," p. 3. [IRCC RFI #2 Documents]

[129] If the conditions preventing the collection of biometrics are temporary, applicants may be required to provide biometrics at a later date. If the conditions are permanent, the biometric requirement may be waived. For examples of permanent injuries and conditions that interfere with biometric collection, and for general guidelines on dealing with such conditions in the context of immigration applications, see Government of Canada, "Conditions that interfere with biometrics collection," July 30, 2018. Accessed 2 August 2021. https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/identity-management/biometrics/conditions.html.

[130] P. Drozdowski et al., "Demographic Bias in Biometrics: A Survey on an Emerging Challenge," April 14, 2020. Accessed 1 August 2021. https://arxiv.org/pdf/2003.02488. See also R. Austin Hicklin and Christopher L. Reedy, "Implications of the

Examples include individuals of East Asian origin, women, those working in certain trades, and older individuals. These groups may be subject to higher error rates when their fingerprints are verified (e.g. compared to an existing fingerprint holding).[131] Mitigation strategies identified by CBSA included hardware and software adjustments that would improve the ability of PIKs (the kiosks used for SFV) to capture and analyze fingerprints.[132]

90. In terms of transparency, there is significant material available to the public regarding biometrics and the immigration application process. Much of this content is practical in nature, intended to guide prospective applicants in the provision of their biometric information.[133] IRCC also explains the program benefits of using biometrics, including that they help facilitate entry into Canada, ensure that the person seeking entry is the same as the one who was granted a visa, permit, or permanent residence, and to help prevent the use of stolen, borrowed, or altered visas and/or permits to enter Canada.[134] While national security justifications are provided, the emphasis is on service delivery and the broader imperatives of identity management.

91. Overall, fingerprints appear to be a reasonable, appropriate choice of biometric to use in the immigration system. They can be collected relatively easily, with little intrusion, and while they are reliable identifiers, they offer comparatively little extrinsic evidence about individuals' lifestyles or personal choices. Moreover, they offer a vital inter-operability across domestic immigration and law enforcement systems, as well as with those of nearly all foreign jurisdictions. The privacy costs of relying on biometrics for immigration screening therefore appear to be reasonable and proportionate to the benefits they convey to the state and the integrity of its immigration system.

92. Once collected, the use of biometrics for screening and verification are proportionate to the objective of identity management. From a national security perspective, decisions about admissibility – who may and who may not enter the country – are fundamental. So, too, is the

---

IDENT/IAFIS Image Quality Study for Visa Fingerprint Processing," October 31, 2002. Accessed 1 August 2021. https://www.eumonitor.nl/9353000/1/j4nvgs5kjg27kof_j9vvik7m1c3gyxp/vjf4n9jouqzh/f=/blg266612.pdf.

[131] Hicklin and Reedy, "Implications of the IDENT/IAFIS Image Quality."

[132] CBSA, "Gender-Based Analysis Plus and the Primary Inspection Kiosk: Summary of Key Findings," May 2016, p. 3. [NSIRA_202002_03_012, p. 3.]

[133] This information includes: what biometrics are; what biometric information is collected; whose biometric information is collected (and who is exempt); how biometric collection/verification works; where and how to enroll; how much the process costs (fees); how privacy is protected; and answers to frequently asked questions. See CBSA, "Biometrics screening," August 12, 2020. Accessed 1 August 2021.https://www.cbsa-asfc.gc.ca/security-securite/biometrics-biometrique-eng.html; IRCC, "Biometrics expansion," February 4, 2019. Accessed 1 August 2021. https://www.canada.ca/en/immigration-refugees-citizenship/campaigns/biometrics.html.

[134] IRCC, "Why do I have to give my biometrics (fingerprints and photo) when I apply?" September 29, 2021. Accessed 5 October 2021. https://www.cic.gc.ca/english/helpcentre/answer.asp?qnum=703&top=19

desire to prevent fraudulent entry. At the screening stage, biometrics are particularly helpful in linking information across databases – e.g. in connecting information about an individual held in domestic or foreign repositories. The ability to make such linkages even in the face of multiple names or biographical profiles – perhaps cultivated for *mala fide* purposes – is largely unique to biometrics as a class of information. Likewise, verification – confirming that an individual is who they say they are when presenting at the border – is significantly enhanced through biometric analysis.

93. The activities are not without risks, however. The availability of immigration biometrics to Canadian law enforcement, for example, has the potential to stigmatize the immigrant population by associating them with criminality. In 2015, the European Union's EURODAC (European Asylum Dactyloscopy Database) was heavily criticized by civil rights groups for "criminalizing" asylum seekers by making their fingerprints available to European law enforcement agencies.[135] While held in different repositories, immigration and criminal fingerprints exist within the same RCMP system, and both are searchable by law enforcement, including when attempting to identify latent fingerprints taken from crime scenes.[136]

94. There are benefits to making immigration fingerprints available to law enforcement, most immediately in assisting police with the enforcement of Canadian criminal law and, consequently, in returning information to IRCC and CBSA which may be relevant for enforcing the *IRPA*. At the same time, if the fingerprints of all Canadian citizens were in the possession of the government and searchable by Canadian law enforcement, that too would benefit the enforcement of Canadian law, though few – if any – would consider such an arrangement proportionate or desirable. It is therefore legitimate to question whether the availability of immigration fingerprints – collected in the course of applying to come to Canada – to law enforcement is proportional in all circumstances, or whether it should be limited to certain serious offences.

---

[135] Sergio Carrera et al., "When mobility is not a choice: Problematising asylum seekers' secondary movements and their criminalization in the EU,"*CEPS,* December 2019. Accessed 1 August 2021. https://www.ceps.eu/wp-content/uploads/2019/12/LSE2019-11-RESOMA-Policing-secondary-movements-in-the-EU.pdf. See also Andrea Dernbach (transl. Erika Korner), "Eurodac fingerprint database under fire by human rights activists," *Euractiv,* February 9, 2016. Accessed 1 August 2021. https://www.euractiv.com/section/justice-home-affairs/news/eurodac-fingerprint-database-under-fire-by-human-rights-activists/.

[136] While immigration fingerprints are not searched against latent repositories at enrolment, latent prints collected in the course of criminal investigations may be searched against immigration repositories. RCMP written response to NSIRA, 1 October 2021.

Passport Program

95. The Passport Program, led by IRCC, is responsible for "issuing, refusing to issue, revoking, withholding, cancelling, recovering and providing instructions on the use of Canadian passports and other travel documents."[137] The program's ultimate purpose is to enable the travel of eligible Canadian citizens, permanent residents, and refugees. Preventing individuals who are ineligible or not entitled to a passport from obtaining and travelling under official documents is the obverse of this goal. A subset of applicants will be ineligible for reasons related to national security. Established pursuant to the royal prerogative on passports, the Canadian Passport Order (CPO) constitutes the main legal framework for the issuance of regular and temporary passports by the Passport Program.[138] It provides the authority for IRCC to collect and use personal information, including biometrics, for the processing of applications and determining an individual's entitlement to a passport.[139] IRCC maintains that this collection is consistent with s. 4 of the *Privacy Act*, given that collection relates directly to the administration of a lawfully authorized program.[140]

---

[137] IRCC, "Evaluation of the Passport Program," March 2020. Accessed 18 August 2021. https://www.canada.ca/content/dam/ircc/documents/pdf/english/corporate/reports-statistics/evaluations/e3-2018-evalation-of-passport-program-accessible-english-pdf.pdf, p. 6. Cancellation and revocation are two separate administrative processes intended to respond to different situations. *Revocation* decisions are considered final as of the date the decision is rendered, and follow a detailed investigation, in which the subject is given an opportunity to respond before the decision is made. This includes cases where the Minister of Public Safety and Emergency Preparedness has "reasonable grounds to *believe* the decision is necessary to prevent the commission of a terrorism offence, as defined in section 2 of the Criminal Code," or where there are reasonable grounds to believe the revocation is necessary to protect "the national security of Canada or a foreign country or state" (see CPO s. 10.1). *Cancellation* occurs in circumstances where such communication with the passport holder would not be appropriate, such as where the Minister has reasonable grounds to *suspec*t that the decision is necessary to prevent the commission of a terrorism offence, as defined in section 2 of the Criminal Code, or where confidentiality is necessary to protect "the national security of Canada or a foreign country or state" (see CPO, s. 11.1(2)). A person may apply in writing to have the decision to cancel their passport reconsidered, within 30 days after the day in which they become aware of the cancellation (see CPO, 11.3 and the possibility of reconsideration, at CPO, s. 11.31). In both instances, law enforcement and border control officials are notified of the cancellation or revocation, and the passport is no longer valid for travel. See also IRCC, https://www.canada.ca/en/immigration-refugees-citizenship/services/canadian-passports/security/refusal-revocation.html#s2.

[138] Full text available at: https://laws.justice.gc.ca/eng/regulations/SI-81-86/.

[139] The CPO authorizes these activities with respect to regular (blue) and temporary (white) passports. For other official travel documents – including special (green) and diplomatic (red) passports, as well as Certificates of Identity, Refugee Travel Documents, and Emergency Travel Documents – authority relies on the Minister of Immigration, Refugees, and Citizenship's exercise of the Royal Prerogative. The Royal Prerogative applies to activities not explicitly authorized by statute but historically exercised by the executive.

[140] The CPO similarly provides authority for the Minister of Employment and Social Development (s 12), (through Service Canada) (s12) and the Minister of Foreign Affairs (s13) (through GAC) to collect personal information as part of the applications

96. Specifically with respect to biometrics, s. 8.1(1) of the CPO allows IRCC to convert an applicant's photograph into a digital format and insert it on the electronic chip in the ePassport. Section 8.1(2) facilitates the use of the FRS by authorizing the conversion of the 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."[141] This provision similarly authorizes the use of the System Lookout-Facial Recognition System (SL-FRS) described below.

97. As with the Immigration Program, the full range of benefits associated with biometrics extend beyond national security outcomes. According to IRCC, the "use of biometrics in the Passport Program does not *per se* constitute a security and intelligence activity."[142] Rather, as in the immigration context, biometrics serve identity management, with potential national security benefits downstream of that broader ambit.

98. Two identical, printed facial photographs, meeting certain International Civil Aviation Organization (ICAO) standards, must be submitted as part of applications for all Canadian travel documents.[143] According to IRCC, all application information is transmitted via secure systems, and all facial recognition data traffic is secured through encryption.[144]

99. The collected photograph is used for two purposes. First, it is screened using facial recognition to help establish identity and inform an assessment of the applicant's eligibility and entitlement to Canadian travel document services.[145] Second, it is embedded in the document and used by border officials to validate the identity of the holder when crossing an international border.

100. The applicant's digitized photograph is transferred to the Facial Recognition Solution (FRS) application. The FRS then converts the image into a biometric template using a proprietary algorithm and stores it in an accompanying database. If the application is linked to a previous application, such as renewals or the replacement of lost or stolen passports, one-to-one facial verification is performed against the applicants' previous template(s). For both renewals and new applications, one-to-many facial identification is performed against existing templates (approximately 55 million, from previous applications) in the FRS database from adult (age 16+)

---

process. In addition, the authority for GAC to intake and process Emergency Travel Document applications is provided under the royal prerogative.

[141] CPO, s. 8.1 (2).

[142] IRCC written response to NSIRA, 4 December 2020, p. 1.

[143] These guidelines specify size, position, lighting conditions, background, and facial expression. IRCC written response to NSIRA, 4 December 2020, p.4.

[144] IRCC written response to NSIRA, 4 December 2020, p. 6.

[145] Applicants under the age of 16 do not have their photographs screened using facial recognition, given known challenges with facial matching accuracy for children.

applicants and photographs supplied as part of the Passport System Lookout (SL). The SL-FRS , as it is called, is effectively a watchlist comprised of individuals who are considered high-risk for identity fraud, including those known to have a history of using false identities or multiple aliases, or who have otherwise been identified by security partners – including CSIS and the RCMP – as high-risk for such behaviour. [146] The precise criteria or circumstances for inclusion on the list are not clear, and appear to be highly discretionary.[147] IRCC caveats, however, that "only a small number of IRCC Passport Program officers have the ability to add entries to the list." [148] The list has been in operation since February 2018, and currently includes fewer than 100 individuals.[149]

101. According to IRCC, the use of the FRS protects the integrity of the Canadian passport. IRCC cites 2016 ICAO guidelines on security in the issuance of travel documents noting that the issuance phase – or the "beginning of the chain" – is becoming the primary target for fraud given "the rapid development of new technologies and new security techniques" which make forgery increasingly difficult, including, for example, the security features associated with the ePassport.[150]

102. The authority to refuse passport applications for national security reasons lies with the Minister of Public Safety, as per the CPO.[151] Biometric screening through FRS may inform that decision-making process by detecting identity fraud or flagging individuals from the SL-FRS. No such decisions are automatic; individuals on the SL-FRS may still be entitled to a passport or travel document following review.

103. Preventing fraud (whether through deterrence or detection) in the issuance of official travel documents offers clear national security benefits. The movement of *mala fide* actors across

---

[146] IRCC written response to NSIRA, 3 August 2021, pp. 1, 6.

[147] Hypothetical examples provided to NSIRA during a 14 October 2020 briefing included a security partner – "usually the RCMP" – advising that an individual ineligible for a passport may attempt to apply for one under another name, or that "brokers" were buying IDs in certain communities so as to facilitate the acquisition of travel documents on behalf of ineligible individuals. In a written response to NSIRA on October 1, 2021, IRCC further averred that "The Passport program is currently conducting a review of the System Lookout (SL) which aims to better document the purpose, format and use of the SL, clearly identify stakeholder roles and responsibilities, and review compliance with departmental and relevant legislative/regulatory parameters. Any identified areas for improvement in functionality, efficacy, or operational procedures will be addressed by the responsible stakeholder(s)."

[148] IRCC written response to NSIRA, 3 August 2021, p. 8.

[149] IRCC written response to NSIRA, 3 August 2021, p. 8.

[150] ICAO, "ICAO Guide for Assessing Security of Handling and Issuance of Travel Document," 2016. Accessed 4 August 2021, p. 3. Available at: https://www.icao.int/security/fal/trip/pages/publications.aspx

[151] See CPO, ss. 10.1, 11.1(2) and s. 11.4 (whereby the Minister of Citizenship and Immigration supports the Minister of Public Safety and Emergency Preparedness by giving effect to his decision).

borders threatens both international and Canadian security. While identity fraud is committed for a host of reasons – including criminal, financial, or personal – the possibility that terrorism, espionage, or other national-security threats may involve the misuse of passports is well documented.[152] Again, rare events can have significant consequences.

104. The second fundamental usage of the collected biometric is by way of the ePassport[153] itself during the course of international travel. When the passport is issued, the facial photograph is both printed on the biographical page and embedded as a digital image on an electronic chip within the document.[154]

105. The embedded digital photograph enables three-way verification between the image on the passport, the image on the chip, and the person presenting the passport. Certain countries – including Canada (see the discussion of the PIK in paragraphs 125-137, below) – leverage facial recognition technology for this purpose. The result is greater confidence in a) the integrity and authenticity of the document, and b) that the individual presenting the document is the individual to whom it was issued. The chip is digitally signed using Public Key Infrastructure (PKI) techniques allowing for the verification of the document against the issuing country and to ensure that the data contained within has not been modified.[155]

106. Photographs submitted as part of passport applications, as well as the biometric templates derived therefrom, are retained until an applicant has reached 100 years of age.[156] IRCC

---

[152] See for example Martin Rudner "Misuse of Passports: Identity Fraud, the Propensity to Travel, and International Terrorism," *Studies in Conflict & Terrorism*. 2008. 31 (2): 95-110; Stefano Musco and Valter Coralluzzo "Sneaking Under Cover: Assessing the Relevance of Passports for Intelligence Operations," 2016. *International Journal of Intelligence and Counter Intelligence*. 2016. 29 (3): 427-446.

[153] As discussed in Section 4, Canada's ePassport was rolled out in 2013. The ePassport is now an internationally standard document, issued in over 135 countries and guided by ICAO specifications.

[154] The facial photograph is mandatory for ePassports as per ICAO guidelines. See ICAO, "Doc 9303: Machine Readable Travel Documents," Eighth Edition, 2021. Accessed 4 August 2021. https://www.icao.int/publications/Documents/9303_p9_cons_en.pdf. These guidelines also allow iris scans and fingerprints as optional biometrics, but Canada does not collect or include either in the Canadian version of the ePassport. At the rollout of the ePassport in 2013, Passport Canada indicated no plans to collect iris scans, fingerprints, or any other biometric information as part of the Passport Program, and acknowledged that regulatory adjustments and/or new Privacy Impact Assessments would be required before doing so. Passport Canada, "PIA National Rollout of ePassport 2013," p. 112 [IRCC RFI #2 Documents].

[155] The process is outlined here: ICAO, "Basics of ePassport Cryptography," N.D., Accessed 20 August 2021. https://www.icao.int/Security/FAL/PKD/BVRT/Pages/Basics.aspx

[156] If an individual holds a valid Canadian passport that will expire after his/her 100th birthday, the passport application and supporting documentation are retained electronically for one additional period that is equivalent to the validity period of the passport. IRCC written response to NSIRA, 4 December 2021, p. 6.

assesses that this retention period is consistent with the practices of international partners (e.g., the United Kingdom and Australia[157]), and balances, in their estimation, the need to issue secure, trusted travel documents with the requirements of the *Privacy Act* to retain personal information only for as long as necessary.[158] Hard paper copies of the passport applications, including photographs, are retained for six weeks following conversion to digital format, and subsequently shredded.

107. The length of the retention period facilitates identity management as individuals renew their passports over the course of their lifetime. Each returning adult applicant (e.g. renewal, replacement, etc.) can be verified through the FRS against previous applications from the same individual. Similarly, one-to-many FRS screening includes templates from most adult applicants, maximizing the scope of detecting possible identity fraud.

108. IRCC discloses photographs and related biographic information collected by the Passport Program to other government departments (OGDs). Unlike in the Immigration Program, these disclosures are not systematic. Rather, they come in response to *ad hoc* requests from OGDs with criminal, national security, and intelligence mandates. The OGDs make the requests pursuant to their own legislation, and their scope is circumscribed by s. 4 of the *Privacy Act*.[159] According to IRCC, the context of many of these requests is often the need for information regarding Canadians travelling abroad to engage in foreign conflicts or unlawful acts.[160]

109. Such requests can involve confirmation or validation of biometric information provided by the OGD against passport records, or identifying individuals of security concern by processing a photograph provided by the OGD through the FRS.[161] For example, the RCMP may identify a person of national security concern, but have only a photograph of the person (e.g. from their social media presence); CSIS may provide IRCC with a photograph of an individual they are investigating but cannot identify. Alternatively, the RCMP and CSIS may share photographs of known individuals with the IRCC. The purpose of these checks is to ensure the person has not obtained a passport under another identity.[162] The IRCC states that, for the RCMP, the scenarios

---

[157] Passport Canada, "PIA National Rollout of ePassport 2013," p. 121. [IRCC RFI #2 Documents]

[158] IRCC written response to NSIRA, 4 December 2020, p. 6.

[159] IRCC written response to NSIRA, 4 December 2020, pp. 9, 12; see, for example, ss. 12 and 19(2) of the *CSIS Act*, RSC 1985, c C-23; and s. 18(a) of the *RCMP Act*, RSC 1985, c R-10.

[160] IRCC written response to NSIRA, 4 December 2020, p. 9.

[161] IRCC written response to NSIRA, 4 December 2020, p. 9.

[162] IRCC written response to NSIRA, 4 December 2020, p. 9

described herein may require the RCMP to obtain a Production Order, depending on the particular circumstances of the request.

110. In both cases, the IRCC converts the photograph provided by CSIS/RCMP into a biometric template and runs it through FRS. In the first instance, in the event of a possible match, the IRCC would return limited biographic and/or biometric information to the RCMP or CSIS to assist in confirming the person's identity. In the second instance, the IRCC may validate the person's previously known identity and confirm whether the person's photograph is associated to any other identities logged by the Passport Program. The scope of information disclosed by the IRCC, in both cases, depends on the nature of the investigation and its authorities to disclose.[163]

111. The IRCC discloses this information pursuant to s. 5 of the *Security of Canada Information Disclosure Act* (*SCIDA*), if applicable, or may rely on s. 8(2)(e) of the *Privacy Act* in the case of specific requests.[164] Section 5 of *SCIDA* allows the IRCC to disclose information to the RCMP, CSIS and other specified institutions[165] where it is satisfied that the disclosure will contribute to the exercise of the recipient institution's jurisdiction in respect of activities that undermine the security of Canada. To disclose under *SCIDA*, the IRCC must also be satisfied that the disclosure will not affect a person's privacy interest more than is reasonably necessary in the circumstances.[166] In contemplating such disclosures, the IRCC affirms that it first obtains sufficient details to ensure these conditions are met.[167] In other instances, such as when the disclosure is to assist a law enforcement investigation, the IRCC may rely on s. 8(2)(e) of the *Privacy Act* to provide specific investigative bodies[168] with information they have requested in writing, for the purpose of enforcing Canadian law or carrying out a lawful investigation.[169] Where

---

[163] IRCC written response to NSIRA, 4 December 2020, p. 9.

[164] IRCC written response to NSIRA, 4 December, p. 12; see also *Security of Canada Information Disclosure Act*, SC 2015, c 20, s 2, s. 5; *Privacy Act*, R.S.C., 1985, c. P-21, s. 8(2)(e).

[165] See *Security of Canada Information Disclosure Act*, SC 2015, c 20, s 2 at s. 5(1) and Schedule III. Eligible recipient institutions also include the CBSA, CSE, and the Department of Public Safety and Emergency Preparedness.

[166] *SCIDA,* ibid s. 5(1).

[167] IRCC written response to NSIRA, 4 December 2020, p. 12. See, also, NSIRA and the OPC's "Review of Federal Institutions' Disclosures of Information Under the *Security of Canada Information Disclosure Act* in 2020" regarding the IRCC's general practices in this respect.

[168] These agencies are listed in Schedule II of the *Privacy Regulations,* SOR/83-508, and include CSIS, the RCMP, and 3 sub-groups within the CBSA, namely its Inland Enforcement Division, Intelligence and Targeting Operations Directorate, and Criminal Investigations Division.

[169] IRCC written response to NSIRA, 4 December, p. 12; see also s. 8(2)(e) of the *Privacy Act*.

a production order or warrant supports the OGD requests, section 8(2)(c) of the *Privacy Act* authorizes the disclosure of information for the purpose of complying with the warrant.

112. In addition to these disclosures to assist national security or law enforcement investigations, the IRCC may disclose information to the Department of Public Safety, where necessary to assist the Minister of Public Safety in rendering a decision under the CPO. Sections 10.1 and 11.1(2) of the CPO authorize the Minister of Public Safety to decide that a passport should not be issued, or that a current passport should be revoked or cancelled, when such action is necessary to prevent the commission of a terrorist act or protect the national security of Canada or a foreign state.[170] By virtue of this authority, the IRCC may collect information on an ongoing basis to verify an individual's continued entitlement to possess the document.[171] The IRCC also relies on the CPO to disclose, to the Minister of Public Safety, information necessary to support his decision on such matters.[172] In practical terms, this includes IRCC's disclosure of the relevant passport application, including the digitized photo, to Public Safety.[173] Section 5 of *SCIDA* and section 8(2)(a) of the *Privacy Act* (on consistent use) further support these disclosures.[174]

Assessing the Passport Program

113. A significant source of public concern regarding the use of facial recognition is the possibility that the technology will be inaccurate. In the passport context, false positive identification could lead to inconvenience and/or additional investigative attention for individuals.[175] False negatives, by contrast, worry operators, as they potentially undermine the security benefits of the system.

114. The FRS has certain natural advantages with respect to accuracy. First, it predominately uses high-quality probe images (templates extracted from passport photographs taken according to ICAO specifications) and searches them against the same (a gallery populated by templates

[170] CPO, s. 10.1, 11.1(2).

[171] IRCC written response to NSIRA, 4 December 2020, p. 11.

[172] IRCC written response to NSIRA, 4 December 2020, p. 8. See also CPO, s. 11.4.

[173] IRCC written response to NSIRA, 4 December 2020, pp. 8-9.

[174] IRCC written response to NSIRA, 4 December 2020, p. 12.

[175] Facial recognition results cannot lead automatically to the denial of an application, as decisions are not rendered on the basis of such results alone. However, if a false positive is not caught or corrected, it is conceivable that the weight of such evidence could be decisive in terms of denying an application. Because a false positive that is not caught or corrected would not be classified as an error, it is impossible to collect data on such instances.

extracted from passport photographs).[176] Exceptions are the images on the SL-FRS and images supplied by OGDs for checking against FRS, which may be of lesser quality. Second, the matching process is not time sensitive (as would be the case in a live environment such as a POE). Adjudication – triage, analysis, and investigation – of possible matches (one-to-many) or non-matches (one-to-one) can be conducted thoroughly before any decisions are made which affect individuals.

115. A related concern is that certain groups will be disproportionately affected by system inaccuracies. Extant research has demonstrated that age, gender, and ethnicity, among other factors, may influence the ability of a facial recognition system to accurately identify individuals, leading to possible bias and discrimination.[177]

116. IRCC employs several mitigation measures. First, enrolled templates are stored in one of six separate galleries according to age (adults 16+ and children under the age of 16) and self-identified gender (male, female, or other). Age and gender are known to be confounding factors in facial recognition; separating the database into galleries according to these characteristics allows thresholds to be adjusted as necessary to improve the performance of the system.

117. In January 2021, IRCC completed an evaluation of a next generation algorithm for possible use in FRS.[178] The results were favourable in terms of the accuracy observed in testing, and implementation of the new algorithm is set for 2021-22.[179] Specifically, the new algorithm demonstrated superior performance in terms of age and gender disparity as compared to the algorithm currently in use. The new algorithm demonstrated improvement in matching photographs taken at lengthy time intervals (e.g. 15 years), which is directly relevant to passport renewals. The testing did not evaluate, however, the algorithm's performance with respect to race and ethnicity.

118. IRCC provides public information regarding the use of facial recognition in the passport application process. The photograph guidelines posted on the IRCC website state that "The [ICAO] recommends that passport photos be taken with a neutral expression. *This lets us use facial recognition systems to help prevent fraud*."[180] Similarly, a Privacy Notice Statement is included

---

[176] The NIST identified image quality as an important factor reducing bias in facial recognition algorithms. See NIST, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," December 2019. Accessed 5 August 2021. https://doi.org/10.6028/NIST.IR.8280

[177] NIST, "Face Recognition Vendor Test (FRVT) Part 3."

[178] IRCC, "IRCC Facial Recognition Algorithm Analyses 2021." [IRCC RFI #2 Responses]

[179] IRCC written response to NSIRA, 3 August 2021, p. 4.

[180] Government of Canada, "Passport photos," October 5, 2010. Accessed 5 August 2021. https://www.canada.ca/en/immigration-refugees-citizenship/services/canadian-passports/photos.html, emphasis added.

on passport application forms, describing the collection, use, disclosure and retention of personal information, including biometrics.

119. The biometric embedded on the electronic chip in the ePassport does not constitute a significant risk or expansion beyond what was included in analog passports prior to the ePassport's implementation. What is on the chip – the facial image and biographical information – is also on page 2 (the biographical page) of the physical document itself.

120. By contrast, the issuance process – including the use of FRS – directly implicates both biometric information and national security considerations. Preventing *mala fide* actors – including those posing a threat to national or international security – from obtaining *bona fide* travel documents warrants stringent processes and security measures during the issuance phase. At the same time, information collected and used in the context of the issuance process will impact all individuals – millions of Canadians and individuals living in Canada – who apply for a passport or other official travel document.

121. The key consideration is whether the privacy impact of the FRS is commensurate with the benefit to national security associated with its collection, use, retention, and disclosure of biometric information.

122. The OPC's recent investigation into the RCMP's use of facial recognition services supplied by the private firm Clearview-AI is worth considering in this context.[181] In that case, the OPC found that the RCMP's leveraging of biometric information collected by Clearview-AI from social media and other internet sources violated the *Privacy Act* because Clearview-AI's collection of that information had been unlawful. More relevant for the present discussion, however, is the OPC's characterization of the *practical effect* of law enforcement's use of Clearview AI, which meant that "billions of people essentially found themselves in a '24/7' police line-up."[182] That is, the existence of their biometric information in a database available to law enforcement meant they were subject to identification by law enforcement at any time.

123. In national security investigations, there may be different policy justifications, security benefits, and disclosure limitations that render use of the IRCC's passport database proportionate. The disclosure of this information by the IRCC to the RCMP is also supported by law (see paragraph 111). The connection between passport biometrics and the investigations and activities of the RCMP, CSIS and CBSA remains a striking example, however, of the connections made possible by

[181] Office of the Privacy Commissioner, "Police use of Facial Recognition Technology." Please note, Clearview AI was never used by the RCMP in connection with the immigration program. We invoke the OPC's investigation for illustrative purposes as to the nature of privacy issues that may be raised by biometrics in general.

[182] Office of the Privacy Commissioner, "Police use of Facial Recognition Technology."

biometrics. Moving forward, NSIRA may wish to review these arrangements, to assess their reasonableness and necessity in terms of balancing individual interests (privacy, liberty, etc.) and the state's security goals.

Arriving into Canada

124. The Passport and Immigration programs are the major programs governing Canada's border continuum. Together, they help manage the processes by which individuals enter the country, largely by providing the documentation that makes international travel possible. Related to these larger programs is the actual process of arriving at a POE and going through Canadian customs and immigration. While the above discussions of both Immigration and Passport touched on these processes, this section discusses two additional activities that involve the analysis of biometric information to verify the identity of individuals arriving into Canada.

Primary Inspection Kiosks (PIKs)

125. Primary Inspection Kiosks (PIKs) are automated, self-serve kiosks present at ten major Canadian airports.[183] The kiosks facilitate the immigration and customs process for international arrivals into Canada.

126. As discussed in relation to the Immigration Program, biometrically-enrolled foreign nationals are subject to biometric verification upon arrival into Canada. At airports equipped with Systematic Fingerprint Verification (SFV), this occurs through PIKs.[184] Additionally, PIKs validate ePassports and help verify the identity of ePassport holders (including Canadians) using facial recognition (one-to-one matching) technology.

127. In 2019, PIKs processed 21,853,422 individuals, an average of 59,872 travellers per day.[185] This means that most individuals – whether Canadian or foreign – arriving in Canada by air have their biometrics analyzed in some way (either as biometrically-enrolled foreign nationals,

[183] Toronto-Pearson, Montreal-Trudeau, Ottawa, Vancouver, Quebec City, Winnipeg, Calgary, Edmonton, Halifax, and Toronto-Billy Bishop.

[184] The first generation PIK (1.0), deployed in 2015, did not have SFV capability. The second generation (2.0), deployed as part of the Biometrics Expansion Project between 2017-19, introduces the SFV capability, but is not yet deployed at all major international airports in Canada.

[185] CBSA, "Primary Inspection Kiosk (PIK) Program, ePassport Validation 2020, Version 1.0," CBSA, June 9, 2020, p. 6. [NSIRA_202002_03_015, p. 6.]

ePassport holders, or both).[186] CBSA derives its authority to collect information from individuals as they arrive in Canada from s. 11 of the *Customs Act* and ss. 15 and 18(1) of the *IRPA*.

128. The PIK facilitates risk assessment by sending passport and biographical information to CBSA for processing in real time. CBSA uses the information to check the traveller against existing traveller processing systems. This includes the Interdiction and Border Alert System and the Integrated Customs Enforcement System.[187]

129. According to CBSA, all information passes between the PIK and CBSA through an encrypted tunnel and is purged prior to the next traveller using the device.[188]

130. The use of the facial photograph embedded on the ePassport's electronic chip is for identity verification at the kiosk and during primary inspection. Facial recognition – or facial "matching" as it is called by CBSA in this context – occurs on a one-to-one basis by extracting the digital photograph from the chip and comparing it to a live photograph of the traveller captured by the kiosk. A match score is generated, based on the vendor's proprietary algorithm, and the score is sent to the CBSA to determine whether it is above or below a pre-determined threshold. The result is printed on the PIK receipt.[189] The CBSA itself defines the match/no-match threshold; it is not determined by, nor shared with, either the vendor or Airport Authorities.

131. The PIK receipt also includes the facial photograph taken by the kiosk. The traveller presents the receipt to a Border Services Officer (BSO); in the event of a no-match, the BSO may correct obvious non-technical errors (for example, one individual was photographed twice as part of a

---

[186] However, travellers are still able to select manual processing if they so choose. According to the PIA on the PIK, "the CBSA is targeting to direct 100% of travellers for processing via PIK, [but] a subset of travellers will choose or be directed to in-person processing for a number of reasons including language, technology aversion, documentation issues, or age." CBSA, "Primary Inspection Kiosk (PIK) Implementation 1.0: Privacy Impact Assessment (PIA)," December 2016. [NSIRA_202002_03_014, p. 15.] In 2019-20, 93.2% of travellers used the PIK at airports where it was available, and the agency has set a target of 95% for this metric by 2022. See CBSA, "2021-22 Department Plan" 2021. Accessed 20 August 2021. https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/rpp/2021-2022/report-rapport-eng.pdf, p. 18. Finally, while ePassports are now internationally the norm, there remain analog passports in circulation, which can be scanned by PIKs but do not facilitate facial recognition; analog passport holders have their passport image manually verified by BSOs.

[187] These system queries provide additional information by checking various sources including Targets, Lookouts, prior enforcement records, CBSA's Lost and Stolen Fraudulent documents dataset, INTERPOL's Stolen and Lost Travel Document database, and Canadian Police Information Centre (CPIC) wants and warrants. CBSA written response to NSIRA, 10 June 2021, p. 2.

[188] CBSA written response to NSIRA, 6 July 2021, p. 2.

[189] The result is coded on the receipt and not interpretable by the traveller.

group of two travellers) through visual verification, ask additional questions, and/or refer the individual to secondary inspection on a discretionary basis.

132. The inclusion of the photograph on the receipt was a significant issue in the 2012 PIA conducted for the PIK project. CBSA justified the practice on the basis of efficiency (quicker processing by the BSO collecting receipts) and security (preventing receipt swapping prior to egress at primary inspection).[190] The PIK receipt – including the printed photograph – is retained by CBSA for seven years.[191] The OPC expressed concerns regarding this retention period given the presence of the traveller's photograph.[192] In essence, the retention of these photographs constitutes a database of (nearly) all travellers who enter Canada. While CBSA asserted that the photographs are not searchable nor used for facial recognition purposes, OPC noted the sensitivity of retaining biometric information[193] in centralized databases and has urged CBSA to consider mitigation strategies.[194]

133. The CBSA details the necessary specifications and requirements for PIKs, but relies on Airport Authorities to procure both the hardware and software (including the algorithm used for facial matching). This means that different versions exist at different airports across Canada. The accuracy of the facial matching process consequently varies between locations. The algorithms are proprietary, meaning CBSA does not have visibility into precisely how they operate, though it does have access to data on accuracy and performance through the US Department of Commerce's National Institute of Standards and Technology (NIST) as well as from in-house performance testing.

134. In 2020, CBSA evaluated the performance of the four face-matching algorithms integrated in the three kiosk designs currently in use, and determined that opportunities existed to improve performance in certain airports by adjusting facial matching thresholds.[195] The testing similarly

---

[190] CBSA, "Primary Inspection Kiosk (PIK) Implementation 1.0: Privacy Impact Assessment," Passenger Processing Unit, N.D., [NSIRA_202002_03_014.]

[191] CBSA written response to NSIRA, 4 February 2021, "Annex 5 - Travellers Branch (PIK & SFV)," p. 1.

[192] OPC letter to CBSA, "Re: Privacy Impact Assessment – Primary Inspection Kiosk (PIK) Implementation 1.0," October 16, 2017. [NSIRA_202002_03_013, p. 4.]

[193] Even if not presently used for, or searchable by, facial recognition, the quality of the photographs and the existence of the database means that such information *could* be used for biometric analysis in the future.

[194] For example, redacting the photographs prior to storing the receipt, or eliminating the photograph from the receipt and requiring the BSO to examine the passport photograph of the traveller instead.

[195] CBSA, "Memorandum: PIK/Nexus Kiosk Performance as Function of Matching Threshold: Opportunity for Improvement in Toronto," Chief Data Scientist, October 20, 2020, p. 1. [NSIRA_202002_03_001, p. 1.]

examined issues of possible demographic bias.[196] The results suggested that small discrepancies[197] along the lines of gender (lower matching rates for females) and age (lower matching rates for younger and older) did exist in airports using a particular algorithm. Recommendations for mitigation included shifting vendors and/or setting gender-specific match thresholds, though the latter option was considered potentially problematic in terms of inviting higher false positive match rates.

135. Public reporting has expressed concern that higher facial matching error rates for certain ethnicities might result in more frequent referrals from PIKs to secondary inspection.[198] It has been observed, for example, that rates of referral are higher for nationals from Iran and Jamaica, as compared to countries such as Iceland and Denmark.[199] The CBSA indicated to NSIRA that no referrals to secondary inspection occur as a result of the facial matching process (i.e. there are no referral codes associated with facial matching leading from the PIK to secondary inspection). In practice, however, a failed match will lead to greater scrutiny as a BSO at primary inspection assesses the reason for the failed match. It is possible that discretionary referrals to secondary occur as a result; the CBSA does not track statistics associated with this scenario.[200]

136. CBSA is aware of concern regarding possible bias associated with higher facial match error rates for certain ethnicities,[201] and points to improvements in the overall accuracy of algorithms that will help close any gaps in performance across demographic categories. Further, CBSA notes that its "work in this area is nascent and is not yet conclusive with significant work still to be conducted." Given the significance of the public interest and concern associated with possible bias, NSIRA encourages CBSA to continue its work in this area. In addition to technical solutions

---

[196] CBSA, "Memorandum: Gender 'Bias' in PIK/Nexus Kiosks," Chief Data Scientist, October 21, 2020. [NSIRA_202002_03_002]

[197] Between 2-4%. CBSA, "Memorandum: Gender 'Bias'...," p. 2. [NSIRA_202002_03_002, p. 2.]

[198] See for example Evan Dyer, "Bias at the border? CBSA study finds travellers from some countries face more delays," *CBC News,* April 24, 2019. Accessed 6 August 2021. https://www.cbc.ca/news/politics/cbsa-screening-discrimination-passports-1.5104385; Beaumont, "When Border Security Crosses a Line,"; Israel, "Facial Recognition at a Crossroads."

[199] Dyer, "Bias at the border?" CBSA responded to these observations by stating that a "macro level analysis…found no systematic evidence of bias" and that different referral rates were likely a reflection of on-average differences between populations in terms of reasons for seeking admission to Canada (e.g. more Iranians arriving to settle – which consequently invites additional scrutiny – as compared to Icelanders arriving for tourism).

[200] By contrast, CBSA does track referrals to secondary based on fingerprint verification. In FY2020-21, there were 300,033 total referrals from PIKs to secondary inspection. Of these, 28,998 were under the referral code "Bio Verification Required", indicating the verification with RCMP databases was incomplete, inconclusive, or resulted in a no-match. CBSA written response to NSIRA, 10 June 2021, pp. 4-5.

[201] CBSA, "Biometrics (Face Recognition) in CBSA: Overview of Latest Research Findings, Networks and Resources," Chief Data Office, October 1 2020. [NSIRA_202002_03_003.]

aimed at further closing identified gaps, an examination of the implications of facial matching errors on travellers might suggest policy solutions to mitigate any possible disparate impacts.

137. The PIK will continue to play an integral role in future applications of biometric technology at Canada's international airports. As noted in the CBSA's 2021-22 Departmental Plan, the agency is set to integrate the PIK into new applications of mobile technology with the aim of further streamlining the customs and immigrations arrival process.

NEXUS

138. NEXUS is a voluntary trusted traveller program intended to expedite border crossing between the US and Canada for preapproved, low-risk travelers ("NEXUS").[202] Section 11.1(1) of the *Customs Act* authorizes the Minister to administer such programs, by allowing him to authorize persons to present themselves at the border "in an alternative manner."[203] The program is jointly managed by CBSA and US Customs and Border Protection (CBP).[204] As mentioned in Section 4, although NEXUS began as a pilot initiative prior to 9/11, it was expanded and implemented following the attacks with an eye toward robust identity verification and traveller facilitation in the context of enhanced border security.

139. In 2019, NEXUS underwent a "modernization" process, which saw the adoption of the PIK facial-matching model into NEXUS-dedicated kiosks for air arrivals,[205] replacing iris scans with facial matching as the biometric modality for identity verification.[206] In order to facilitate facial matching, CBSA collects the biometric from electronic passports, stores it in the NEXUS database, and uses the photograph to verify identity during travel.[207] The process is similar to how the PIK operates in other traveller streams and produces roughly similar outcomes.[208] The main

---

[202] Applicants undergo pre-screening against criminal, immigration, and customs databases.

[203] The manner being alternative to s. 11(1) of the *Customs Act,* which requires every person arriving in Canada to enter Canada only at a customs office designated for that purpose and present themselves without delay to an officer and truthfully answer any questions. See also the *Presentation of Persons (2003) Regulations*, s. 6.1, and *IRPR*, s. 38(a).

[204] Membership composition is roughly 20% American and 80% Canadian. CBSA, "NEXUS Modernization Air Mode," June 7, 2018, p. 4. [NSIRA_202002_004, p. 4]

[205] This section primarily deals with NEXUS Air Mode (i.e. NEXUS at air POE); the NEXUS program similarly offers expedited processing at land (21 major land border crossing into Canada) and marine (22 NEXUS only sites) POE. However, no technology-based biometric analysis occurs in the NEXUS Land or Marine modes. CBSA written response to NSIRA, 4 February 2021, "Annex 4 - Travellers Branch (NEXUS program)," p. 1.

[206] CBSA, "NEXUS Modernization Air Mode," June 7, 2018. [NSIRA_202002_004]

[207] CBSA written response to NSIRA, 4 February 2021, "Annex 4 – Travellers Branch (NEXUS program)," p. 2.

[208] CBSA, "PIK/NEXUS Kiosks: Performance Audit Report," May 21, 2020. [NSIRA_202002_03_005]

difference here is that the photograph taken at the kiosk is matched against the traveller's image in the NEXUS database.[209] NEXUS' purpose in using the passport photograph is the same as in the regular PIK process: to verify the individual's identity prior to allowing them admission into Canada. NEXUS' use of the passport photograph was preferred because the image provides better facial recognition matching (given that it was taken according to ICAO specifications) as compared to the membership photograph (taken by border services officers under varying conditions – light, background, distance, etc.). NEXUS participants are informed of the extraction of their passport photograph for facial matching purposes.

140. NEXUS' voluntary nature, and the consistent purpose of using the passport photograph within NEXUS to facilitate identity verification and travel, renders this second use of the ePassport photograph reasonable in NSIRA's view. The consistency of purpose between the programs also respects the norms and the requirements of sections 7 and 8 of the *Privacy Act.*

141. The use of the passport photograph for facial matching within NEXUS is nevertheless noteworthy as an example of when it has been beneficial to use an existing biometric in an additional program. The dual-use of biometrics in this case is relatively benign, but the dynamic which produced it – that is, the convenience, availability, and possible value-added (accuracy in identification) of existing biometric information – is likely to be common to scenarios which may be of more concern, as discussed below (see paragraphs 191-201, below).

6. BIOMETRICS *FUTURE*

142. We expect the landscape detailed in the preceding sections of this report to change significantly in the short-, medium-, and long-term. In this section, we highlight select projects and initiatives to illustrate how biometrics in the border continuum are likely to evolve, and to mark key points of consideration for Canadians – and NSIRA – as we move into this unfolding technological future.

143. The GoC has publicly committed to continued research, development, and deployment of biometric technologies in the border continuum. For instance, Budget 2021 allocates $656.1 million over five years (beginning in 2021-22) and $123.8 ongoing to the CBSA for the

[209] CBSA written response to NSIRA, 4 February 2021, "Annex 4 – Travellers Branch (NEXUS program)," p. 3.

"modernization" of Canadian borders.[211] CBSA "proposes to utilize new technologies, such as facial recognition and fingerprint verification" as part of such efforts.[212]

144. The agency has announced the creation of an Office of Biometrics and Identity Management (OBIM)[213] under a newly formed Biometrics Transformation Directorate (BTD) within the Chief Transformation Officer Branch (CTOB). CBSA indicated to NSIRA that the purpose of the BTD is to coordinate biometric initiatives (including design, implementation, and operation) across the agency. In addition to its coordination role, OBIM will act as a Centre of Expertise and focal point within CBSA for guidance on the appropriate use of biometrics. This will include developing and managing CBSA's biometrics governance, risk and compliance framework.[214] A June 2021 Notice of Proposed Procurement (NPP) solicited proposals from contractors for aid in establishing the OBIM and "to work with the [CBSA] in researching, planning for and rapidly developing a strategy and roadmap related to the use of Digital [sic] solutions enabled by supporting technologies in biometrics, in response to the COVID 19 situation and other operational priorities."[215] The proposal further specified that the successful contractor would aid in "the development of a comprehensive approach and plan to manage, evolve and adapt in using biometrics" to fulfill CBSA's mandate and objectives.[216] As part of this coordinating function, the OBIM will review current steady-state biometric activities and make recommendations where necessary for aligning them with overarching CBSA standards and objectives.[217]

145. With respect to immigration, CBSA's Departmental Plan 2021-22 commits to "explor[ing] measures to standardize the collection of biometric information on potentially inadmissible travellers to strengthen compliance verification at the border."[218] In July 2021, IRCC released a tender notice soliciting industry information regarding the procurement of a next generation

---

[211] Government of Canada, "Budget 2021: A Growth Plan for Jobs, Growth, and Resilience," 2021. Accessed 8 August 2021. https://www.budget.gc.ca/2021/pdf/budget-2021-en.pdf, p. 144.

[212] Government of Canada, "Budget 2021," p. 493.

Canadian Press Staff, "Canada's border agency urgently developing biometric plans in response to COVID-19," *CTV News,* June 7, 2021. Accessed 8 August 2021. https://www.ctvnews.ca/health/coronavirus/canada-s-border-agency-urgently-developing-biometric-plans-in-response-to-covid-19-1.5459521.

[214] IRCC written response to NSIRA, 1 October 2021.

[215] Public Services and Procurement Canada, "Biometrics and Identity Management (1000357607)," June 14, 2021. Accessed 8 August 2021. https://buyandsell.gc.ca/procurement-data/tender-notice/PW-21-00958775.

[216] Public Services and Procurement Canada, "Biometrics and Identity Management (1000357607),"

[217] CBSA written response to NSIRA, 22 July 2021, p. 1.

[218] CBSA, "2021-22 Departmental Plan," p. 16.

Canadian Immigration Biometric Identification System (CIBIDS).[219] The new system will "take advantage of the latest technologies [...] to modernize [IRCC's] biometric technology solution" and may include the "design and development of a new IRCC custom Biometric Collection Solution."[220]

146. "Next generation" development is occurring in the Passport Program as well, with "a new passport booklet, incorporating advancements in technology to enhance the document's durability and security features"[221] aimed, in part, at "alignment with documents issued by our Five Nations Passport Group partners."[222] Phased rollout of the new ePassport will occur between 2023 and 2024.

147. Passport issuance, similarly, is undergoing "modernization", as part of an ongoing process initiated in 2013 to facilitate the transition of the Passport Program from the Department of Foreign Affairs, Trade and Development to CIC (now IRCC). The Passport Program Modernization Initiative (PPMI) is a multi-year project that is scheduled to be completed in 2023. PPMI intends to streamline "all aspects of Passport Program operations" and "keep pace with evolving international passport issuance and identity management best practices."[223] The initiative also aims to systematize passport services across intake locations, and lay "the foundation for online passport services and automation to improve the service experience."[224]

148. In June 2020, IRCC issued an NPP for a "Passport Digital Services Project" that "will allow Canadians to apply online for passports, using a computer, tablet or mobile device, as a convenient alternative to mail-in or in-person service options."[225] The procured platform will transmit passport applications – including digital photographs – from individuals to IRCC. Media

---

[219] Public Services and Procurement Canada, "CIBIDS Next Generation LOI (B8465-220030/A," July 29, 2021. Accessed 10 August 2021. https://buyandsell.gc.ca/procurement-data/tender-notice/PW-XQ-012-39765.

[220] Public Services and Procurement Canada, "CIBIDS NextGen Technical RFI," July 8, 2021. Accessed 10 August 2021. https://buyandsell.gc.ca/cds/public/2021/07/08/7df664b99b6dc89db6043394db82e957/ABES.PROD.PW__XQ.B012.E39765.EBSU000.PDF, p. 2.

[221] IRCC, "Evaluation of the Passport Program," p. 32.

[222] IRCC, "Status Report on Transformation and Major Crown Projects," March 10, 2020. Accessed 11 August 2021. https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/departmental-plan-2020-2021/status-report-on-transformational-major-crown-projects.html.

[223] IRCC, "Status Report on Transformation and Major Crown Projects."

[224] IRCC, "Status Report on Transformation and Major Crown Projects."

[225] Public Services and Procurement Canada, "Passport Digital Services Project," June 22, 2020. Accessed 11 August 2021. https://buyandsell.gc.ca/cds/public/2020/06/22/90ca86cfd313f44e57da7fd116f6e317/ABES.PROD.PW__XS.B002.E38054.EBSU000.PDF.

reporting in early 2021 indicated that IBM was selected as the successful bidder.[226] The proposed system has generated privacy concerns, particularly with respect to transmitting biometric information (digital photographs) over a private platform.[227] We can expect the tension illustrated here, between convenience and privacy, to be a key theme in public conversations surrounding new biometric activities in the coming years.

149. In this vein, CBSA's Department Plan 2021-22 highlights several experimentation and innovation initiatives involving mobile technology (e.g. smartphones), including "explor[ing] digital identity concepts and opportunities to pilot digital identity in the travel continuum from a border management perspective." Digital Identity refers to paper-less identification, whereby trusted and secure digital proof of one's identity replaces traditional, physical documentation (e.g. passports, driver's licenses, etc.).[228]

150. A Digital Identity is typically linked to an individual through biometrics. ICAO's first iteration (Type 1) Digital Travel Credential (DTC), for example, "binds" a traveller to their Digital Identity by way of the biometric embedded in the ePassport, limiting the need to produce the physical document during travel.[229] The DTC is an international project that, while coordinated by ICAO, includes input from jurisdictions around the world and encompasses several future iterations (Types 2 and 3). IRCC and CBSA are currently members of ICAO's New Technology Working Group (NTWG) and the NTWG's Digital Travel Credentials (DTC) sub-group. Ultimately, the long-term vision of the DTC

---

[226] Estelle Côté-Sroka, "Virtual passport app presents real data risk, experts warn," *CBC News,* February 22, 2021. Accessed 11 August 2021. https://www.cbc.ca/news/canada/ottawa/passport-application-online-program-1.5920625.

[227] Côté-Sroka,"Virtual passport app presents real data risk," In a written response to NSIRA on 1 October 2021, IRCC noted that "[w]hile IBM was the successful bidder, the solution has been deployed in the IRCC Protected B cloud. The solution is compliant with TBS guidelines. All personal details of Canadians are under the control of IRCC. Further, the department conducted a PIA on the new […] solution as part of the pilot development to identify and provide a means to correct any other privacy concerns. OPC was engaged throughout the pilot development process."

[228] The implementation of Digital Identities is set to increase in the coming years, across both the private and public sectors. The vision of an organization like the Digital Identification and Authentication Council of Canada (DIACC) (https://diacc.ca/the-diacc/) – a non-profit coalition of public and private sector entities – is "to establish a…digital ecosystem" whereby a common and recognized Digital Identity would be transferable between contexts (from applying for a mortgage to accessing government services). See also Identity North (https://www.identitynorth.ca/).

[229] R. Rajeshkumar, "Digital Travel Credentials," ICAO, May 2021. Accessed 10 August 2021. https://www.icao.int/Meetings/TRIP-Symposium-2021/PublishingImages/Pages/Presentations/Digital%20Travel%20Credential%20%28DTC%29%20Policy%20and%20Guiding%20Principles.pdf.

project is to replace physical passports with Digital Identity "tokens" (which would include the facial photograph from the ePassport) stored on mobile devices.[230]

151. As discussed in Section 4, IRCC and CBSA's FASTER-PrivBIO Project (2015-2017) also explored the use of identity "tokens," stored in a mobile application, in the context of Electronic Travel Authorizations (ETAs). FASTER-PrivBIO closed in 2017, and "Phase II" of the project became the Chain-of-Trust (CoT) initiative, led by CBSA in collaboration with IRCC, Defence Research and Development Canada (DRDC), the University of Ottawa, and industry partners.

152. CoT further explored the adoption of mobile technology in the eTA process, while also expanding to include other steps in the travel continuum. As described in CBSA's Blueprint 2020 Report (published in December 2018):

> [t]he Chain of Trust process would require travellers to download an app to their smartphone and create an account including a unique identifier built from their biometrics. At every stage of the trip – from flight reservation, to obtaining a boarding pass, to disembarking the plane – the traveller's data would be collected and used to speed up the traveller's passage. Just before landing, the traveller would create an e-declaration and digitally sign it using biometric facial verification. Upon arrival, cameras would match the biometric face to the traveller's unique identifier.[231]

153. The purpose of the process, ultimately, is to enhance risk assessment. Linking traveller information to traveller identity throughout the travel continuum (including by using facial recognition as an individual moves through the airport) facilitates the flow of low-risk travellers (including by minimizing touch-points with border control, a feature that will take on additional significance in the context of post-COVID 19 travel), while enhancing the detection of possible high-risk travellers.

154. In 2018, a simulated prototype demonstrated the basic features and process flow of the CoT to Canadian government officials.[232] While the prototype project closed in 2019, the overarching CoT initiative continues, as per CBSA's 2021-22 Departmental Plans, through the deployment of "small-scale minimum viable products to assess feasibility in a live environment and obtain user experience feedback."[233] The stated goal of CoT remains the streamlining of "traveller

---

[230] ICAO, "The ICAO Digital Travel Credential," March 2020. [NSIRA_202002_012]

[231] CBSA, "CBSA – Blueprint 2020 Report: Chain of Trust Prototype," December 2018. Accessed 10 August 2021. https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/bp2020/2018/trust-confiance-eng.html.

[232] World Reach, "Canada's Chain of Trust Project," N.D., Accessed 10 August 2021. https://worldreach.com/resources/video-library/canadas-chain-of-trust-seamless-travel/.

[233] CBSA, "2021-2022 Departmental Plans," p. 16.

identification through the use of digital travel credentials and biometrics."[234] Notably, CoT is explicitly aligned with other international initiatives and projects, including ICAO's DTC,[235] reflecting the extent to which coordination exists in the broader ecosystem of biometric experimentation.

155. To be clear, the features of CoT described above do not reflect current practice at the border, nor do they represent commitments from CBSA (or any other GoC entity) regarding what the traveller experience will look like in the future. By the time the CoT, some version of it, or a new project operating in similar terrain, is implemented, the specifics of how biometrics verify identity or travellers move through the airport may have significantly changed. Nonetheless, the trend lines are apparent, as Digital Identity, mobile technology, and biometric verification converge on the traveller experience.

156. An additional example is the Known Traveller Digital Identity (KTDI) pilot project, led by Transport Canada (TC) in collaboration with the World Economic Forum (WEF), the government of the Netherlands, and commercial partners. In 2018, Canada announced its participation in the WEF's broader KTDI vision[236] and, in 2019, committed to a proof of concept pilot project which would operate between Canadian (Toronto-Pearson and Montreal-Trudeau) and Dutch (Amsterdam-Schiphol) airports on Air Canada and KLM Royal Dutch Airlines flights.[237] This project may access required funding under Budget 2021, which proposes $105.3 million over five years to develop an approach to digital identity for air travellers.[238]

---

[234] CBSA, "2021-2022 Departmental Plans," p. 16.

[235] Others include the World Travel & Tourism Council's Safe and Seamless Traveller Journey and IATA's OneID. World Reach, "Chain of Trust – Canada," 2020. Accessed 10 August 2021. https://worldreach.com/wp-content/uploads/2019/11/CaseStudy_CanadaChainofTrustProject_v2.pdf.

[236] Transport Canada, "The Government of Canada to test cutting-edge technologies to support secure and seamless global travel for air passengers," News Release. January 25, 2018. Accessed 10 August 2021. https://www.canada.ca/en/transport-canada/news/2018/01/the_government_ofcanadatotestcutting-edgetechnologiestosupportse.html.

[237] Toronto Pearson, "Toronto Pearson collaborates with government, industry to pilot paperless travel," Press Release. June 26, 2019. Accessed 10 August 2021. https://www.torontopearson.com/en/corporate/media/press-releases/2019-06-26

[238] Government of Canada, "Budget 2021," p. 74.

157. KTDI will combine blockchain technology[239] and facial recognition to "provide a seamless and secure air travel experience facilitated via a mobile application."[240] Travellers will have their facial photograph captured for one-to-one matching against their ePassport photograph at different touch points in the travel continuum (e.g. boarding and customs). They will be able to "push" their information (including their facial biometric) to relevant partners (e.g. airlines or Dutch or Canadian customs) at their own discretion, or revert to conventional identity verification (e.g. ePassport) at any time. While TC will interface with CBSA to conduct checks on ePassports at enrolment (to verify authenticity and ensure that the document is not lost or stolen) no passenger risk assessments will be conducted.

158. At the time of writing, the pilot is not yet live. The COVID-19 pandemic has impacted both the project's timelines and its operational context. Originally, part of the rationale for KTDI was to accommodate increasing traveller volumes; although the pandemic has led to a decrease in travel volumes, it has also amplified the need for low-contact, 'touchless' travel.[241] Indeed, the budget commitment noted in paragraph 156 was linked to the GoC's investment in "safe air travel […] that limits transmission of COVID-19 and protects travellers."[242] For present purposes, the KTDI is important for what it suggests about the general trajectory of biometrics in the air travel and border continuum.

159. The Canadian KDTI pilot traces its origins to the broader KDTI vision articulated by the WEF. In the WEF's KTDI concept, passports would effectively be replaced with digital credentials stored on mobile devices, while facial recognition-enabled gates (often referred to as smart gates or e-gates) would allow passengers to transit through airports from arrival to boarding to customs and exit with little to no interruptions.[243] Other elements of the travel experience – for example hotel and car rentals, or shopping at duty free – would also be incorporated. Over time, travellers would compile a trail of interactions – or "attestations" – from various entities (border control,

---

[239] Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. NIST, "Blockchain Technology Overview," October 8, 2018. Accessed 15 September 2021. https://www.nist.gov/publications/blockchain-technology-overview.

[240] Transport Canada briefing to NSIRA, 20 July 2021, slide 3.

[241] See the discussion in "How biometrics can help airlines take off again," *Biometric Technology Today*, 2021 (1): 8-11. https://doi.org/10.1016/S0969-4765(21)00010-2. Accessed 5 October 2021.

[242] Government of Canada, "Budget 2021," p. 74. See also the mention of "KTDI" during parliamentary debate on 20 April 2021. Accessed 10 August 2021. https://www.ourcommons.ca/DocumentViewer/en/43-2/house/sitting-84/hansard.

[243] Facial recognition at check-in, baggage drop, security, boarding, etc. would limit the number of interactions travellers have with airport officials.

commercial entities) that cumulatively built trust in that individual. Risk profiles, supplemented by security screening, would help determine the level of scrutiny applied to a traveller by relevant authorities. Further, the Digital Identity "wallet" (encrypted mobile application) would include more than just passport information and biometrics, storing bank information, health records (including proof of vaccinations), educational degrees, credit scores, etc.[244]

160. This broader vision is ambitious. The Canadian KTDI pilot – even as it evolves to reflect post-COVID priorities – is decidedly more circumspect in its aims. TC was clear in communications with NSIRA that the pilot (while including the WEF as a partner) is distinct from, and not beholden to, the broader WEF vision. Yet the sheer ambition of the latter indicates a probable trend in the future of international travel. As this report has demonstrated, the use of biometrics tends toward expansion over time. Concomitant advances in mobile technology – including the development of secure Digital Identity platforms, predicated on biometrics – find natural application in the border continuum, where identification is key and, increasingly, so is convenience.[245]

161. However, enhanced convenience continues to rub up against privacy concerns, particularly with respect to facial recognition technology. A robust public debate is emerging regarding the legal authority for the use of facial recognition in public spaces. Jurisdictions around the world are grappling with how to manage the proliferation of facial recognition technology, in some cases issuing moratoriums or outright bans on new applications of the technique until its implications are properly considered and new legal and/or regulatory frameworks governing its use are established.[246] The OPC's recent investigations into the use of Clearview-AI by the RCMP reflect the Canadian salient of this broader conversation.

---

[244] World Economic Forum, "Digital Borders: Enabling a secure, seamless, and personalized journey," White Paper. January 2017. Accessed 10 August 2021. http://www3.weforum.org/docs/IP/2017/MO/WEF_ATT_DigitalBorders_WhitePaper.pdf. See also World Economic Forum, "The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel," System Initiative on Shaping the Future of Mobility. January 2018. Accessed 10 August 2021. http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.

[245] IATA, "Global Passenger Survey (2019)," Accessed 4 October 2021. https://www.iata.org/en/pressroom/pr/2019-10-16-01/

[246] See the discussion of "Restriction on the use of facial recognition technologies" in Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?" Human Rights Center: University of Minnesota. 2020. Accessed 12 August 2021. https://www.ohchr.org/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf, p. 26. See also UK Science and Technology Committee, "Current and future uses of biometric data and technologies," February 2015. Accessed18 August 2021. https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/73402.htm . Note also the call for moratoriums by the European Commission and Alphabet chief executive Sundar Pichai, as reported in Taylor Owen and Nasma Ahmed, "Let's face the facts: To ensure our digital rights, we must hit pause on facial-recognition technology," *The Globe and Mail*, February 14, 2020. Accessed 12 August 2021. https://www.theglobeandmail.com/opinion/article-lets-face-the-facts-to-ensure-our-digital-rights-we-must-hit-pause/. For an example in the Canadian context see Letter from Charlie Angus, Member of Parliament

162. The basic contours of the debate are whether existing frameworks for the handling of personal information (in some cases drafted decades ago, before the advent of facial recognition and other biometric technology) are adequate or whether specific legislation is required, designed explicitly for facial recognition.[247] Greater specificity in legislation would enable standards to be set as to when the use of facial recognition is appropriate and proportional. It would also enhance the transparency of the norms set by Parliament and provide public information about the circumstances in which Parliament considers facial recognition to be lawful and reasonable in promoting security and convenience in Canadian society.[248]

163. The OPC is currently drafting new privacy guidance on biometrics, for both the public and private sector, intended to shape how the technology is applied moving forward. While the border context is distinct from other public settings when it comes to privacy, applications of biometric technology at the border cannot be exempt from emerging legal and societal norms. The development of new activities must be aware of such challenges, and account for shifts in the legal and regulatory landscape.

164. Public concern is likely to be most acute with respect to live capture facial recognition, in the vein of the FOTM pilot discussed in Section 4. Static, one-to-one verification of identity at mobile kiosks – for example as currently takes place at PIKs – is well-established, and allows travellers to know when facial recognition is being used. Roving, one-to-many identification – in which biometrics are captured at a distance – are the source of more anxiety. Consider, for example,

---

Timmins-James Bay to Minister of Justice and Attorney General of Canada David Lametti re RCMP Use of Clearview AI's facial recognition software, March 2, 2020. Accessed 4 October 2021. https://www.charlieangus.ca/post/rcmp-use-of-clearwater-ai-s-facial-recognition-software.

[247] See for example the discussions of various facial recognition cases in INCLO, "In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World," January 2021. Accessed 11 August 2021. https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf. See also the statement from the Association for Computing Machinery's US Technology Policy Committee, "Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies," June 30, 2020. Accessed 11 August 2021. https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf. As well as the discussion of "lawfulness" in the Council of Europe's Guidelines on Facial Recognition: "Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," January 28, 2021. Accessed 11 August 2021. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3, p. 4.

[248] See for example Government of Canada, "National Security Transparency Commitment," December 22, 2020. Accessed 12 August 2021. https://www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html#s2.

the legal challenge to the use of this type of facial recognition in the UK[249] and the multiple calls for moratoriums with respect to the use of facial recognition in public places.[250]

165. Given the developments described above, NSIRA expects that biometric information will be systematically incorporated into the traveller experience across the border continuum moving forward. Security considerations and general identity management will remain important, but so too will traveller convenience and, in the wake of COVID-19, 'touchless' or decongested travel. The use of mobile technology and Digital Identities reflect broader societal trends that are particularly well-suited for application in the border continuum. Informed consent, and/or specific, transparent legal authorities are important considerations for ensuring that such applications occur lawfully and with sound public understanding surrounding when biometrics are collected, how they are used, and how they are protected when in the possession of the government.

7. OBSERVATIONS

166. This report has documented and described the GoC's use of biometrics in the border continuum. The scope of these activities is large and growing. For government, biometric information offers a firm foundation for identity management. At the same time, civil society groups, academics, and other concerned Canadians worry about the privacy implications of the government collecting, using, retaining, and disclosing information about immutable physical characteristics. The fundamental purpose of the present study was to inform this ongoing conversation, to both demystify present government activities and evaluate them from NSIRA's unique, crosscutting perspective. In this final section, we leverage that perspective to articulate our observations according to nine general themes.

1. Biometrics and National Security

167. Biometrics enhance identity management; identity management at the border in turn serves national security. As outlined in Section 4, the impetus for the expanded collection and use of biometrics, particularly post-9/11, was their purported national security benefits.

---

[249] Liberty Human Rights, "Legal Challenge: Ed Bridges v. South Wales Police," N.D., Accessed 11 August 2021. https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/.

[250] *Supra* note 246.

168. Nonetheless, **the centrality of national security as a justification for biometric activities has waned over time relative to other objectives.**

169. First, there were the broader benefits associated with identity management, including assessing admissibility and entitlement, preventing fraud, and introducing efficiencies into service delivery. Of note, the CBSA and IRCC do not currently characterize their steady-state biometric activities primarily in national security terms. The Passport Program's purpose is to enable the travel of eligible Canadians, while the Immigration Program's purpose is to manage the flow of foreign nationals into Canada, the vast majority of whom arrive for legitimate reasons. Biometrics are information about individuals that facilitate these functions. The benefits to national security, in each instance, are a consequence of the robust identity management to which biometrics contribute.[251] More recently, traveller facilitation has risen to the fore, with programs and pilots incorporating biometrics and mobile technology in pursuit of "seamless" and "touchless" travel (the latter of particular interest given COVID-19).

170. Although biometrics extend beyond the national security domain, the national security outcomes they support are undeniable. Part of identity management is identifying *mala fide* actors, including possible terrorists, Canadian extremist travellers, and other national and international security threats. Biometric screening for both immigration and passport applications, for example, includes querying databases (domestic and foreign) that may return information pertinent to national security (e.g. presence on a watchlist, suspected terrorist activity, previous national security convictions, multiple identities, etc.).

171. The assessment of these programs' proportionality must therefore be done in light of the full panoply of benefits that biometrics contribute to Canada's activities at its border. This includes their benefits for identity management in admissibility and passport decisions, traveller screening, and also national security.

172. As pertains to areas for future NSIRA review, the present study's overview of the border continuum highlighted several possibilities:

- The collection of biometrics at Visa Application Centres (VACs). Here the national security concern stems from personal information – including biometrics – passing through VACs operating in high-risk jurisdictions and run by private contractors and sub-contractors. A review of VACs would include the risks associated with the collection and transmission of

[251] For example, fraudulent passport applications may be deterred or detected; foreign nationals posing a security risk may be deterred from applying to come to Canada or, if they do apply, identified through their biometrics, leading to the denial of their application.

biometric information, but also cover the broader security arrangements and national security implications pertaining to the overall operation of such locations.

- Instances where biometrics link information across databases for national security purposes. For example, when automated querying occurs with M5 partners in the immigration context, what are the statistics and other metrics associated with national security outcomes (e.g. information that leads to a decision of inadmissibility on *IRPA* s. 34 grounds)? What about case-by-case exchanges with M5 and other partners that occur because of national security concerns? Finally, what role, if any, has biometric information played in cases where the Minister of Public Safety has denied, revoked, or cancelled a Canadian passport for reasons of national security? These examples illustrate the potential for review of national security activities *made possible by biometrics.* In such instances, the balance between privacy and security – between protecting sensitive personal information and the security objectives of the state – suggests a clear role for NSIRA in terms of reviewing lawfulness, reasonableness, and necessity.
- Other situations where biometrics collected for one purpose are subsequently used for any other program or purpose (see the discussion of dual-use in paragraphs 191-201, below).

2. The Steady-State Activities

173. **Overall, the GoC's steady-state biometric activities in the border continuum are well-supported by current legal authorities and are consistent with international practice**.

174. The IRCC and CBSA's use of biometrics in their steady-state programs is well-established and supported by detailed, statutory authority. Canada's collection and verification of fingerprints and facial photographs in the immigration context is also consistent with that of other M5 members.[252] By design, the use of fingerprints facilitates information sharing with the M5, who similarly collect fingerprints in support of their own immigration programs and to enforce domestic immigration law.[253]

175. The Canadian ePassport, similarly, adheres to standards established by the International Civil Aviation Authority (ICAO), which mandates the use of facial photographs as a biometric measurement. Globally, more than 140 countries currently use ePassports based on ICAO specifications, making the system interoperable and facilitating international travel for Canadian

[252] IRCC, "Evaluation of the Biometrics (Steady State)." [NSIRA_202002_005]

[253] CBSA, "Biometrics Collection for Immigration Purposes M5 Comparison," N.D. [NSIRA_202002_039]

passport holders. The use of facial recognition in the passport application process is consistent with ICAO guidelines and best practices on the issuance of travel documents.

176. The legislative framework for the steady-state activities provides a solid basis for the collection, use, retention and disclosure of biometrics as part of the GoC's immigration and passport programs. Nonetheless, there may be more targeted areas of concern, as articulated below.

3. Expanding Use of Biometrics over Time

177. **The use of biometrics in the border continuum has significantly expanded over the last three decades, and is likely to continue expanding in the future. The trend is driven, in part, by advancing technological capabilities and evolving challenges in identity management.**

178. Beginning with asylum claimants and deportees in 1993, the collection of biometrics now covers all non-exempt foreign nationals entering Canada and, through the passport program, all Canadian citizens who apply for a passport as well as permanent residents who apply for a Certificate of Identity and refugees who apply for a Refugee Travel Document.[254] The Biometric Expansion Project was initiated with the expressed aim of widening the scope – collection, sharing, and use – of biometrics. The M5 partners meet regularly in working groups to refine and enhance (frequently, to extend) the immigration information that is shared between them. Pilot and research projects conducted within the last several years have examined the use of facial recognition technology in airports, while others have explored the integration of mobile technology into biometric identity management in the travel continuum.

179. Undoubtedly, developments in technology drive some of this momentum. We *can* do more, so we do. Leveraging new capabilities to enhance program delivery is a legitimate objective. At the same time, however, such technological determinism cannot justify the collection of sensitive information in its own right. New biometric activities must be justified according to the necessity and proportionality of collecting and using biometrics for intended objectives.

180. Also at play is the impetus to keep pace with other jurisdictions. As countries around the world expand their biometric activities, it is natural for Canada to do the same; doing so facilitates global travel for Canadians, makes it easier for non-Canadians to travel to and through Canada, and helps Canadian officials identify possible security risks (as in M5 information-sharing). Yet keeping up with others, even Canada's close international partners, is not on its own a valid

[254] While photographs have been collected as part of passport applications for decades, it is only since 2010 that IRCC has employed its Facial Recognition Solution, turning the passport photograph into a biometric; similarly, the ePassport became standard only in 2013.

justification for the expanded collection and use of sensitive personal information. Again, each new activity must be assessed, and justified, independently.

181. **Exploiting the possibilities created by technological developments and keeping pace with other jurisdictions cannot justify the expanded use of biometrics in their own right. New biometric activities must be justified according to the necessity and proportionality of collecting and using biometrics for particular, intended objectives.**

4. Pilot Projects

182. **Pilot projects and initiatives raise more concerns than do steady-state activities, as they risk being implemented on an experimental basis, without sufficient legal analysis or policy development. These projects represent an area of continued interest for NSIRA**.

183. Pilots are vehicles of expansion: a forum for new techniques and technologies that may strain the proportional balance between the government's goals and intrusions on personal privacy. Furthermore, there tends to be less public information available to Canadians about pilot activities. In this report, we describe several such projects, though it was beyond the scope of our emphasis on current activities to determine whether any single pilot was proportionate in terms of its collection and use of biometrics.

184. Nonetheless, an illustration of the challenges and possible concerns associated with pilots is provided by the Faces-on-the-Move (FOTM) project. The pilot relied on legislative authority under sections 15-18 of the *IRPA;* yet, these provisions were drafted before facial recognition technology was contemplated. NSIRA is not satisfied that sections 15-18 of the *IRPA* provide clear authority for the collection of travellers' facial biometrics, particularly prior to – and away from – the point of formal examination. In the future, legal advice should be sought to ensure that any similar activities are well-founded in the CBSA's legislative authorities and consistent with the requirements of s.8 of the *Charter*. Attention must also be paid to the policy framework governing pilot activities to ensure the proper characterization of the affected personal information. Privacy notice statements and public signage should also ensure an appropriate degree of public transparency about the deployment of new technologies and the purposes for which they will be used.

185. **Pilot projects that entail the collection of private or personal information must receive commensurate legal and policy attention.[255] Despite the temporary or experimental nature of a**

[255] For example, the final report on FOTM notes: "The privacy and security protocols for surveillance cameras are well established for notification, viewing, use, storage and deletion. *The addition of machine aided identification may require an*

project, NSIRA expects that departments will conduct the analysis necessary to ensure that legal authority is in place to conduct the activity, and that the attendant collection, use, retention and disclosure of personal information is well-governed by policy.

5. Evolving Legal and Societal Norms

186. **The public debate surrounding legal authorities questions whether existing standards and protections are sufficient for regulating biometric activities or whether new standards and protections are required.**

187. This debate is growing, especially as relates to facial recognition technology. Biometrics are personal information, but they have particular features that may set them apart: they capture immutable personal characteristics, they allow for reliable identification at a distance, and they act as unique identifiers that can be used to discover and connect information about individuals across multiple datasets. The question is whether it is appropriate to treat biometrics as being commensurate with other personal information collected by the government in the course of its programs and activities. Are specific legal regimes necessary to create standards that appropriately reflect the potential intrusiveness and sensitivity of certain biometric data, and ought there be specific use limitations beyond those currently applicable by virtue of the *Privacy Act*?[256]

188. The Office of the Privacy Commissioner (OPC) commented on this issue in the context of its recent investigation into the RCMP's use of facial recognition via the private firm Clearview AI. "Canada's privacy laws were designed to be technology neutral", wrote the OPC, "which is positive, given the pace of technological change compared to that of legislative modernization. However, the risks of [facial recognition] technology are such that [...] specific rules may be warranted."[257] The report further noted that many jurisdictions around the world have developed privacy laws which specifically regulate biometric activities. Quebec is presently the only Canadian jurisdiction to have enacted a law that specifically addressed biometrics.[258] Other

---

extension to the current protocols." (emphasis added) Face4 Systems Inc., "Face4 Final Report For CSSP Project CSSP – 2014," p. 2. [NSIRA_202002_072, p. 2.]

[256] Office of the Privacy Commissioner, "Police Use of Facial Recognition Technology in Canada and the way forward."

[257] Office of the Privacy Commissioner, "Police Use of Facial Recognition Technology in Canada and the way forward."

[258] An Act to establish a legal framework for information technology, SQ 2001, c 32, at sections 44 and 45. Full text available at: http://legisquebec.gouv.qc.ca/en/showdoc/cs/C-1.1. See also la Commission d'accès à l'information du Québec, "Biometrics: Principles and Legal Duties of Organizations," July 2020. Accessed 8 October 2021. https://www.dataguidance.com/sites/default/files/cai_g_biometrie_principes-application_eng.pdf.

jurisdictions are calling for, or implementing, outright bans on facial recognition technologies.[259] The European Data Protection Supervisor, for example, has called for a ban on facial recognition in public spaces, arguing that such applications constitute a "deep and non-democratic intrusion into individuals' private lives."[260]

189. Civil liberty organizations have been vocal in raising concerns about biometric activities, as have academia and the media. Governments, meanwhile, can benefit from new capabilities and innovation in pursuit of program objectives, but must do so in a way that respects fundamental human rights. The tension at the core of this debate – how to achieve government objectives efficiently and effectively, while safeguarding individuals' privacy – is familiar. It is the tension manifest in national security activities more generally, as society balances individual rights against collective protection. In the present context, this evergreen dilemma is catalyzed by advancements in technology, which widen the government's toolkit while also widening the scope of possible intrusion on individual privacy, specifically the collection and use of sensitive personal data. Moving forward, the question of how biometric activities are designed, implemented, and regulated will be determined, in part, by shifting societal norms, established legal principles (including Charter considerations), and long-standing Canadian values associated with democracy and individual rights.

190. **While the border is, comparatively, a space in which greater intrusiveness is considered reasonable, the boundaries of those justifications are not limitless, and will require careful calibration. For NSIRA, as for other review bodies, evolving legal and societal norms will shape how considerations such as compliance and reasonableness ought to be applied.**

6. The Dual-Use of Biometrics

191. Dual-use refers to when biometrics collected for one purpose are subsequently used for any other program or purpose. The logic is appreciable. Biometrics constitute robust identifying information about individuals; if they are useful in one context, they are likely to be useful in another. However, this dynamic constitutes one of the main privacy concerns associated with biometrics.[261]

---

[259] See *supra* note 246.

[260] European Data Protection Supervisor, "Artificial Intelligence Act: A welcome initiative, but ban on remote biometric identification in public space is necessary," Press Release. April 23, 2021. Accessed 19 August 2021. https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en.

[261] See the contributions to Patrizio Campisi (ed.) *Security and Privacy in Biometrics* (Springer: London, 2013) for examples within the academic literature.

192. **NSIRA observed several instances of possible dual-use of biometric information in the activities examined in this report.**

193. First, photographs collected under the Passport Program are also used for facial matching purposes in NEXUS.

194. Second, fingerprints collected from foreign nationals as part of immigration applications become searchable by law enforcement in the course of criminal investigations. While the RCMP maintains separate repositories for immigration fingerprints and criminal fingerprints, both are searched when law enforcement submit fingerprints for identification purposes.

195. Third, CSIS, RCMP and CBSA can submit photographs to IRCC to have them checked against passport and travel document application photographs using facial recognition. This can occur in the context of national security or law enforcement investigations in an attempt to identify an unknown individual, to determine if a known individual has multiple identities, and/or to assist in the execution of a warrant.

196. Dual-use does not always present a compliance issue. Indeed, many such uses are well-supported in law given the "consistent use" standard in s. 8(2)(a) of the *Privacy Act,* the ability for certain institutions to request personal information under s. 8(2)(e) of the *Privacy Act,* and other sector-specific legislative provisions (see, for example, paragraphs 85, 109, and 112, which outline the authorities that govern the law enforcement uses discussed above). With respect to NEXUS, in particular, the use of passport photographs is a clear consistent use (see paragraph 140). Privacy concerns are further muted given the program's voluntary nature and individuals' prior consent.

197. **However, even where they pose demonstrable benefits, new uses of previously collected biometrics must be carefully considered to ensure their reasonableness and proportionality. In addition, all new uses must be justified and well-authorized in law.**

198. Though authorized by law, the situations in which biometrics collected in the border continuum are leveraged for purposes outside of that continuum (such as when investigative agencies use biometric information initially compiled for immigration or passport purposes) may be worthy of particular scrutiny. NSIRA may return to these cases as it contemplates future review of biometric activities.

199. **Additionally, the principle of "purpose limitation" may be a way of guarding against unjustified dual-use in the context of biometric activities.**[262]

200. Purpose limitation involves explicitly stipulating the specific purpose for which the collected biometrics will be used, with a commitment to not use them for any additional purposes in the future.[263] It is well established in UK and European jurisprudence and is more restrictive than "consistent use." While the "consistent use" principle reflects the GoC's standing commitment to limit the repurposing of personal information, the standard ought to be read as narrowly as possible for biometric information. Again, biometrics are unique compared to other personal identifiers because they are essentially permanent and immutable.[264] This means that once they are collected, if they are not subject to clear retention/deletion policies and purpose limitations, the government has a ready repository of information for identifying individuals in the future – perhaps in activities that are less benign than the activities under which the biometrics were originally collected.[265]

201. It is premature for NSIRA to make a finding on whether the possible instances of dual-use identified above are reasonable or proportionate. Future review, whether by NSIRA or another review body, may consider the question in greater depth.

---

[262] Information Commissioner's Office (UK), "Principle (b): Purpose limitation," N.D. Accessed 12 August 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/?q=DPIA.

[263] Information Commissioner's Office (UK), "Principles," N.D. Accessed 12 August 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.

[264] The European Union's *General Data Protection Regulation* (GDPR) declares biometric information a "special category of data" (article 9) given its sensitivity. (Full text available at: https://gdpr.eu/article-9-processing-special-categories-of-personal-data-prohibited/). Similar categorizations are made by the Brazilian *General Data Protection Law* (article 5) (full text available at https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf) and India's proposed *Personal Data Protection Bill* (article 3, paragraph 36) (full text available at: https://prsindia.org/files/bills_acts/bills_parliament/Personal%20Data%20Protection%20Bill,%202019.pdf).

[265] Consider for example Pakistan's National Database and Registration Authority (NADRA). Created in 2000 for the purpose of modernizing registration for identity cards, the NADRA database has subsequently been linked to SIM card registration for the purpose of combating terrorism, and to facial recognition technology through CCTV cameras in several major Pakistani cities. See Privacy International, "Identity Policies: The Clash Between Democracy and Biometrics" January 30, 2018. Accessed 19 August 2021. https://privacyinternational.org/long-read/1100/identity-policies-clash-between-democracy-and-biometrics.

7. Technical Systems

202. NSIRA reviewed high-level technical information about the activities documented in this study. This included information pertaining to the various systems and databases used in the course of the GoC's biometric activities.

203. **There is significant overlap between the technical systems and databases used across the steady-state biometric activities.**

204. Both the Passport Program and Immigration Program use the Global Case Management System (GCMS)[266], and IRCC, CBSA and RCMP have access to GCMS.[267] In the immigration context, facial photographs are stored in GCMS, while fingerprints are sent to the RCMP and stored in one (immigration) of several repositories of the Automated Fingerprint Identification System (AFIS). The immigration repository is then searchable by domestic law enforcement and can be queried by Canada's M5 partners for immigration purposes.

205. The passport and travel document applications in the Passport Program, meanwhile, are stored in both GCMS and in IRCC's Central Index (see Annex A), though IRCC has communicated that a full transition to GCMS is planned moving forward.[268] The digitized photograph from the application is sent to IRCC's FRS, converted into a biometric template, sent for evaluation in the FRS database, and stored in the CI. In both the Immigration Program and Passport Program, the intake of applications – and biometrics – employ a range of systems at different intake locations around the world, all of which connect back to IRCC servers in Canada.

206. **The overall architecture of this system – biometric collection, transmission, and storage in the course of the GoC's activities in the border continuum – is complex, though not necessarily problematic**.

207. In keeping with the foundational nature of the study, NSIRA makes these observations as a first step in mapping the relevant systems architecture. This mapping, summarized in Annex A, will support NSIRA should it choose to review in detail the various technical systems used for biometrics in the course of border activities, including how they overlap and what privacy or security issues, if any, might arise from the present structure.

---

[266] While the Passport Program primarily uses the Integrated Retrieval Information System (IRIS), IRCC indicated to NSIRA that it is "currently transitioning [from IRIS] to the [GCMS]" beginning with diplomatic and special passports, Refugee Travel Documents, and Certificates of Identity. IRCC written response to NSIRA, 4 December 2020, p. 5.

[267] The 2017 MOU Paragraph 8.4 of the Annex on Information Sharing to the 2017 IRCC-CBSA MOU.

[268] IRCC written response to NSIRA, December 4, 2020, p. 5.

8. Visibility into Algorithms

208. In addition to the public concern about governmental surveillance noted above, there is related apprehension about automated decision-making and about decision-making aided by automation, particularly when it occurs in conjunction with biometric identification.[269] The general concern with respect to algorithms and automation is that the decision-making process is opaque, even to the human operators who rely on the algorithms or systems to do their work.[270]

209. **In the Immigration Program, Passport Program, and at PIK kiosks, IRCC, CBSA, and the RCMP have limited visibility into how the algorithms used operate.**

210. The algorithms are procured from private vendors, and the details of how they work are proprietary. They are, in this sense, essentially a 'black box'. NSIRA supports greater transparency in how algorithms work when analyzing personal information. Such transparency is necessary for third-party verification of the algorithms' accuracy and reliability and would enhance public confidence in both the algorithms' ability to function fairly and without discrimination and in the departments' ability to mitigate any shortcomings in that respect.

211. **Each department and agency did, however, demonstrate that performance metrics (e.g. error rates) are known and tested, and that customizations (such as adjusting match thresholds) are applied when appropriate**.

212. Moreover, for IRCC's FRS, and for the RCMP's AFIS, human intervention occurs to either verify system results or complete matches if necessary. Facial matching at PIKs, by contrast, occurs without human adjudication, though any obvious errors may subsequently be corrected by BSOs through visual verification.

9. Preventing Bias and Discrimination

213. Related to the opacity of algorithms is the possibility that automated biometric analysis – e.g. facial recognition and fingerprint matching – may be subject to bias. It is well documented in the academic literature, for example, that many facial recognition algorithms are less reliable in identifying women, the very young and very old, and individuals with darker skin tones.[271] Similarly, fingerprint capture and matching may be more difficult and/or less accurate for

---

[269] Israel, "Facial Recognition at a Crossroads," p. 61.

[270] Israel, "Facial Recognition at a Crossroads," p. 61.

NIST, "Face Recognition Vendor Test (FRVT) Part 3," https://doi.org/10.6028/NIST.IR.8280. See also Alice O'Toole et al., "Demographic effects on estimates of automatic face recognition performance," *Image and Vision Computing.* March 2012. 30 (3): 169-176; also Nicholas Furl et al., "Face recognition algorithms and the other-race effect: Computational mechanisms for a developmental contract hypothesis," *Cognitive Science.* November-December 2002. 26 (6): 797-815.

females, particular ethnic groups, and individuals working in certain trades (which may reflect socio-economic status).[272] Given that important decisions in the border continuum – including the issuance of official travel documents, the granting of visas, asylum, and/or residency status, and possible referral for additional questioning/inspection during the immigration and customs process – are informed by automated analysis, the possibility of systematic bias is of concern.

214. **IRCC and CBSA have conducted preliminary analyses to explore how their biometric activities may impact diverse groups of people, though the implementation of possible mitigation strategies was not always apparent.**

215. For example, CBSA's GBA+ for the PIK, completed in May 2016, suggested that the agency apply gender-specific thresholds for facial matching; an October 2020 analysis on possible gender bias at PIKs made a similar recommendation. For facial recognition in both FRS (IRCC) and PIK (CBSA), recent performance testing explicitly addressed the possibility of demographic bias. This analysis noted minor imbalances in terms of gender accuracy, but emphasized that advancements over time (updated algorithms) have steadily reduced, though not eliminated, the gap.

216. **In some contexts, technological advancements have helped to reduce, but not eliminate, differential impacts.**

217. The work to comprehensively address these issues – beyond noting that small discrepancies do exist – remains to be done. CBSA noted, for example, that its "work in this area is nascent and is not yet conclusive with significant work still to be conducted."[273] This includes GBA+ on facial recognition technologies, work on the visibility of bias in data, and the development of possible policy mitigations.[274] Similarly, IRCC stated that "further demographic bias assessments will […] be conducted" following the implementation of a new algorithm in the FRS.[275]

218. This is not to suggest that efforts to mitigate possible bias have been insufficient to this point; rather, both IRCC and CBSA have demonstrated that they are aware of possible issues and committed to future work in this area. However, such efforts should not be confined to accuracy testing, and relying on improving algorithms. Solutions at the policy level should also be explored, including the implementation of previously identified mitigation strategies and the analysis of the possible consequences of biometric errors for the experience of affected individuals.

---

[272] P. Drozdowski et al., "Demographic Bias in Biometrics," See also Hicklin and Reedy, "Implications of the IDENT/IAFIS Image Quality,"

[273] CBSA written response to NSIRA, 4 February 2021, "Annex 5 - Travellers Branch (PIK & SFV)," p. 3.

[274] CBSA written response to NSIRA, 1 October 2021.

[275] IRCC written response to NSIRA, 3 August 2021, p. 4.

219. A commitment to continuing to minimize discrepancies in the algorithms' function for diverse groups, and to ensure such differences are taken into account by the human decision-making that follows biometrics screening, will continue to be important in ensuring the reasonable use of these algorithms in the future.

220. **More work remains in terms of mitigating differential impacts on segments of the population. At the same time, the departments and agencies examined in this study have demonstrated their awareness of possible systemic inequalities and their commitment to addressing them.**

8. Conclusion

221. Biometrics play a fundamental role in the border continuum. The Government of Canada uses biometrics to verify and establish identity. The question of who is coming into the country – and whether they have a right to – is more confidently answered as a result. In the immigration context, this involves the screening, verification (at arrival), and ongoing assessment of admissibility of foreign nationals coming to Canada as temporary or permanent residents. Applicants for Canadian passports (and other official travel documents) are screened to confirm eligibility to passport services and entitlement to a passport, and subsequently use their biometric, embedded in the ePassport, during the course of international travel. These two streams converge at Canadian airports, where CBSA verifies the identity of travellers using facial recognition at automated kiosks.

222. The purpose of this study was to examine and contextualize these activities. We looked back, tracing the evolution of the GoC's biometric activities in the border continuum, noting a shift from strict national security objectives to broader goals of identity management. We looked forward, to possible future biometric applications, including the adoption of Digital Identities, and even greater systematization of biometrics into the overall traveller experience.

223. Our observations are meant to inform both the Canadian public as it contemplates the government's collection and use of biometric information, and NSIRA as it plans future review of the same. We noted that the steady-state activities are well-supported by current legal authorities, and are consistent with international practice. At the same time, certain areas raise potential concern. These include pilot projects, which are vehicles for experimentation and require careful legal consideration; the ongoing possibility of systemic inequalities across diverse groups of people resulting from algorithmic biometric analysis; and the possible dual-use of biometric information, including the availability of biometric information to investigative agencies.

224. Public debate about the government's application of biometric technology will continue to evolve, driving change in the legal and regulatory frameworks associated with such activities. As such,

continued scrutiny from NSIRA is warranted, particularly in those instances where the collection and use of biometric information is justified by explicit reference to national security outcomes.

Annex A. Technical Note: Immigration and Passport Program Systems

This technical note provides details on the technical systems used in support of identity management for the Immigration Program and identity management in the issuance of Passports.

Systems Map

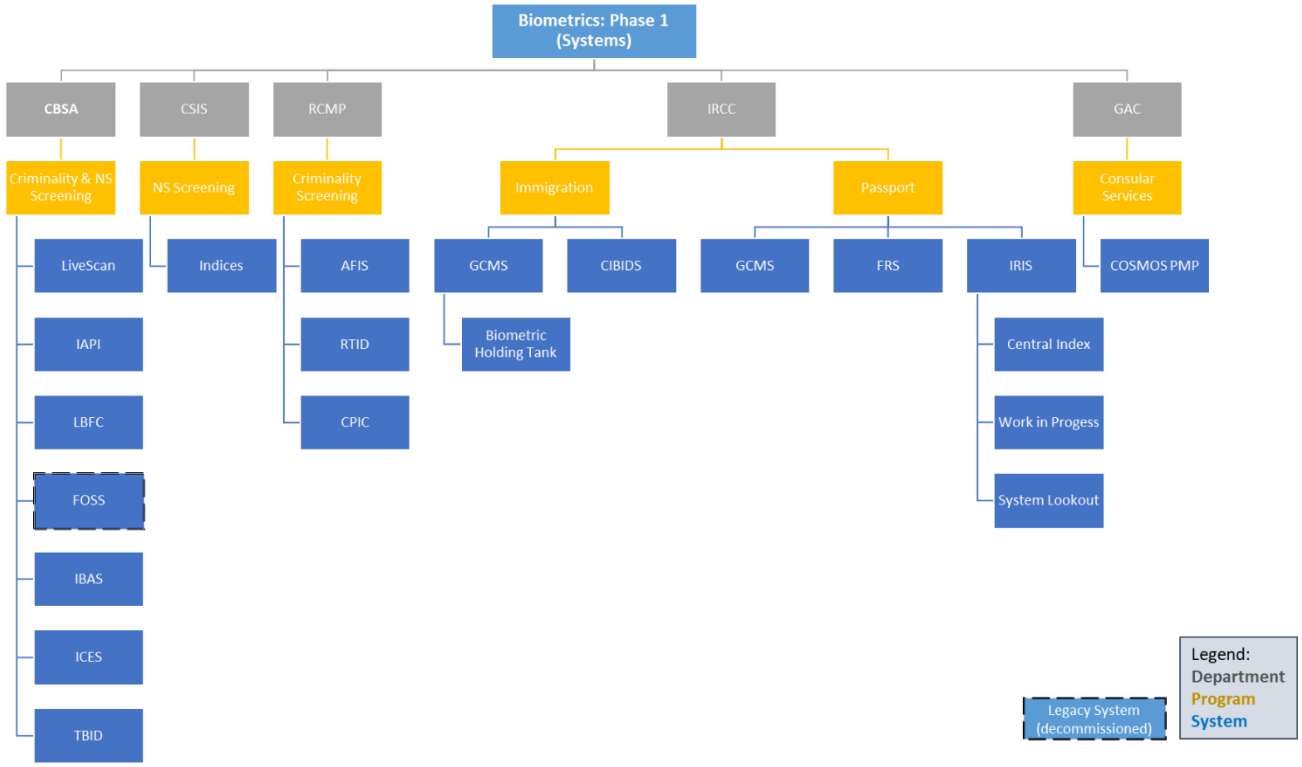

Figure 1 Systems Map: Department, Program, System

Immigration Program

Systems Inventory List and Description

Systems Inventory supporting the Immigration Program				
System Name	Owner	Accessed By	Description and Purpose	Interconnections
GCMS	IRCC	IRCC, CBSA, RCMP	Global Case Management System (GCMS)	COSMOS
AFIS	RCMP	IRCC, CBSA, RCMP	Automated Fingerprint Identification System (AFIS)	RTIDS, CPIC, NCIC
CIBIDS	IRCC	IRCC, CBSA	Canadian Immigration Biometric Identification System (CIBIDS)	
EFDC	IRCC	CBSA, ServiceCanada, VACs	Electronic Fingerprint Capture Device (EFDC)	CIBIDS
LiveScan	CBSA	CBSA	LiveScan is a device used to electronically capture and transmit fingerprints. In addition, LiveScan allows the biometric query of the US criminal databases (FBI IAFIS).The Criminal Record Check workflow can be used to confirm a NCIC result (biographic query of the US criminal system).	FBI IAFIS
IAPI	CBSA	CBSA, TC,	The Interactive Advanced Passenger Information (IAPI)	
LBFC	CBSA	CBSA	Land Border Face Capture (LBFC) Project	CIBIDS, AFIS
RTIDS	RCMP		Real Time Identification System (RTIDS)	
TBID	CBSA	CBSA	Travelers Biometric Identifier Database (TBID)	RTIDS
FOSS	CBSA	CBSA	Field Operations Support System (FOSS)	
IBAS	CBSA	CBSA	Interdiction and Border Alert System (IBAS)	CSIS, SLTD, PIK, I-SLTD

ICES	CBSA	CBSA	Integrated Customs Enforcement System (ICES)	CSIS, CPIC
US NCIC	US DHS	CBSA	United States National Criminal Information Centre (NCIC)	CPIC, CIBIDS

System Functional Descriptions

Global Case Management System (GCMS) is IRCC's integrated and worldwide web-based system used to process immigration and citizenship applications. It stores applicants' photographs and fingerprints and allows IRCC to process applications for diplomatic and special passports, refugee travel documents, and certificates of identity. In addition, GCMS is used for biometric information sharing between Canada and the M5 Partners (U.S., Australia, and New Zealand). Biometric information not associated to an individual is held in a "biometric holding tank" managed by IRCC. Biometric information may be "unassociated" due to a technical glitch or an input error.

Automated Fingerprint Identification System (AFIS) is the RCMP owned system capable of storing and comparing fingerprints. The system uses a proprietary commercial vendor algorithm.

Canadian Immigration Biometric Identification System (CIBIDS) and its Biometric Collection Solution (BCS) is the main system used for the collection and enrolment of both fingerprints and digital photographs. In addition to biometrics, the CIBIDS records biographical data as listed on the biographic data page of the applicant's passport or travel document.

Electronic Fingerprint Capture Device (EFDC) are fingerprint enrollment devices used to capture fingerprints for the CIBIDS system. These devices used in Canada (such as at Service Canada centres) and abroad in Visa Application Centres must operate in accordance with RCMP NPS-NIST-ICD 2.1.1 guidelines. Vendors who implement the systematic fingerprint verification solution used at collection points must comply with the above guideline.

LiveScan kiosk machines are used to capture digital fingerprint images, biographic information, and digital photographs from travelers. The information collected through LiveScan kiosks are electronically submitted to the RCMP through the RTIDS for traveler identification and verification. The RCMP sends back the information to the machine where a CBSA officer reviews the results. Livescan machines can enrol refugee prints into the Immigration database on behalf of IRCC and Livescan machines can request the RCMP to transmit the fingerprints to other foreign systems on a manual basis, such as the FBI.

The Interactive Advanced Passenger Information (IAPI) program, implemented in March 2016, mandated commercial air carriers to provide passenger data to CBSA prior to departure to Canada. CBSA relays back to the air carrier with "board" or "no-board" for each traveler. This project denies boarding to passengers deemed inadmissible to Canada. The system outlines specific carrier

messaging requirements, which airlines must adhere to when submitting passenger name record data.

Land Border Face Capture (LBFC) Project was piloted by CBSA and Face4 Systems Inc., to identify and evaluate technologies and methods for facial image capture through vehicle front windshields. The project's goal is to enhance land border security by means of efficient facial recognition. The LBFC Project used two camera systems and concluded that both were adequate for one-to-many identification matching in the context of land board capture.

The RCMP's Real Time Identification System (RTIDS) maintains the national repositories for criminal and immigration fingerprints. RTIDS includes the Automated Fingerprint Identification System (AFIS), a Verification subsystem, a National Police Services National Institute of Standards and Technology (NPS-NIST) NNS server and works in tandem with the Criminal Justice Information Management Service (CJIM). The NNS manages the RTIDS submissions and responses, the CJIM server manages criminal record updates, and the Verification subsystem verifies a set of fingerprints collected at Canadian border point of entry against the set obtained during the application process to confirm the individual's identity upon arrival to Canada.

Travelers Biometric Identifier Database (TBID) is used by CBSA to store RCMP fingerprint reference numbers (IIDs) along with other biometric enrollment details derived from primary inspection kiosks during traveler pre-screening.

Field Operations Support System (FOSS) Until 2014 the FOSS application was used to collect applicant biographic and biometric data in support of the processing of refugee applications. The biographic data was stored in the FOSS database while the biometric data (fingerprints) were stored in the Legacy Refugee Database at the RCMP. In 2014, the FOSS application was decommissioned and replaced by GCMS (application processing) and CIBIDS (biometric collection).

Interdiction and Border Alert System (IBAS) is an automated system used for risk assessments and data processing on biometrically enrolled travelers. IBAS is used to determine a person's admissibility by verifying other systems and databases, such as the Canadian Security Intelligence Service (CSIS) lookout or Interpol's Stolen, Lost Travel Document (SLTD) database. This system functions as a CBSA backend verification system through the Primary Inspection Kiosk (PIK) Service.

Integrated Customs Enforcement System (ICES) is, similarly to IBAS, a CBSA backend system used to determine a biometrically enrolled traveler's admissibility by using biographic data to conduct indices checks similar to IBAS and CPIC.

The United States Department of Justice **National Criminal Information Computer (NCIC)** is used by CBSA during biometric enrolment to determine if there is a biographical match for criminality screening or to determine if previous records exist within the USA, which could raise doubts about the applicant's identity.

Passport Program

The passport program uses facial recognition to help determine the entitlement of an applicant to hold a Canadian passport or travel document.

Systems Inventory List and Description

Systems Inventory supporting the Passport Program				
System Name	Owner	Accessed By	Description and Purpose	Interconnections
IRIS	IRCC	ESDC, GAC	Integrated Retrieval Information System (IRIS)	GCMS, COSMOS
FRS	IRCC	IRCC	Facial Recognition Solution (FRS)	
COSMOS	GAC	IRCC	Consular Management and Operations System (COSMOS)	IRIS
GCMS	IRCC	IRCC	Global Case Management System (GCMS)	COSMOS/PMP, Central Index

Integrated Retrieval Information System (IRIS) is used by the Passport Program to manage passport and travel document applications and to issue Passports. This activity is presently transitioning to GCMS. IRIS interfaces with the ePassport Personalization System (EPPS), which was the software used by passport printers to provide the information necessary to produce the main biographic page and write data on the electronic radio frequency identification chip (RFID). The EPPS was developed by the Canadian Bank Note Company (CBN). The IRIS system has three components:

> **Central Index (CI)**: Master index of passport records, which includes digitized images of passport application forms and supporting documentation.
> **Work in Progress (WIPs):** Databases used to process and store passport applications that are in process; data is transferred to the Central Index post-production (i.e. after passports are issued.
> **System Lookout (SL):** Database containing index biographic details (names, date of birth) on individuals whose passport entitlement may require further review or investigation under the Canadian Passport Order.

Facial Recognition Solution (FRS) is used in the administration of the passport program for new applications and renewals. It is a biometric identification technology used to authenticate identities and detect fraud. The technology converts an applicant's picture into a digital biometric template and compares it to a database of over 55 million adult applicant photos to validate their identity. The templates are stored within the FRS database.

The FRS software vendor provided Facial Recognition User Guide, outlines the procedures used to perform all tasks available in the FRS software. Before using the system or making any analysis decisions, IRCC employees must complete mandatory training offered by IRCC on Facial Comparison. IRCC's Integrity Risk Management Branch, which is responsible for the FRS, also monitors the usage, user access, system behaviours, accuracy, demographic variances, and other FRS system or user issues on an ongoing basis.

Consular Services Management and Operations System (COSMOS) is the platform used by GAC to intake travel document applications while providing consular assistance abroad. Passport applications are managed through a Passport Management Program (PMP) module, which interfaces with IRCC's IRIS to transfer case files. The module allows for passport application intake, processing and printing. Only staff that have achieved passport certification with IRCC's authorization may access PMP. Biographical information is digitized and stored in either COSMOS or IRIS.

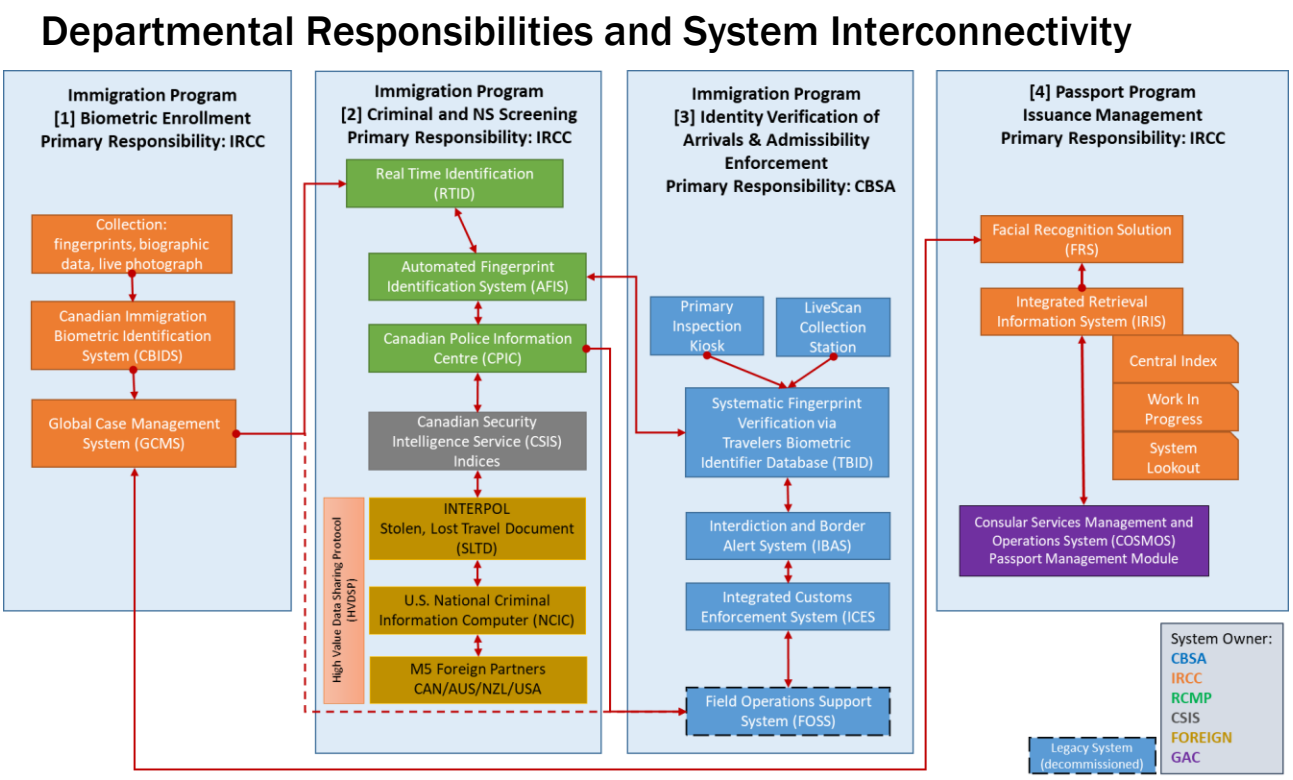

Figure 2: Departmental Responsibilities and System Interconnectivity

[1] Biometric Enrollment (IRCC)

IRCC is the primary department responsible for the biometric collection and management in support of its Immigration Program. Biometric and related biographical information [fingerprints, biographic data, live photograph] are collected at an enrollment location and securely transmitted to CIBIDS at IRCC. Once CIBIDS receives the biometric and related biographical data, the fingerprints are securely transmitted to the RCMP

RTIDS. Once the RCMP conducts automatic searches, the results are provided to IRCC into the GCMS case file. The biographic data and live photograph from CIBIDS are stored in the GCMS case. Once these checks are completed, a Visa Officer makes a final decision and if a temporary resident visa is approved, a notification is sent to CBSA to add to their operational files.

[2] Criminal and NS Screening (IRCC)
Once an applicant is enrolled, checks are conducted to inform decisions on admissibility. These checks involve several queries based on submitted fingerprints and biographic data and start with GCMS sending fingerprint checks to RTIDS which then uses AFIS for automatic fingerprint identification. This step interfaces with additional systems such as CPIC, CSIS indices as well as foreign indices checks. If flags are identified, they are sent back to GCMS for an Immigration Officer to review. If no adverse results, this is recorded in GCMS and the applicant data is submitted to CBSA FOSS to be registered for the applicant's arrival into Canada.

[3] Identity Verification of Arrivals & Admissibility Enforcement (CBSA)
When an applicant arrives at a port of entry and they present themselves through a primary inspection kiosk or a LiveScan terminal, Systemic Fingerprint Verification is conducted to confirm the identity of the person through TBID and AFIS. CBSA will conduct additional screening through IBAS, ICES and FOSS. Separately, should a temporary resident become known to law enforcement, any fingerprint enrollment in CPIC will trigger a flag sent to CBSA's FOSS system which will then send a flag to IRCC's GCMS system for potential matches of temporary residents.

[4] Passport Program Issuance Management (IRCC)
Domestic Passport and travel document applications are managed in the IRIS or GCMS systems which use the FRS system to match a facial biometric template against existing records to verify applicant identities and prevent fraud. If abroad, the COSMOS system is used to process the application and interfaces with IRIS, with the case file eventually being stored in the Central Index.