Biometric Data Retention for Passport Applicants and Holders

March 2014
The following table compares the regulation of biometric data obtained in connection with passport applications and the preservation of such data in fifteen selected countries.

<table>
<thead>
<tr>
<th>Country</th>
<th>Availability of Biometric Database</th>
<th>Purpose of Database</th>
<th>Access to Data</th>
<th>Duration of Data Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Argentina</strong></td>
<td>Biometric data collected includes fingerprints and photographs.¹</td>
<td>Criminal investigation; national security²</td>
<td>Federal Police, Border Patrol, Coast Guard, Airport Security Police, National Registry of Individuals, and National Directorate of Migration³</td>
<td>Decree 1766/2011 creating SIBIOS does not include a time limitation for data storage. However, the Law on Personal Data Protection states that data must be destroyed when no longer need for the purpose for which it was collected.⁴</td>
</tr>
<tr>
<td><strong>Australia</strong></td>
<td>The Australian Passport Database stores information about passport applicants, including digitized photographs. Digitized</td>
<td>Passport applicant photographs are compared to images from any previously held Australian travel document. This includes digitally matching</td>
<td>Information held in the Australian Passport Database, including photographs,⁵ may only be disclosed to “a person specified in a Minister’s</td>
<td>Relevant legislation does not specify timeframes for data storage but passport applicants’ personal information is subject to the Australian Privacy</td>
</tr>
<tr>
<td>Country</td>
<td>Description</td>
<td>Purpose</td>
<td>Entity Accessing Information</td>
<td>Date of Deletion</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>---------</td>
<td>-------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Brazil</td>
<td>The Brazilian passport database (Sistema Nacional de Passaporte, SINPA) includes personal data and biometric information (facial image and two fingerprints) of passport holders, which is also found in a chip that has been inserted in the passport’s cover page since 2010.</td>
<td>Processing of passports and record keeping</td>
<td>Federal Police, and possibly other official institutions that may enter into an agreement with the Federal Police</td>
<td>Deletion date unspecified</td>
</tr>
<tr>
<td>Canada</td>
<td>Canada maintains a facial recognition database that uses biometric data to match the photo submitted</td>
<td>The purpose of the facial recognition database is to match the photo submitted</td>
<td>Data from the facial Recognition Database is accessed and used by</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Biometric Data Retention for Passport Applicants and Holders</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric data may be used by passport applicants against facial biometric information held in the Passport Database.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Office of the Privacy Commissioner (OPC) is working with the Passport Office to “avoid the development of centralized databases containing biometric information.”</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passport Canada. No policy or legislative framework was identified regarding “use, disclosure, retention, [or] disposal of biometric identifiers” in accordance with privacy protections under the <em>Canadian Charter of Rights and Freedoms</em> and the <em>Privacy Act</em>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>France</strong></th>
<th>Biometric and civil status data related to passport applications is kept in a national database called TES.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The principal purpose of the TES database appears to be the processing of passport applications, deliverances and renewals, and the prevention of passport falsification.</td>
</tr>
<tr>
<td></td>
<td>The ETS database may be accessed by authorized government personnel for the purpose of processing passport applications and issuing passports. Law enforcement personnel assigned with verifying the authenticity of passports and the identity of passport-holders may access the data stored on the microchip of individual passports. Specially authorized law enforcement and intelligence personnel may access the national TES database for antiterrorism purposes.</td>
</tr>
<tr>
<td></td>
<td>Fifteen years for information related to the passport of an adult, ten years for information related to the passport of a minor, and ten years for information related to a service or mission passport.</td>
</tr>
<tr>
<td>Country</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Germany</td>
<td>The German Passport Act states that Germany will not have a federal database of biometric passport data. According to the same Act, the Passport Register contains photographs and relevant personal data of passport holders and nothing else. Fingerprints may not be stored after a passport is issued.</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Hong Kong does not appear to have any legislation specifically regulating such a database. Hong Kong started issuing electronic biometric passports in 2007. The Passports Ordinance was not changed for that purpose.</td>
</tr>
<tr>
<td>Israel</td>
<td>On a trial basis: Biometric identification data of facial characteristics and of Identification and verification of ID and travel documents.</td>
</tr>
</tbody>
</table>
Biometric Data Retention for Passport Applicants and Holders

<table>
<thead>
<tr>
<th>Country</th>
<th>Description</th>
<th>Purpose</th>
<th>Access Regulations</th>
<th>Time Limit</th>
</tr>
</thead>
</table>
| Japan       | Japan has a database that stores application forms for passports, which include applicants’ photos. There is no separate database to store the biometric data of all passport applicants.  

| South Korea | The Ministry of Foreign Affairs has a database on names, dates of births, and fingerprints.  

|                                             | Management in the Ministry of Interior (MOI). Data will be accessible by authorized MOI employees for purposes of issuing ID documents; and by policemen, prison wardens, authorized employees of the Defense Authority, soldiers, the security personnel of the Knesset (Parliament) and other public bodies, guards employed by the agency for the protection of witnesses, and other employees of public bodies responsible for verification of identification by law.  

|                                             | examine its impact on volunteers and the utility of maintaining and using the biometric databank. Biometric data used to verify authenticity of an individual passport or identity of its holder must be erased after this examination is concluded.  

|                                             | The principal purpose of the database is to process passport applications, prevent double issuance, and find false applications.  

|                                             | Access is regulated by the general personal information protection law.  

<p>|                                             | The period of keeping and management of fingerprints cannot exceed |</p>
<table>
<thead>
<tr>
<th>Country</th>
<th>Biometric Data Retention</th>
<th>Storage Time</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mexico</td>
<td>photos, fingerprints, addresses, passport issuance records, etc., of passport holders. There is no separate database to store passport applicants’ biometric data.</td>
<td>three months. Storage time for other personal information is not specified.</td>
<td>N/A</td>
</tr>
<tr>
<td>New Zealand</td>
<td>The website of Mexico’s Department of Foreign Relations (DFR) indicates that biometric data (fingerprints and photograph) are collected from passport applicants. Mexico’s Passport Regulation and a website maintained by the DFR briefly mention a passport database but do not provide details.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Since 1998, electronic passport application files, including photographs, have been stored in a secure database. Since 2005, biometric photographic information has been stored in chips embedded in ePassports. In addition to other information-matching processes using the passport database and with other agencies, facial recognition technology is used to compare an applicant’s photograph with those held in the passport office may disclose passport information, including photographs, to “any appropriate agency, body, or person to aid border security, facilitate the processing of passengers, verify the identity of a</td>
<td>The Privacy Act 1993 applies to information held in the passport database. This includes a requirement that an agency that holds personal information “not keep that information for longer than is required for the purposes</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Biometric Data Retention for Passport Applicants and Holders</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Sweden** | Sweden does not have a database that stores the biometric data of passport applicants or holders. All biometric data deriving from passport application documents, including analysis of facial characteristics, are stored with the Passmyndigheten (Passport Agency, part of Police) at the time of application and are destroyed immediately when the finalized passport is presented to the applicant or when the passport application has been revoked or rejected.  

The purpose of collecting biometric information is “to check if the bearer of the passport is the correct person, not to create a photo or biometric registry over travelers.”

However, upon filing, a copy of the application and a photograph, without biometric analysis of facial characteristics, are sent to Rikspolisstyrelsen (Swedish National Police Board).  

The Swedish National Police Board in turn is required to keep a central record of the passports.  

Biometric information is not kept.  

No upper time limit for the copy of the passport application and photograph. The passport registry is covered by secrecy laws and the application and photograph are kept in secret for seventy years. Thereafter, the photographs become public. |
| **database in order to prevent fraud.** | holder of a travel document, or determine whether a person is a New Zealand citizen.”  

Formal written agreements with requesting organizations must be entered into by the passport office.  

for which the information may lawfully be used.”  

The Passports Act 1992 also specifies that when the holder of a New Zealand passport dies, cancelation of the passport “may be effected by cancelling the electronic record of that document stored in or on a passport database.”  

The photographs may not be used during automated searches.  

A search for the photo using the passport holder’s ID number or name is still permissible.  

The passport registry may only be accessed by Rikspolisstyrelsen and the passmyndigheten.  

Information from the registry may be delivered by the Rikspolisstyrelsen to the Police, Economic Crime Authority, Embassy, Consulate, Armed Forces, Coast Guard, Customs, Tax Authority, and Enforcement Authority.  

Biometric information is not kept.  

No upper time limit for the copy of the passport application and photograph. The passport registry is covered by secrecy laws and the application and photograph are kept in secret for seventy years. Thereafter, the photographs become public. |
| **Ukraine** | All residence registration, civil status, and biometric information required for the issuance of national identification card and passport for travel abroad is stored in the Unified State Demographic Registry. Biometric data includes the passport applicant’s digital photograph, digital signature, and fingerprints. The Unified State Demographic Registry was created in 2011 with the purpose of collecting, storing, and processing information required for the processing, issuance, and renewal of domestic and travel passports of Ukrainian citizens, and the processing of other documents that require the use of information collected by the Registry. Migration control and issuance of documents for migrants and alien residents is another purpose for collecting personal information in the Registry. The Registry is maintained by the Ukraine’s National Migration Service, which is a part of the Ministry of Internal Affairs (police). All government agencies and institutions, including provincial authorities, involved in providing services that require information collected and stored by the Registry have access to the database. Office of the Human Rights Commissioner, who is appointed by the national legislature, is responsible for monitoring access to the registry and reviewing measures aimed at protecting personal information stored in the database. There is no specific timeframe for storing biometric information in the Registry. The Registry Law states that “data shall be preserved for a period no longer than it is necessary for the purposes this information has been collected for.” Because most of the documents based on data stored in the Registry require renewal every ten years, one may assume that data in the system is preserved for at least a ten-year period. |
| **United States** | The US State Department’s Consular Consolidated Database (CCD) contains information about US citizens, US lawful permanent residents, and foreign nationals, including, among other Automated screening of passport, visa, and other service applicants; automated checking of applicant fingerprints; registration of applicant facial images for facial recognition; administrative management; access by Internal use by US State Department; use by external agencies including Department of Homeland Security (DHS), Customs and Border Protection, Department of Defense Intelligence and Security Command, Federal Bureau No clear statement is provided regarding the duration of the storage of data in the CCD. |
Biometric Data Retention for Passport Applicants and Holders

| things, biometric data such as fingerprints and facial images. | outside federal agencies. | of Investigation, DHS Terrorist Screening Center, US Citizenship and Immigration Services, and others. |


2 Id. art. 1.

3 Id. art. 3.


7 Schedule 2 of the Australian Passports Determination 2005 (Cth) sets out what information may be disclosed, including “the document holder’s photograph.”

8 Australian Passports Act 2005 (Cth) s 42(5).

9 Id. ss 45 & 46. Particular purposes for disclosing information include informing specified persons about the status of an Australian passport (e.g., where passports are lost, stolen, suspicious, etc.); confirming or verifying applicant information; facilitating or otherwise assisting international travel of a passport holder; law enforcement; “the operation of family law and related matters”; and other purposes specified by a Minister’s determination.


12 Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) (amending the Privacy Act 1988 (Cth)) sch 1 pt 4 cl 11 (Australian Privacy Principle 11–security of personal information).
Biometric Data Retention for Passport Applicants and Holders

13 *Passaporte*, MINISTÉRIO DA JUSTIÇA, [http://portal.mj.gov.br/main.asp?ViewID={923C474A-20F4-4842-B0CD-EFF29EA89DA8}&params=itemID={1CFC912B-84F8-4CF7-B5FE-2541B95B82D7};&UIPartUID={2868BA3C-1C72-4347-BE11-A26F70F4CB26}](http://portal.mj.gov.br/main.asp?ViewID={923C474A-20F4-4842-B0CD-EFF29EA89DA8}&params=itemID={1CFC912B-84F8-4CF7-B5FE-2541B95B82D7};&UIPartUID={2868BA3C-1C72-4347-BE11-A26F70F4CB26}).

14 Information provided over the phone by a Brazilian official.

15 *Id.*

16 *Id.*


24 *Id.* art. 18.


28 Décret No. 2005-1726, as modified by the Décret No. 2008-426 art. 24

to be equipped with an electronic storage medium that stores photograph, fingerprints and the personal data contained in the passport, and that these data are to be secured against unauthorized access, change, or erasure.

30 Id. § 21(1), (2).
31 Id. § 16 (2).
32 Id. § 16a.
33 Id. § 21 (2).
34 Id. § 16a.
35 Id. § 22 (1).
36 Id. § 22.
37 Id. § 16a.
38 Id. § 21 (4).
40 Id. § 41(1).
41 Inclusion of Biometric Identification Means and Biometric Identification Data in Identification Documents and in a Databank (Test Period) Decree, 5771-2011 (hereinafter IBI (Test Period) Decree), § 33, KOVETZ HATAKANOT 5771 No. 7025 p. 1287.
42 IBI Law § 1(1)–(2).
43 Id. §§ 10–11.
44 Id. § 14.
45 Id. § 6.
46 Id. § 41(1); IBI (Test Period) Decree § 33.
47 IBI (Test Period) Decree §8(4).
50 Preguntas Frecuentes [FAQs], 22. Si deseo realizar el trámite de pasaporte de mi menor hijo ¿Es necesario que éste acuda personalmente a realizar el trámite? [If I wish to get a passport for my minor child, is it necessary for him/her to appear personally ?], SECRETARIA DE RELACIONES EXTERIORES, http://www.sre.gob.mx/index.php/component/content/article/76-pasaportes/249-pasaportespreguntas-frecuentes (last visited Mar. 13, 2014).
Biometric Data Retention for Passport Applicants and Holders


60 Passports Act 1992, s 27H.


64 23§ PASSPORT INSTRUCTION.

65 6b § PASSPORT ACT.


67 23 § PASSPORT INSTRUCTION.
68 23 § PASSPORT INSTRUCTION.

69 See Sweden’s second column.

70 § 7, SFS 2009:641, as provided for by ch. 22;1 § ÖFFENTLIGHETS- OCH SEKRETESSLAGEN [PUBLIC INFORMATION AND SECRECY ACT] (Svensk Författningssamling [SFS] 2009:400).


72 Id.

73 Id. art. 4.

74 Id. art. 13.

75 Id. art. 2

76 Id. art. 11.


78 Id. art. 19 (translation by GLRD staff).

79 Id. art. 21.


81 Id. at 6.

82 Id. at 14–16.

83 The PIA for the CCD states, under the topic “[h]ow long is information retained?,” that “[t]he complete disposition schedule for passport records is specified in the U.S. Department of State Records Disposition Schedule, approved by the National Archives and Records Administration.” Id. at 8. The cited records disposition schedule for passport records is a thirty-one-page document listing various terms of disposition for different categories of documents. U.S. DEP’T OF STATE, U.S. DEPARTMENT OF STATE RECORDS SCHEDULE, Ch. 13: Passport Records, http://foia.state.gov/docs/RecordsDisposition/128494.pdf (last visited Mar. 12, 2014). Under the schedule, some passport files are to be retained permanently, some are to be destroyed after 100 years, some physical files are to be destroyed after fifteen years after being microfilmed, and some are to be destroyed “when active agency use ceases.” Id. at 1–3. The schedule includes disposition for data contained in the State Department’s database called the Travel Document Issuance System (TDIS), stating that such data should be deleted after six months. Id. at 20. The TDIS is one source of information for the CCD. CCD PIA, supra note 1, at 2. It is unclear, however, whether the data in the CCD from the TDIS is deleted from the CCD after six months. Disposition of data from other sources of CCD electronic data identified in the PIA, such as the Passport Lookout Tracking System and the Passport Information Electronic Records System, id. at 2, is not specifically provided for in the disposition schedule.