Mexican Law Review
New Series
VOLUME VII
Number 1

# LEGAL CHALLENGES OF BIOMETRIC IMMIGRATION CONTROL SYSTEMS*

Vanessa Díaz**

Abstract. *This article analyzes the deployment of biometric systems in immigration control. It argues that public policy for biometric data collection and processing must be based on legal principles and involve the participation of diverse actors, including civil society organizations, industry associations, special privacy advocates and government officials. Such deployments must also involve control mechanisms that help ensure transparency and accountability. Based on a comparative study of biometric immigration control system deployment in four countries (Australia, Mexico, New Zealand and Spain), two types of asymmetries stand out: first, notable differences in the types of information collected, stored, processed, retrieved, updated, analyzed and exchanged; Second, the purposes for which biometric systems are currently used. In the latter case, wide divergence exists in areas for which these systems are employed, such as border control strategies and the use of travel documents, revealing that each nation chooses to use these systems at different points in the immigration process. These asymmetries pose both short and long-term challenges for international cooperation.*

Key words: *Biometrics, biometric systems, border controls, ePassports.*

Resumen. *A través de un estudio comparado se analiza la implementación de sistemas biométricos como política migratoria. Resalta la importancia de incluir no sólo la participación activa de diferentes actores, tales como la industria, la sociedad civil, juristas especializados y funcionarios públicos en todas las políticas públicas de implementación de tecnología biométrica, sino también establecer criterios de transparencia y rendición de cuentas como mecanismos de control en dicho despliegue de sistemas biométricos. Revela dos tipos de asimetrías en la implementación de este tipo de tecnología en materia migratoria. Por un lado, existen diferencias entre la información recogida, almacenada, recuperada, ac-*

* This paper is based on my ongoing PhD research concerning Transborder Biometric Information Flow: Legal Challenges to Personal Privacy and the Need for Public Debate. PhD research sponsored by Consejo Nacional de Ciencia y Tecnología (CONACYT) and the Instituto de Ciencia y Tecnología del Distrito Federal.

** PhD Candidate from the Faculty of Law of the University of Tasmania (diazd@postoffice.utas.edu.au) and Researcher at the *Instituto de Investigaciones Jurídicas* of the National Autonomous University of Mexico (IIJ-UNAM).

*tualizada, analizada e intercambiada en los cuatro países analizados, lo que lleva a suponer que el despliegue de los sistemas biométricos no es homogéneo. Mientras que, por el otro, en cada uno de los países examinados los sistemas biométricos se despliegan en diferentes áreas de migración, como estrategias de control transfronterizo y documentos de viaje. Por lo que los países no están implementando esta tecnología al mismo ritmo, lo que supone el planteamiento de controversias a corto y largo plazo para la cooperación internacional.*

Palabras clave: *Biometría, sistemas biométricos, controles fronterizos, ePasaportes*.

## Table of contents



## I. Biometrics Used in Immigration Control: Information Flow

This article analyzes Transborder Biometric Information Flow[1] (TBIF) in the wider context of immigration control. Four countries, two from the Civil Law tradition (Mexico and Spain) and two from Common Law (Australia and New Zealand), are compared to help identify several noteworthy TBIF-related challenges.

This article provides insights into (a) the interaction between biometric systems deployed to enhance border control; and (b) ways in which these systems are currently used in four different countries to collect, store, process and exchange immigration-related data. It also emphasizes the lack of public debate about responsible deployment of these systems within the TBIF framework, and analyzes the diverse types of immigration data utilized by these four nations. It concludes by arguing that integration of these systems in a comprehensive legal framework requires greater transparency, accountability and supervision.

[1] The term Transborder Biometric Information Flow (TBIF) refers to the biometric data collected by governments through the deployment of biometric systems with the intention to exchange biometric information nationally or internationally.

A comparative study of TBIF in these four countries shows an absence of international biometric treaties and industry self-regulation. As a result of this vacuum, standards on the deployment of such systems have been mostly based on the efforts of two organizations —the International Civil Aviation Organization (ICAO) and the International Organization of Migration (IOM). Two other regional organizations —the European Union (EU) and the Asia Pacific Economic Cooperation (APEC)— have also played a limited role through recommendations, specs and standards for biometric border control systems.

These organizations' work and publications have focused mostly on technical issues. Although discussion of these issues is useful, there has been a notable absence of discussion regarding the extensive framework needed for responsible public debate, transparency and adequate scrutiny.[2]

The TBIF comparison set forth in this article reveals two types of asymmetries: (1) differences between the types of data collected, stored, processed, retrieved, updated, analyzed and exchanged; and (2) differences in border control strategies and biometric travel requirements. One example is Mexico's recent issue of biometric passports, which poses both short and long-term challenges for world-wide cooperation.

The deployment of biometric systems for immigration control has generally helped increase efficiency at border control checkpoints through enhanced security and innovative methods to collect and record travelers' identities. These measures also aim to stop illegal immigration, help fight cross-border crimes and prevent terrorism. However, as is discussed below, biometric systems for immigration control cannot stop illegal immigration, cross-border crimes and terrorism.

Although all these measures are commendable public policy, they do not justify a complete absence of informed public debate regarding the deployment of biometrics for immigration control.[3] This article discusses this vacuum in light of major legal, political and ethical concerns.[4]

In light of the urgent need to establish both international and domestic immigration policy, this paper covers several other notable areas: (1) the interplay between biometric border control systems; (2) ways in which the four

[2] Jasanoff has addressed this view in stating that "the pinpoint here are consequences for the day-to-day conduct of society, occur within elites, in the courts, the expert bodies that advice parliaments and presidents, and the professional classes that control much of the meaning making in advanced industrial societies. These are the groups, then, that can be observed enacting and performing some of the continuities of culture, with significant implications for convergence and divergence across national polities." Sheila Jasanoff, Designs on Nature, Science and Democracy in Europe and the United States 2 (Princeton University Press, 2007).

[3] *Id.*

[4] The legal concerns should be tested by the principle of proportionality, however is not the aim of this paper.

countries in this study currently collect, store, retrieve, analyze and handle immigrant data; (3) raise the question of how the legal frameworks established for privacy and data protection are operating effectively; and (4) the need for transparency, accountability and supervision of national and worldwide immigration controls.

## II. Transborder Biometric Information Flows: The Need for Informed Public Debate

Although the deployment of biometric border control systems has increased notably, there has been surprisingly little public discussion outside industry circles and a small cadre of public officials working in this area. Despite the fact that "popular media and official discourse are two major ways in which people acquire "knowledge" for everyday life,"[5] little about these systems —and how they impact privacy and civil liberties— has entered public discourse.[6]

The dynamics of the interaction between popular media and official discourse are the major ways for society to know about the implementation of biometric systems. The author agrees with Pedro de Vega's assertion that public opinion plays an essential role in a democratic State.[7] This is especially true given the legal, political and ethical issues involved, including important privacy and data protection rights.

Immigration policy decisions made in each of the four countries studied shows that the decision-making process has been influenced not only by domestic concerns but also international security, including illegal immigration, cross-border crime and terrorism.

Apart from this disproportionate interest in security, surprisingly few multidisciplinary official studies have been made public regarding the pros and cons on biometric surveillance systems. There is also an absence of public discussion of potential privacy right violations posed by linking centralized biometric immigration data with criminal databases and TBIF between nations and organizations. Why is public discussion of these issues so important? Be-

---

[5] *Id.*

[6] Interview with Ernesto Villanueva Villanueva and Issa Luna Pla, Researchers, Institute of Legal Research of National Autonomous University of Mexico, in Mexico City (November 23, 2011); interview with Charlotte Epstein, Professor, University of Sydney, in Sydney (October 28, 2011); interview with Katina Michael, Associate Professor, University of Wollongong (Sydney, 21 February 2012). This component of the research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011.

[7] Pedro de Vega's research has focused on public opinion: Pedro de Vega García, *El principio de publicidad parlamentaria y su proyección constitucional*, 43 Revista de Estudios Políticos 45-66 (1985); Pedro de Vega García, *Significado constitucional de la representación política*, 44 Revista de Estudios Políticos 53-74 (1985).

cause countries need to balance properly the public interests in national security with individuals' civil rights and liberties, when biometric systems are deployed and TBIF between and within jurisdictions are implemented. The first scenario involves the linkage or exchange of biometric data between the requesting country and other countries. The second is the linkage of national and regional databases with those of international organizations such as Interpol, Eurodac, the Schengen Information System and APEC.

National governments commonly deploy four different types of biometric databases for immigration control. These databases are used by border control agencies at seaports, airports and overland crossings in each of the four countries examined. Mexican and Spanish immigration agencies utilize facial image and fingerprint databases. Australian and New Zealand immigration authorities, on the other hand, prefer iris pattern and facial image databases. Each of these linkages raises major privacy concerns and deserves open public discussion in the interest of transparency and civic responsibility.[8]

Domestically, the establishment of biometric databases raise privacy legal challenges and ethical concerns about: who can access immigration data; data integrity contained in centralized databases; immigration data protection for third parties; classification of individuals upon arrival (discrimination issues); data storage restrictions; as well as subsequent use of data for crime control purposes and its impact on privacy. On an international level, privacy legal challenges are magnified because the impact on privacy and data protection affects a wider range of people compared to those listed in national databases and not all countries are fully committed with privacy rights contained in different treaties and agreements. This is particularly true given the demands posed by globalization and a significant increase in TBIF for purposes of immigration control.

People should have ownership rights to their biometric data once border protection personnel have extracted them for identification and verification purposes.[9] Another commentator feels that "in a direct democracy a simple citizen must —should— know the issues over which he decides, as well as be competent on the topics assigned to his competence."[10] Citizens should be aware that they may exercise rights of access, rectification[11] and challenges to

[8] Jasanoff, *supra* note 2.

[9] Based on one prominent critic's argument of Jasanoff. *Id.* at 27.

[10] Giovanni Sartori, Homo Videns, la sociedad teledirigida 163 (Taurus, 2004).

[11] In countries with Civil Law tradition, the Data Protection principles and obligations relies in the exercise of ARCO rights. In Mexico and Spain the control over personal data is exercised by ARCO rights set in their legislation, ARCO rights are a set of forth rights of data subjects to protect effectively their personal information and control over it. This ARCO rights are: 1) Access their Personal Data; 2) Rectify erroneous or incomplete Personal Data and processors shall have the obligation of notifying data subjects of any errors or incomplete Personal Data; 3) Cancel the use of Personal Data and 4) Objection the use of Personal Data at any time. Data Protection and Privacy Jurisdictional Comparison (Monika Kuschewsky ed., Thomson Reuters, 2012).

the processing[12] of their biometric personal data under privacy and data protection laws. In a functioning democracy, citizens must *demand* transparency and accountability, specifically regarding (a) how biometric data is handled for immigration purposes; and (b) how TBIF is exchanged by nations and organizations. This includes the right to identify the national and international entities involved in processing biometric data and cross-border exchanges.

The principle of transparency has permeated beyond the idea of mere public acts or functions of State organizations. While "transparency" extends to ideas of State authorities' obligations to carry out their actions, as a general rule, according to prescribed powers that are publicly available. "Access to personal information" ideas' extends a right to request any recorded information held by a public authority. Both are important procedures used to "control State's power" and give "democratic legitimacy" of public institutions,[13] theoretically speaking. In both cases, governments should publicly debate or provide information regarding policies issues on the implementation and deployment of biometric systems and privacy rights regarding the collection and process of personal information by biometric systems. It does not matter if those requesting information are or non-citizens. Because at the end, national legislation sets the exemptions for the procedure to request public information and personal information, where at international level it could be possible that non-citizens request the access to their personal information by privacy and data protection agreements.

This article argues on behalf of the development of a legal framework that protects civil liberties through adequate levels of privacy and data protection. This framework must also be accompanied by increased public debate, transparency and accountability about the benefits and risks of biometric system deployment and TBIF. The policy issues must be available to citizens and foreigners in a plain language while privacy and data protection rights are promoted in a cross-border co-operation and collaboration mechanism by international agreements.

## III. Personal Data: Data Collection Inconsistencies

Governments have adopted biometric systems for diverse reasons, including to reduce immigration services costs; decrease identity fraud; help restore public confidence in government; increase border processing efficiency; pre-

[12] In Mexico and Spain, individuals exercise ARCO rights, especially Cancellation and Objection. "Cancellation is individuals' right to block free of charge their personal data when it is inadequate, excessive or unnecessary or when it is stored in a period in excess of that which is established in Law whereas Objection is individuals' right to request that the processing of their personal data not be carried out." *Id.*

[13] Ernesto Villanueva, Derecho a la información 69-72 (Porrúa-Cámara de Diputados-Universidad de Guadalajara, 2006).

vent illegal immigration; reduce cross-border crime; and help prevent terrorism. This section compares the ways in which Australia, Mexico, New Zealand and Spain currently classify, collect and process immigration data. Notably, the comparison shows that these countries do not or cannot easily exchange immigration information mainly for practical reasons (*e.g.*, classification) rather than technical or legal reasons. The types of data collected by each country often differ, including *when* the data is collected in the immigration process and *how* this information is updated. In a word, the data is not *harmonized*. For example, the websites for immigration statistics published by Australia, Mexico, New Zealand and Spain all contain significant information regarding visa types and categories. This said, the four countries use differing terminology and expressions, as well as divergent classifications. Another inconsistency is the widely-varying time periods required between visas. Not only do terms and expressions diverge, many definitions set forth in each nation's immigration frameworks are inconsistent, vague and contradictory.[14]

For this reason, it is difficult if not impossible to directly compare statistical information about immigration information flow in the four countries under study. According to the Global Commission on International Migration (GCIM), it is not possible to achieve uniformity on immigration data collection as the GCIM reported to the United Nations in 2005: "that the data collection, composition, categorization, retrieval, collation and exchange reflect national legislative, administrative and policy imperatives."[15] Therefore, it is difficult to present this data in a consistent and uniform international manner.

Although the Organization for Economic Cooperation and Development (OECD) has access to robust countries databases, the OECD statistics mostly cover economic, population and labor immigration data rather than specific immigration categories.[16] The same is true of the International Organization for Migration (IOM), which lacks immigration data on a global scale.[17]

---

[14] However, it is a common factor in the four countries to exclude citizens departing with the status of military personnel and their dependents and nomads, persons without a fixed place of residence who move from one site to another, are also excluded from their migration statistics.

[15] This GCIM closed in 2005. Kathleen Newland, *The Governance of International Migration: Mechanisms, Processes and Institutions* (Policy Analysis and Research Programme of the Global Commission on International Migration, 2005) *available at* http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/policy_and_research/gcim/tp/TS8b.pdf.

[16] In its entry of international migration data, the OECD notes in material posted on its website under the headings "OECD Factbook 2010" and "Country Statistical Profiles 2010" that the sources of migration statistics in many of the countries it covers are population registries; residence or work permits; acceptances for permanent settlement; censuses; and, surveys. However, it observes that a wide variety of other data sources exists, such as border crossing counts, analyses of passenger landing cards and special surveys like labour force surveys.

[17] IOM collects and collates some regional data considered important to its operations, such as from the Commonwealth Independent States (CIS) and Statistical Information System on Migrations in Central America (SIEMCA), to obtain some of its data. IOM also sources

In 1998, the *Glossary to the UN Recommendations on Statistics of International Migration* was published.[18] The Glossary is a useful study about how countries should collect migration data and share this information for international immigration statistics —including terminology and definitions— with the aim of furthering understanding of the dynamics of international immigration, its causes and effects. In 2004, IOM published its *Glossary on Migration*.[19] Although significant, these reports fail to set mandatory standards for member countries to collect and present migration data, as they only represent non-binding recommendations.

Another problem in immigration data is the absence of universally accepted definitions. This lack of precise terminology and common standards for data collection frequently impedes meaningful data comparisons.[20] From 2008 to 2009, Australia and New Zealand adopted part of the *Glossary of the UN Recommendations on Statistics of International Migration*. Since that time Australia, Mexico, New Zealand and Spain have collected some consistent and complete series of immigration statistics based on standards established by the UN. Despite these accomplishments, definitions for short-term immigration data differ for visa categories, as well as other classification terms. These countries maintain their own databases for foreigners who enter as temporary residents. The problem lies in their current data collection systems and short-term migration categories for foreigners, as all four countries have not yet completely adopted the Glossary.

Australia maintains immigration-based databases that contain significant information, such as name, nationality, facial characteristics, iris characteristics, fingerprints, sex, address, employment, and religion. Data categorized by country of birth, age and sex are usually taken from periodic updates of data taken between censuses and death registries. The immigration data collected through periodical censuses raises concern related to reliability of data. Another example is data on immigrants' employment status, which is based on monthly labor surveys and periodic specific migrant surveys.[21] Statistics for certain immigration categories, such as country of birth, sex and address can be found since 2002.

---

data back to the OECD, Eurostat, UN Population and Statistics Division, US Census Bureau and other UN agencies known to have reliable data on the subject matter it covers.

[18] U.N. Dep't of Int'l Econ. & Soc. Affairs, U.N. Recommendations on Statistics of International Migration, U.N. Doc. ST/ESA/STAT/SER.M/58/Rev.1, U.N. Sales No. E.98.XVII.14 (1998).

[19] Glossary on Migration, International Migration Law (Richard Perruchoud ed., IOM, 2004) http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/published_docs/serial_publications/Glossary_eng.pdf.

[20] U.N. Dep't of Int'l Econ. & Soc. Affairs, U.N. Recommendations on Statistics of International Migration, *supra* note 18.

[21] *Annual Report 2011-2012 of the Department of Immigration and Citizenship*, Australia Government (Sep. 23, 2012).

As a "developed" country, Mexico has updated its electronic immigration data on a monthly basis since 2002. Since 1995, it has maintained statistics for categories.[22] This said, a comparison of Mexican and Australian visa classifications would reveal many inconsistencies. Australia, for example, classifies its visas as "temporary" or "permanent" with 140 visa subclasses. Mexico, on the other hand, classifies visas as "visitor" and "resident" with only 10 subclasses.

In New Zealand, many government agencies collect data on international immigration movements and their outcomes. The fact that diverse agencies collect and collate data often makes comparison extremely difficult. This has led to calls for the development of a cross-agency view based on a "risks and benefits" analysis performed by each respective agency. This said, historical statistics for some immigration categories is only available since 1998.

Spain maintains a mix of physical records and electronic data which is collected and updated every three months. This information is based on data collected from immigrants registered in city council neighborhood lists, required for education, academic employment as well as access to public health care. Historical immigration stats are available since 1996.[23]

The four countries under study all use biometric passports and visas. However, there are three mandatory types of biometric passport (ePassport) generations according to the International Civil Aviation Organization (ICAO):[24]

a) Biometric passports with Basic Access Control (BAC).
b) Extended Access Control (EAC).
c) Supplemental Access Control (SAC).

These biometric passports are known as Machine-Readable Travel Documents (MRTD) embedded with a secure element pursuant to specs established by the ICAO; each element contains a contactless microprocessor chip with biographical data about the passport holder (*e.g.*, name, date and country of birth); medical information; and a facial image.[25] It may also include fingerprints, iris patterns, a facial biometric image (mandatory in accordance with ICAO specifications) and other information approved by the ICAO. A contactless enabled reader is used to read this data.

---

[22] National Institute of Migration (INM), historical statistics website http://www.gobernacion.gob.mx/es_mx/SEGOB/Series_Historicas ,Mexico, The Government Secretary.

[23] National Institute for Statistics (INE), Spain, http://www.ine.es/ss/Satellite?L=0&c=INEPublicacion_C&cid=1259924959454&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout&param1=PYSDetalleGratuitas (*last visited* Nov. 27, 2013, 13:20 hrs.).

[24] The production and issue of biometric passports require different ancillary businesses such as printers, inlay manufacturers, chip makers, standardization manufacturers, high security paper manufacturers and security printer makers, among others.

[25] U.N. International Civil Aviation Organization [I.C.A.O.], Machine readable travel documents (MRTDS): History, Interoperability, and Implementation , U.N. Doc. ISO/IEC JTC1 SC17 WG3/TF1 (March 23, 2007). http://www.icao.int/Security/mrtd/Downloads/Technical%20Reports/ICAO_MRTD_History_of_Interoperability.pdf.

a) *Biometric passports with Basic Access Control (BAC)*. The BAC is a mechanism introduced to ensure that the biographic data and facial images stored on the passport microprocessor chip are read securely. Australia[26] and New Zealand[27] both collect facial and iris biometric info.
b) *Biometric passports with Extended Access Control (EAC)*. The EAC is a second-generation mechanism that restricts access to highly sensitive biometric data, including both optional and mandatory biometric characteristics. This passport is based on asymmetric cryptographic protocols and uses stronger encryption.
c) *Biometric passports with Supplemental Access Control (SAC)*. The SAC is a third-generation Password Authentication Connection Establishment (PACE) that further restricts access to highly sensitive biometric data, including optional and mandatory biometric characteristics. It implements asymmetric cryptography and bases data encryption on a key shared between the reading device and the chip. In December 2014, Spain will begin collecting facial and fingerprints in order to issue biometric passports with Supplemental Access Control (SAC).[28]

We are currently unaware of the type of access control used in Mexican biometric passports. Despite public information stating that biometric passports were first issued at the end of 2012[29] —including an electronic bar code and the holder's hologram in the center right of the document— the contactless microprocessor chip symbol does not appear on the passport's front page. The only biometric data collected in these passports are facial and fingerprints characteristics.[30]

The four countries mentioned above currently do not collect the same biometric data for passports. Data collected from Australian and New Zealand citizens include facial and iris characteristics, whereas Spain and Mexico collect only facial and fingerprints characteristics. For foreign visitors, all four countries use face recognition to verify individuals' identities and check blacklists. Verification, however, depends on the type of visa; not all visas issued are biometric.

Why do biometric border control systems deployed in these four countries differ so widely? Because the four countries differ in their approach on how to manage their borders; for Australia and New Zealand as island States, is very important to have a sustainable population. Note that apart from differences in data collection, all four countries use centralized databases and similar border control procedures. All four also check against criminal biometric databases and share common immigration control strategies.

---

[26] Australia began issuing October 2005.

[27] New Zealand began issuing September 2005.

[28] Spain began issuing biometric passport with Basic Access Control (BAC) since July 2003.

[29] Mexico began issuing November 2012.

[30] The company which won the nationwide passport project in Mexico was Suprema Inc.

## IV. Immigration Policy: International Context

Immigration occurs for many reasons: a search for better economic opportunities; the desire to join family members who have already migrated; or an escape from adverse political or social conditions. Article 13(2) of the *Universal Declaration of Human Rights* recognizes that "everyone has the right to leave any country, including his own and to return to his country."[31] The international community has declared this right as necessary to protect other human rights. The right to travel is a necessary attribute of a democratic constitutional State. Immigration and migration play important roles in the rapid, complex and violent change often present in many parts of the world. This change affects States, regions, societies, economies and policies.[32]

The international legal framework comprised of treaties, conventions, principles and agreements are balanced with States' sovereign rights to protect borders; confer nationality; admit and expel foreigners; combat trafficking and smuggling; and safeguard national and regional security. These international legal frameworks need to be balanced not only with citizens' civil rights but also with other human rights intrinsic to immigration issues,[33] including privacy and data protection rights. This international human rights framework undergird the main pillars of public policy for international immigration.

a) *Biometric Technology Deployment*. The legitimacy of biometric immigration control systems depends on their basis in law and democratic principles.[34] For this reason, elected officials in charge of authorizing and deploying these systems must be familiar with multi-faceted technical and legal issues.[35]

The implementation of biometric systems gives rise to many legal issues, especially regarding individual privacy and data protection rights. Addressing these legal concerns is critical to win political support and public acceptance.

b) *International Immigration Organizations*. Although no international treaties or conventions have been approved by the UN regarding the deployment of biometric immigration control systems, Article 13 of the *Convention on International Civil Aviation* deals with biometric technology and States.[36]

---

[31] Universal Declaration of Human Rights, G/A/RES 217A, at 13(2), U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc. A/810 (Dec. 12, 1948).

[32] Leonard B. Boudin, *The Constitutional Right to Travel*, 56 Columbia Law Review 47-75 (1956).

[33] Trafficking in humans are a particularly abusive form of migration. States resolved to take measures to ensure respect for the protection of the rights of migrants and to intensify their efforts to fight trafficking in the Millennium Declaration.

[34] Eduardo García de Enterría, La Constitución como norma y el Tribunal Constitucional 43 (Civitas, 2006).

[35] Jasanoff, *supra* note 2.

[36] "The laws and regulations of a contracting State as to the admission to or departure from its territory of passengers, crew or cargo of aircraft, such as regulations relating to en-

Two key international organizations operate in the biometric immigration area: the International Civil Aviation Organization (ICAO) for international standards, recommendations and procedures regarding immigration practices. The ICAO —in charge of biometric passports and visa specifications— has been investigating biometrics and its potential to enhance travel document identification since 1995. Not until 2001, however, did they recommend the use of facial recognition as the primary biometric.[37]

The International Organization for Migration (IOM) is another leading organization focused on immigration issues.[38] The ICAO and IOM are the two main international organizations that make recommendations and establish specifications regarding the deployment of biometric border control systems.

c) *International Civil Aviation Organization (ICAO).* This is a specialized UN agency responsible for adopting standards and recommending immigration-related practices and procedures.[39]

The *Convention on International Civil Aviation* establishes the structure of ICAO.[40] It is noteworthy that Australia, Mexico and Spain are all Council member States.[41] ICAO has developed numerous standards regarding travel documents (*e.g.*, passports and visas) and border control identification policies. A passport is not only an identity certificate; it represents the government's promise of protection when travelling in foreign countries —with the caveat that such protection may be withheld if a citizen is considered unworthy.[42]

---

try, clearance, immigration, passports, customs, and quarantine shall be complied with by or on behalf of such passengers, crew or cargo upon entrance into or departure from, or while within the territory of that State." International Civil Aviation Organization, Convention on International Civil Aviation, art. 13, Dec. 7, 1944, Doc 730019.

[37] The IOM offers "advice, research, technical cooperation and operational assistance to States, intergovernmental and non-governmental organizations and other stakeholders, in order to build national capacities and facilitate international, regional and bilateral cooperation on migration matters." U.N. International Civil Aviation Organization [I.C.A.O.], Machine Readable Travel Documents (MRTDS): History, Interoperability, and Implementation, *supra* note 25.

[38] U.N. International Organization for Migration [I.O.M.], *available at* http://www.iom.int/cms/en/sites/iom/home/about-iom-1/mission.html.

[39] International Civil Aviation Organization [I.C.A.O.], *available at* http://www.icao.int/about-icao/Pages/default.aspx. See also Daniel C. Turak, The Passport in International Law 30 (Lexington Books, 1972).

[40] The Convention on International Civil Aviation is also known as the Chicago Convention. It took place in 1944. According to the terms of the Convention, ICAO is made up of an Assembly, a Council of limited membership with various subordinate bodies and a Secretariat. The chief officers of the ICAO are the Council President and the Secretary General. *See* International Civil Aviation Organization, Convention on International Civil Aviation, art. 13, Dec. 7, 1944, Doc 730019.

[41] See member States of ICAO, *available at* http://www.icao.int/about-icao/Pages/member-states.aspx (last visited Nov. 27, 2013).

[42] The standard states that "a valid passport shall be the basic document providing public

Biometric passports issued in compliance with ICAO specifications contain biometric data with controlled access, contactless microchips[43] and a minimum 32kb data storage capacity.

For the ICAO, the only secure way to use ID documents is by means of physiological characteristics accessible in a tamper-proof way. The biometric characteristics used by the ICAO[44] in passports are: (a) facial recognition (mandatory); and (b) fingerprint or iris recognition (optional).

Due to its non-intrusive nature, the ICAO requires facial identification for biometric verification. Face photographs can be utilized by either personnel or automated systems to: (a) confirm identities via database search (*recognition*); or (b) authenticate images (*verification*).[45]

Biometric fingerprint and/or iris characteristics may also be used for recognition purposes when agencies have access to information needed for verification.

d) *International Organization for Migration (IOM)*. Created in 1951 to collaborate with governmental, intergovernmental and non-governmental partners,[46] the IOM is increasingly called upon to assist States address complex border management issues.[47]

IOM works with national governments to assess and improve the integrity of their travel and identity documents. Working with ICAO and the company IBM, IOM helps oversee an "Identity Management" program[48] that covers travel documents and related issuance systems,[49] as well as travel document inspection.[50]

As part of this Identity Management program, IOM manages a Personal Identification and Registration System (PIRS) which facilitates the collection, processing and storage of traveler information, including biometric

---

authorities with information relating to the individual passenger on arrival or departure of a ship." Turak, *supra* note 39, at 35.

[43] International Civil Aviation Organization [I.C.A.O.], *Why ICAO Selected the Face as Primary Biometric Identifier Specified to ePassports*, MRTD Report (2007).

[44] 2 International Civil Aviation Organization [I.C.A.O.], Machine Readable Travel Documents, DOC 9303 (Pt 1, 6th ed, 2006).

[45] Face photographs are used in passports, visas, driver licences or other identification documents. International Civil Aviation Organization [I.C.A.O.], *supra* note 43.

[46] http://www.iom.int/cms/about-iom.

[47] IOM's Immigration & Border Management Programs, http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/01-IOM-IBM-FACT-SHEET-IBM-Programme-general-overview.pdf (last visited Nov. 27, 2013).

[48] IOM's Identity Management, http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/06-IOM-IBM-FACT-SHEET-Identity-management.pdf (last visited Nov. 27, 2013).

[49] Such as visa application systems and language assistance, among others.

[50] OM's Identity Management, http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/06-IOM-IBM-FACT-SHEET-Identity-management.pdf (last visited Nov. 27, 2013).

data.[51] The PIRS can also be linked to Interpol's Lost Travel Documents Database via the service's I-24/7 Global Communication System.

As part of the Immigration and Border Management program, IOM operates the Immigration and Visa Support Solution project (IVSS)[52] which includes different types of support solutions.[53]

e) *Global Interoperability Challenges*. The global interoperability of biometric systems depends on uniform enrolment, data processing, personalization, issuance, storage, reading and image verification. This said, there are currently three classes of fingerprint systems: finger image-based systems, finger minutiae-based systems and finger pattern-based systems.[54] Systems for iris biometrics emerged based on the methodology of an ICAO-recognized technology vendor.[55]

These multiple fingerprint software systems are functional in the short-term, as biometric information stored on biometric passports are matched against information stored in national databases and verified on a citizen's return. In the long-term, however, this lack of uniformity may pose a challenge to global interoperability.

Longer-term challenges are posed by face, fingerprint and iris recognition systems, including:

1) Appearance, including their facial characteristic, hair style and accessories; as well as image capture conditions, such as the camera's field of view, focus and shutter speed, depth of field, background and lighting.[56] Many countries issue biometric passports under their own guidelines for producing and submitting face photographs following ICAO

---

[51] IOM's Border Management Information Systems, http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/08-IOM-IBM-FACT-SHEET-Border-Migration-Information-System-BMIS.pdf (last visited Nov. 27, 2013).

[52] IOM's Immigration and Visa Support Solutions, http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/11-IOM-IBM-FACT-SHEET-Immigration-and-Visa-Support-Solutions-IVSS.pdf (last visited Nov. 27, 2013).

[53] These types of solutions are: "1) country information; 2) logistical assistance to support visa processing; 3) skills and language testing facilitation; 4) visa application assistance; 5) travel document handling; 6) visa application centers; 7) interview facilitation; 8) self-payer health assessments; 9) DNA services; 10) biometrics enrolment; 11) document integrity and verification; 12) self-payer travel assistance; 13) web-based visa appointment scheduling and visa issuance systems; 14) border management information systems; 15) information services and 16) family tracing." IOM's Immigration and Visa Support Solutions, *supra* note 52.

[54] Early on, the systems were not interoperable and as a result, three systems are currently used for fingerprint interoperability: image data storage, minutiae data storage and pattern data storage.

[55] International Civil Aviation Organization [I.C.A.O.], *supra* note 43.

[56] Face Image Data was approved as an international standard by ISO/IECJTC1 SC37 in 2005. This standard defines a data format for digital face images to allow interoperability among face image processing systems.

requirements:[57] this occurs with Australia,[58] Mexico,[59] New Zealand[60] and Spain.[61] ICAO's illustrative guidelines for Machine Readable Travel Document (MRTD) were updated in October 2013.

2) Image quality such as resolution, contrast and brightness affect the accuracy of face and iris recognition. Other factors include subject positioning, pose and expression, lighting uniformity and, in the case of facial recognition, the use of eyeglasses or makeup. Another major consideration is the time difference between compared photographs (iris recognition is considered overly intrusive).[62] During the enrolment process, an expert can determine whether the person suffers from common medical conditions like diabetes, arteriosclerosis or hypertension. The system can produce a false acceptance, false match or false rejection for a person whose iris has already been recorded but has been diagnosed with glaucoma.[63]
3) Fingerprints can also be sometimes hard to identify. Individuals who handle chemical products, for example, often experience false rejection because fingerprint quality is degraded by exposure to chemicals. Other subjects with imprecise fingerprints include the elderly and children under the age of six.

In 2004, the Non-Government Organization (NGO) Privacy International sent an open letter to the ICAO, signed by many other NGOs from around the world about the dangers of biometric passports. In this letter, the NGOs expressed their concern regarding the negative effects of the use of biometric travel documents on privacy and civil liberties. Their biggest concern was the creation of national centralized biometric databases.[64]

---

[57] ICAO has consequently designed illustrative guidelines for portraits in a Machine Readable Travel Document (MRTD) for the next generation of electronic passports, the so-called biometric Passports. 2 International Civil Aviation Organization [I.C.A.O.], *supra* note 44.

[58] Australia general photo guidelines, https://www.passports.gov.au/images/photo_guidelines.pdf#zoom=100 (last visited Nov. 27, 2013).

[59] Mexico photo guidelines, http://www.sre.gob.mx/index.php/primera-vez/252 (last visited Nov. 27, 2013).

[60] New Zealand photo guidelines, http://www.passports.govt.nz/Passport-photos---adults (last visited Nov. 27, 2013).

[61] Spain photo guidelines, http://www.interior.gob.es/pasaporte-29/clases-y-requisitos-183?locale=es (last visited Nov. 27, 2013).

[62] ISO/IEC 19794-5:2005, Information Technology — Biometric Data Interchange Formats —Part 5: Face Image Data— AMENDMENT 1: conditions for taking photographs for face image data (2007). The International Organization for Standardization/International Electro-technical Commission (ISO/IEC) 19794-5 Biometric Data Interchange Formats defines a standard data format for digital face images to allow interoperability among face recognition systems, government agencies, and other creators and users of face images.

[63] Irma Van Der Ploeg, *Biometrics and Privacy: A Note on the Politics of Theorizing Technology*, 6 INFORMATION, COMMUNICATION & SOCIETY 85-104 (2003).

[64] "Privacy International was founded in 1990 and was the first organization to campaign

f) *Regional Organizations*. Aside from the ICAO and IOM, other major regional organizations that implement biometric systems for immigration purposes include the European Union (EU) and Asia Pacific Economic Cooperation (APEC).

Although immigration policies may never achieve uniformity on a worldwide basis (*i.e.*, too many diverging national interests), policy harmonization on a regional basis is becoming more common. In Europe, for example, the Schengen Information System (SIS) and EURODAC system[65] permits any visa issued by a member nation to be valid in any Schengen-zone country.[66] In the Asia-Pacific context, the APEC created a Business Travel Card (ABTC) that facilitates short-term entry to member countries (referred to as "economies").[67] These policies exist because member nations clearly benefit from the movement of travelers and workers through their respective territories.

Each of these regional organizations exerts influence over the interactions between the four countries examined in this paper. Australia, Mexico and New Zealand are APEC members, and interact with the EU —of which Spain is member. These interactions are significant when migration data is exchanged with these regional organizations.

g) *Introduction of Biometric Systems: Regional Organizations*. For the four countries mentioned, three main biometric systems have been identified: two in Europe and one in Asia-Pacific. These three examples are discussed below, including standards for interoperability, security and accuracy designed by ICAO.

In 2009 at the APEC Business Mobility Group, Australia submitted as part of the Proposed Business Mobility Group Goals for 2009 that: "[t]he document 'A guide to Biometric Technology in Machine Readable Travel Documents' has already been recognized as a unique and valuable document by ICAO and the ISO, and also by the IOM, which now has permission from APEC to translate the document into the other languages to assist other governments adopt e-Passports."

---

at an international level privacy issues." Gus Hosein, *Privacy International was founded in 1990 and was the first organization to campaign at an international level privacy issues,* Privacy International (30 March 2004), *available at* https://www.privacyinternational.org/blog/open-letter-to-un-agency-on-dangers-of-biometric-passport-standard.

[65] Council Regulation No. 2725/2000, Concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, 2000 O. J. (L 316) 1-10.

[66] The Schengen zone includes 26 countries: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Slovenia, Slovakia, Spain, Sweden, and Switzerland, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm (last visited Nov. 27, 2013).

[67] Asia Pacific Economic Cooperation, http://www.apec.org/About-Us/About-APEC/Business-Resources/APEC-Business-Travel-Card.aspx (last visited Nov. 27, 2013).

— *EURODAC system*:[68] In 2000, the EURODAC system was linked to the "Dublin Convention" in order to establish a centralized European database of non-European Union nationals apprehended while illegally crossing borders into EU territory. This system includes fingerprints.[69]

Each Member State has national access points and works directly with individual national administrations. If a fingerprint matches one stored in the database, the asylum seeker is redirected to the Member State where his/her fingerprints were originally collected and stored.[70]

— *Schengen Information System*[71] *(SIS II)*: Schengen member States utilize the SIS II to monitor border crossings; this includes a "list" of people who have committed an offence, are filed as "missing" or are under observation.

Member States feed the system with information through national networks which are connected to a central system and supplemented by the SIRENE network[72] made up of representatives of the national and local police, customs agencies and the judiciary.[73]

— *APEC Business Travel Card (ABTC)*: This card is used to facilitate information exchange and enhance business travel. It relays information regarding lost and stolen travel documents to the International Criminal and Police Organization (ICPO-INTERPOL) database.[74]

Each individual Member State issues the Business Travel Card in compliance with card eligibility criteria, service requirements and manufacturing standards.[75] Although the system relies on passports,

---

[68] Council Regulation No. 2725/2000, *supr*a note 65.

[69] EURODAC Automated Fingerprint Identification System (AFIS) was created by the company Steria.

[70] It is important to consider, that sometimes asylum seekers apply to different countries at the same time.

[71] Summaries of European Union Legislation, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm (last visited Nov. 27, 2013).

[72] SIRENE network is a system used by police to exchange information in compliance with the Schengen Convention for the purposes of preventing and detecting criminal offences in Schengen zone by SIS II.

[73] International Organization for Migration [I.O.M.], International Terrorism and Migration, Background Paper, Immigration and National Security 16 (June 2003). This system was reviewed after the "Prüm Convention." Summaries of European Union Legislation, *supra* note 73. The company Steria is leading the second generation of SIS II through increased collection, storage and exchange capabilities.

[74] Business Mobility Group, http://www.businessmobility.org/travel/index.asp (last visited Nov. 27, 2013).

[75] Asia Pacific Economic Cooperation [A.P.E.C.], Guiding Principles for PKI-Based Approaches to Electronic Authentication (2005), *available at* http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel/annex_d.aspx.

travelers from APEC member states do not need visas. Nonetheless, the TBIF requires clearance in advance and requesting card production. The TBIF is encrypted during transfer via a centralized database.

In sum, regional organizations have not only deployed centralized biometric systems but have also promoted TBIF for immigration control. All three regional biometric systems currently use ICAO and APEC technical security standards. The fact that these systems all rely on centralized databases, however, leaves them open to unauthorized access, hacking and other privacy risks.

## V. Immigration Policy Framework in the Four Countries Studied

This section identifies the inclusion of biometric systems in immigration policy framework. This study revealed legal problems, limitations and challenges in TBIF. In Mexico, three governmental agencies (Interior Ministry through the National Institute of Migration (INM))[76] manage arrivals, departures and settlement of migrants. The issue of passports and protection of Mexican human rights overseas is handled by the Foreign Ministry. In Spain, two government ministries[77] also manage arrivals, departures and settlement of migrants. Despite these similarities —attributed to the Civil Law tradition shared by both nations— there is one major difference: in Mexico, the Interior Ministry is responsible for the nation's internal security.[78] Among the two Common Law countries in the study, New Zealand has four authorities involved in immigration[79] whereas Australia[80] has only one. The following figure shows immigration policy in the four countries.

---

[76] National Institute of Migration of Mexico, http://www.inm.gob.mx/index.php/page/pagina_principal/en.html (last visited Nov. 28, 2013).

[77] General Minister for Migration and Immigration, http://extranjeros.mtin.es/es/Organizacion/ (last visited Nov. 28, 2013).

[78] The flow of undocumented people from Mexico, Central and South America across the northern border to the United States continues while Mexico's southern border is increasingly used by citizens from Central and South America as their way into the United States. "Some 200,000 Central Americans attempt to irregularly enter the US via Mexico's southern border. Although 70 per cent of them are detained by Mexican migration authorities and returned to their countries of origin, an estimated 60,000–70,000 eventually reach the US or remain in Mexico." International Civil Aviation Organization, Migration Initiatives Appeal 2010 (2010), *available at* http://publications.iom.int/bookstore/free/Migration_Initiatives_2010.pdf.

[79] New Zealand immigration area of responsibility, http://www.dol.govt.nz/about/responsibilities/ (last visited Nov. 28, 2013).

[80] Department of Immigration and Citizenship (DIAC), http://www.immi.gov.au/ (last visited Nov. 28, 2013).

FIGURE 1. IMMIGRATION POLICY

| | *Australia* | *Mexico* | *New Zealand* | *Spain* |
|---|---|---|---|---|
| Authority | DIAC | Ministry of Interior National, Institute of Migration (INM) and Ministry of International Affairs | Department of Labour, Department of Internal Affairs (Citizenship Brand), and Electoral Enrolment Centre and Department of Internal Affairs (Births, Deaths and Marriages) | Minister of Labour and Migration by the Secretary of Migration and Immigration |
| Legislation | Migration Act 1995 | Migration Law<br>General Population Law<br>Refugees and Complementary Protection Law | Immigration Act 2009 | The 2/2009 Organic Law<br>Royal Decree 1161/2009 |
| Reform/amendments Immigration Policy | yes | yes | No | yes |
| (collection and process of biometrics) | yes | yes | yes | yes |
| Biometric passports | yes | yes | yes | yes |
| Biometric visas | yes | yes | yes | yes |
| Other control strategies deployed | yes | yes | yes | yes |

SOURCE: Legislation of the four countries study, *Migration Act 1995* (Australia), *Migration Law*, *General Population Law*, *Refugees and Complementary Protection Law* (Mexico), *Immigration Act 2009* (New Zealand), *The 2/2009 Organic Law* and *Royal Decree 1161/2009* (Spain).

Immigration policy and the legal framework in each country also differ. Both Australia and New Zealand have just one law[81] dealing with immigra-

[81] Migration Act 1995, 1995 S.N.Z; *see also* Immigration Act 2009, 2009 S.N.Z. No. 51.

tion, whereas Mexico[82] and Spain[83] rely on several pieces of legislation. Australia, Mexico and Spain have recently been active in modifying or reforming their immigration frameworks.

All four countries have actively developed policies that govern the collection and processing of biometric information. Although all four nations issue biometric passports, implementation varies. As a member of the EU, Spain follows EU regulations, whereas Australia and New Zealand —as members of the Five Nations Passport Group— adhere to the common consensus on biometric passports technology.[84] Only Mexico is unilaterally responsible for its internal border control strategies.[85]

In regard to biometric info collected for visas, these four countries differ not only in terms of visa categories but also which nations they deem eligible for visas. Despite these differences, however, all four share common criteria for biometric data collection for refugees. Figure 2 illustrates the asymmetries of visa categories.

---

[82] Ley de Migración [L.M.] [Migration Law], *as amended*, Diario Oficial de la Federación [D.O.], 25 de Mayo de 2011 (Mex.); Ley General de Población [L.G.P.] [General Population Law], *as amended*, Diario Oficial de la Federación [D.O.], 7 de Enero de 1974 (Mex.) and Ley sobre Refugiados y Protección Complementaria [L.R.P.C.] [Refugees and Complementary Protection Law], *as amended*, Diario Oficial de la Federación [D.O.], 27 de Enero de 2011 (Mex.).

[83] Organic Law 2/2009 amending Organic Law 4/200 on the Rights and Liberties for Foreigners in Spain and their Social Integration (B.O.E. 2009, 19949); Royal Decree on the Entry, Free Movement and Residence in Spain of Citizens of the Member States of the European Union and Other States Party to the Agreement on the European Economic Area (B.O.E. 2007, 4184).

[84] The Five Nations Passport Conference is a forum between the passport issuing authorities in Australia, Canada, New Zealand, the United Kingdom and the United States to "share best practices and discuss innovations related to the development of passport policies, products and practices." *Annual Report 2010-2011 of the Department of Immigration and Citizenship*, Australia Government (Oct. 14, 2011).

[85] A programme called the Security and Prosperity Partnership (SPP) was adopted by Mexico, Canada and the United States. Its spheres of action involved the movement of people and it discussed a number of issues not covered by the North American Trade Agreement (NAFTA), like border security and antiterrorism measures, energy sector integration, environmental protection, emergency preparedness and safety standards, among others. The principle of shared responsibility for immigration among sending and receiving countries was at the heart of ongoing reflection in Mexico. However, in 2009, the SPP was abandoned by the U.S. government and NAFTA was renegotiated. At the same time, the U.S. government implemented the Global Online Enrolment System (GOES). This includes the FAST Driver Programme between the United States and Canada or the United States and Mexico. FAST is the trusted traveller programme for commercial truck drivers along Canadian and Mexican land borders. FAST allows for the expedited release of approved commercial truck drivers making fully-qualified FAST trips between the United States and either Canada or Mexico.

FIGURE 2. FOUR COUNTRIES TYPE OF VISA

| *Types of visa* | *Australia* | *Mexico* | *New Zealand* | *Spain* |
|---|---|---|---|---|
| Permanent | 6 | 3 | 2 | 2 |
| Temporary | 6 | 7 | 4 | 7 |

SOURCE: Legislation of the four countries study, *Migration Act 1995* (Australia), *Migration Law*, *General Population Law*, *Refugees and Complementary Protection Law* (Mexico), *Immigration Act 2009* (New Zealand), *The 2/2009 Organic Law* and *Royal Decree 1161/2009* (Spain).

Given these asymmetries, it is difficult if not impossible to make a direct comparison between the visa category terms used by the four countries. Despite being Civil Law countries —as mentioned above— Mexico and Spain do not use the same terminology. Mexico employs "visitors and residents" whereas Spain utilizes "stays (estancias) and residence." Australia and New Zealand also differ; the former uses "permanent and temporary" while New Zealand employs "residence class and temporary entry class."

The differences in visa categories and subcategories used by each nation is astonishing. Australia uses six permanent visa categories and six temporary visa categories, with both categories broken into approximately 140 subclasses —each with their own eligibility criteria. New Zealand's residence class visa has two subcategories, while its temporary entry class visa has four subcategories (both subcategories have additional eligibility criteria). In Mexico, there are seven types of visitor visas and three types of resident visas. Spain uses seven types of visitor visas (*estancia*) and two types of residence visas.[86]

Despite the above, all four nations use common, though not uniform, standards for biometric border control.

1) *The Implementation of Biometrics in Immigration as Policy.* This section point out the inclusion of biometrics in the four countries' immigration policy.

In general, biometric immigration control systems are used to monitor incoming visitors and their movement information before their arrivals, departures and settlement of migrants. Biometric systems provide identification and verification by matching TBIF.[87] The following figure shows the biometric systems implemented by each nation:

[86] Minister of Immigration, New Zealand Government, Immigration Act Review (April 2006); *Annual Report 2008-2009 of the Department of Immigration and Citizenship*, Australia Government (Oct. 16, 2009); Ley de Migración [L.M.] [Migration Law], *as amended*, Diario Oficial de la Federación [D.O.], 25 de Mayo de 2011 (Mex.); Organic Law 2/2009 amending Organic Law 4/200 on the Rights and Liberties for Foreigners in Spain and their Social Integration (B.O.E. 2009, 19949).

[87] *Annual Report 2010-2011 of the Department of Immigration and Citizenship*, Australia Government (Oct. 14, 2011); Acuerdo por el que se expide el Manual de Criterios y Trámites Migratorios del Instituto Nacional de Migración [Criteria and Migratory Proceedings Manual of the National Institute of Migration of the Minister of Interior of 21 September 2010], Diario Oficial de la Federación [D.O.], 29 de Enero 2010 (Mex.); New IT System for Immigration

FIGURE 3. BIOMETRIC SYSTEMS IN THE FOUR COUNTRIES STUDY

| Countries | Information and Biometric ID Systems |
|---|---|
| Australia | SmartGates<br>Business Travel Card (APEC)<br>Movement Alert List (MAL) |
| Mexico | Foreigners and Refugees List<br>Business Travel Card (APEC)<br>Consular Management Integrated System (ACIS)<br>Integrated Migration Operations (SIOM) |
| New Zealand | SmartGates<br>Business Travel Card (APEC)<br>Movement Alert List (MAL) |
| Spain | Eurodec<br>Schengen List<br>Visa Information System (VIS) |

SOURCE: Legislation of the four countries study, *Migration Act 1995* (Australia), *Migration Law*, *General Population Law*, *Refugees and Complementary Protection Law* (Mexico), *Immigration Act 2009* (New Zealand), *The 2/2009 Organic Law* and *Royal Decree 1161/2009* (Spain).

In sum, Australia's system permits cross-checking among diverse databases, including those for Immigration, Passports, Tax and Social Services departments. Provisions in Australia's migration legislation authorize information sharing among agencies. Mexico's electronic system allows cross-checking of registered foreigners and refugees who hold valid visas and wish to change their status inside the country. Mexican legislation also contains provisions for APEC Business Travel Card data exchange. New Zealand's immigration legislation authorizes the collection, storage and use of specific biometric information[88] for verification purposes. It also contains provisions which permit the sharing of personal information —including biometric data— with national and international agencies. Foreign national's personal data may also be shared with other New Zealand agencies to check their eligibility for publicly-funded services. Spain uses the EURODAC, Schengen System (SIS II) and Visa Information System (VIS).

2) *Current Biometric Systems and Passports.* This section describes the current biometric border control systems deployed in the four countries under study. It provides the actual collection, storage and TBIF during the border control process.

New Zealand http://www.immigration.govt.nz/migrant/general/generalinformation/newitsystems (last visited Nov. 28, 2013); Organisation for Economic Co-operation and Development [O.E.C.D.], *Recent Changes in Migration Movements and Policies: Country Notes* (2010); see also INTERNATIONAL ORGANIZATION FOR MIGRATION [I.O.M.], MIGRATION INITIATIVES APPEAL 2010 (2010).

[88] Fingerprints, iris and facial characteristics.

The biometric border control systems currently deployed reveals a dynamic interaction between governments, citizens and the biometric industry. For instance, the enormous information flow required by travelers of Australia and New Zealand have forced both countries to collaborate closely and utilize a fast track process called SmartGate.[89] Australia and New Zealand have also introduced an online immigration system for visa applications. The Australian version is called the Visa Entitlement Verification Online System;[90] whereas in New Zealand it is called the Immigration Global Management System.[91]

In contrast, Spain employs three regional systems: EURODAC, Schengen System (SIS II) and Visa Information System (VIS). The first two are discussed above; the VIS is a centralized biometric database of national systems that facilitates access by Schengen Member States.[92]

Mexico currently employs three biometric databases for: (a) refugees; (b) foreign visa holders who wish to change their immigration status; and (c) temporary and/or definitive APEC Business Travel Card holders. These biometric databases are operated by the National Institute of Migration (INM) and interconnected with the Consular Management Integrated System (ACIS) verifying migration real-time alerts at the time issuing visas the Electronic System for Migration Procedures (SETRAM).[93] The overall system is known as the Integrated Migration Operations (SIOM).[94]

---

[89] This programme is a kiosk that checks whether Australian and New Zealand travellers are eligible for self-processing and the gate performs the identity check and clearance using Australian and New Zealand biometric passports with Basic Access Control (BAC). SmartGate is available at Sydney, Adelaide, Brisbane, Cairns, Melbourne, Perth, Gold Coast and Darwin international airports. In New Zealand, the SmartGate was implemented at Auckland International Airport in 2009 for arriving passengers from Australia and New Zealand. It is also operational for departing passengers from Australia and New Zealand at the Auckland, Wellington and Christchurch international airports. Australian Customs and Border Protection Service, SmartGate, http://www.customs.gov.au/site/page5552.asp (last visited Nov. 28, 2013); Customs Service website, http://www.customs.govt.nz/features/bordersector/transtasmantravel/Pages/default.aspx (last visited Nov. 28, 2013).

[90] Australia, Visa Entitlement Verification Online System, http://www.immi.gov.au/Services/Pages/immiaccount.aspx (last visited Nov. 28, 2013).

[91] New IT System for Immigration New Zealand, http://www.immigration.govt.nz/migrant/general/generalinformation/newitsystems/ (last visited Nov. 28, 2013).

[92] Each visa application contains 10 fingerprints and a digital photo. Schengen Member States and Visa Information System, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm (last visited Nov. 28, 2013).

[93] *Action Lines in Sector Programs Accountability, Transparency and Fighting Corruption Committed in 2009. Final Report*, National Institute of Migration, Mexican Government (2008-2012), *available at* http://www.inm.gob.mx/static/transparencia/PND/Formatos_A_y_B.pdf.

[94] The INM also launched the interconnection of the Integrated Migration Operations ("SIOM") with the INM's Electronic Immigration Procedures ("SETRAM"), the Consular Management Integrated System ("ACIS") of the Ministry of Foreign Affairs ("SRE"). This interconnection allows Mexican consulates to automatically verify migration real-time alerts

Biometric passports are a major component of biometric immigration systems, must generally be submitted by travelers to a border control officer. The border control officer will scanned the data page of the biometric passport and checked security features through the border control system while the border control officer makes some questions to the traveler. The border control system with facial recognition program reads the contactless chip from the biometric passport and checks data authenticity.

Then, the border control officer takes a photograph (face biometric verification)[95] and the border control systems validates the photograph taken in that moment with the photograph template stored in the biometric passport and the program runs a facial biometric verification through checking national blacklists and Interpol's databases.[96] This final step, the checking national and international blacklists, is a subsequent aggregated use of immigration information that may pose some challenges, such as false identification of a traveler.

Based on our analysis, information collected by the border control system is stored automatically in their national immigration databases. Each data point collected has a specific purpose.[97] We found that biometric passports and visas, have been used as identity-based filters and *not* to strengthen border control. The immigration information has a subsequent aggregated use within integrated data systems for cross-checking within a number of national agencies and international databases for national security and defense.[98] This subsequent aggregated use shall be voluntary or inform to the

---

at visa-issue time in order to assess the issuance of the type of visa requested. The INM also informs the SRE of the permits granted to foreigners to obtain their visas at the corresponding consulates. Instituto Nacional de Migración, "Consolida INM simplificación de trámites migratorios" (Press Release, 7 September 2011), http://www.inm.gob.mx/index.php/blog/show/Consolida-INM-simplificaci%C3%B3n-de-tr%C3%A1mites-migratorios.html (last visited Nov. 29, 2013).

[95] Sometimes fingerprints are also requested.

[96] Interview with David Philp, General Manager-Passport, Department of Internal Affairs, in Wellington (Oct. 25 2011); interview with Francisco Villanueva Díez, Deputy General Director of Information Systems and Communications for Security Matters, Spanish Minister of Interior, in Madrid (Nov. 8 2011); interview with Alejandro del Conde, Secretary of Data Protection, Federal Access Information and Data Protection Institute, in Mexico City (Nov. 16 2011); interview with Jeremy Johnson, Director National Biometric and Child Protection Services, CrimTrac Agency, in Canberra (Oct. 18 2011); interview with Alex Webling, Policy Director, Biometrics and Identity, Attorney General's Department, in Canberra (Oct. 20 2011). This component of the research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011.

[97] Pursuant to the Data Protection Principles theory, "the collection of information is necessary for a specific purpose." Data Protection and Privacy Jurisdictional Comparison, *supra* note 11.

[98] The subsequent aggregated use is prohibit in Data Protection Principles where "the personal information collected shall not be used for a purpose other than that for which it was collected." *Id.*

traveler the process of cross-checking personal information. In Australia and New Zealand, the TBIF for immigration control is generally realized by data exchange requests to specific agencies; in contrast, both Spain and Mexico employ systematic data sharing. As these procedures affect travelers' privacy and data protection rights, they should be properly reassessed and balanced based on law.

Why? Because too little public debate has focused on (a) the risks of centralized biometric databases for immigration purposes; or (b) the ways in which this information is used (*e.g.*, shared or exchanged) in relation to international criminal databases. This absence of public scrutiny, along with a lack of statistics regarding access, transparency about the difficulties encountered in biometric information processing and the way TBIF is implemented by countries raise several legal concerns. These issues relate not only to civil liberties, related to privacy and issues of intrusiveness, disclosure, purpose, misuse and consent, among others. It should be noted that there is, for example, asymmetry in the exercise of the right to access to personal information because this affects personal data protection nationally and internationally. The data protection legal framework in the four countries examined establish specific procedures for the right to access personal information, however, internationally these procedures are different.[99] These data protection legal framework also establishes restrictions regarding national security issues and these restrictions prevent Data Protection Commissioners from being able to properly monitor and supervise these databases.

Nationally, two scenarios surface with the exercise of the right to access to personal information: (1) certain data protection regimes set a direct procedure to be followed by national agencies when requesting access to personal information. In this case, citizens exercise their right by making their requests directly to the authority or agency; (2) data protection regimes set an indirect procedure for requests through a privacy commissioner, an ombudsman or a specific body. This situation means that citizens cannot directly access their information because the request is presented to the privacy commissioner, who then proceeds to request the information from the corresponding agency on the citizen's behalf.

c) *Commonly-Deployed International Immigration Control Strategies*. Deployment of biometric systems and TBIF for immigration purposes worldwide has intensified. Internationally, the implementation of biometric systems in immigration policies was marked by combined international cooperation and the facilitation of cross-border information.

There are three major areas in which these countries revealed biometric control strategies "as a trade-off for faster immigration processing, passengers will have to accept a system which has the potential to generate a vast

[99] International organisations set their own procedure or rules to access personal information.

amount of international traffic in their personal data."[100] These three common areas are:

— Transborder information flow, which includes passenger pre-inspection at departing country and advance passenger information before arrival.[101]
— Civil Aviation Security, which includes Immigration Liaison Officers (ILOs) working together with national and international law enforcement agencies to prevent irregular migration and help close down criminal operations;[102] and Airline Liaison Officers (ALOs) who are immigration inspection officers working together with airline staff to prevent individuals from traveling with fraudulent documents.[103]
— Carrier Sanctions within Civil Aviation Law. This national legislation aims to make carriers co-liable for transporting improperly documented travelers with fake biometric passports or without visas.[104] In Australia and New Zealand these sanctions form an integral part of pre-boarding activities for international flights.[105]

With their long sea borders, proximity to one other and relative distance from the rest of the world, Australia and New Zealand have implemented more extensive offshore clearance processes than both Mexico and Spain. In sum, each nation adopts the policies, structures and laws best suited to its own circumstances and needs.

## VI. Conclusions

This article explored TBIF in the context of immigration mainly because immigration represents an extensive and growing area within TBIF. The pa-

[100] S. Davies, *The Brave New World of Biometric Identification*, 2 Privacy Law and Policy Reporter 30 (1995).

[101] Involves an agreement between countries, as well as between airlines and governments, permitting passenger manifests to be sent by the airlines ahead of flights to the immigration authorities of the country of destination for pre-checking before arrival. International Organization for Migration [I.O.M.], *supra* note 73, at 16.

[102] *Id.*; Civil Aviation Legislation (Mutual recognition with New Zealand) Act 2006, 2006 S.N.Z No. 102; Ley de Aviación Civil [L.A.C.] [Federal Civil Aviation Law], *as amended*, Diario Oficial de la Federación [D.O.F.] 12 de Mayo de 1996 (Mex.); Civil Aviation Act 1990, 1990 S.N.Z. No. 104. The most recent version of New Zealand Act excludes amendments that are not yet in force from 1992, 2007 and 2013. Law 21/2003 of security aviation (B.O.E. 2003, 13616).

[103] *Id.*

[104] *Id.*

[105] Australia and New Zealand link visa issuance abroad with entry clearance at the port of entry and departure, monitoring at the port of exit. International Organization for Migration [I.O.M.], *supra* note 73, at 16.

per considered short and long term challenges related to TBIF among the four countries examined and their interaction with international organizations. This debate should not be confined to the technical aspects of the types of data collected and processed in Australia, Mexico, New Zealand and Spain. Any credible discussion must involve ways to increase public engagement, transparency and scrutiny of the deployment of biometric immigration control systems.

The absence of debate regarding current deployment of biometric databases is exacerbated by a lack of international laws and regulations. Organization such as ICAO and IOM —as well as regional organizations such as APEC and EU— have taken the lead in establishing specifications and recommendations for the use of biometric info in travel documents and immigration control systems. Although these organizations have made considerable efforts to create a framework for the deployment of biometric systems and TBIF, widespread success requires the active participation of many diverse sectors, including government, industry and civil society. This is turn necessitates (a) an inclusive strategy to increase public debate about technical (security) risks and limitations on civil liberties; (b) promotion of privacy and data protection rights; and (c) transparency and accountability regarding the management of these databases.

Although the field of biometrics is not new, the automated systems that facilitate the collection and processing of huge volumes of immigration-related information *is*. The proliferation of these systems formed the basis for our four-nation comparative study, which revealed asymmetries and convergences within TBIF in immigration context. All four countries issue biometric passports and employ biometric systems to issue visas; in each nation, electronic Border Control Systems are operated by border control officers. Given these realities, many questions arise, including the efficacy of biometric border control processes; transparency about who can access immigration information; the reliability of immigration information (data integrity); clarification about the risks of data protection in third countries; assessment of potential misclassifications of individuals' data as a result of exchange of information; data storage restrictions; and subsequent use of immigration data through dissimilar system interoperability at both national and international levels. Finally, and in legal terms the most critical area, how TBIF affects individual privacy and data protection rights.

The current interactions of TBIF in the context of immigration information flow requires a common and harmonized framework with specific rules governing the subsequent use of biometric data, cross-border rights and cross-border challenges. In addition, each country should have the capability of addressing these legal challenges by balancing public interests (*e.g.*, national security and defense) with individual privacy and data protection rights. A strengthened common legal privacy and data protection framework is needed to protect individual rights, as well as to facilitate the TBIF in immigration.

The amount of biometric information collected, stored, retrieved and exchanged will progressively increase. Therefore, TBIF must be seen as an increasingly important part of a sensitive legal privacy or data protection regime that requires a high level response in national legal frameworks. Legislators and policy makers must establish specific rules for governing TBIF. Revised legal frameworks should be publicly available and written in a way that all citizens can understand the implications not only of the deployment of biometric systems, but also, of their right to access their own information, the subsequent use of their biometric information, updates made to their personal information and, critically, about transborder exchanges.