Biometric Data Retention for Passport Applicants and Holders

March 2014

The Law Library of Congress, Global Legal Research Center
(202) 707-6462 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

Biometric Data Retention for Passport Applicants and Holders

Ruth Levush
Senior Foreign Law Specialist (Coordinator),
and the Staff of the Global Legal Research Directorate

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.

Country	Availability of Biometric Database	Purpose of Database	Access to Data	Duration of Data Storage
Argentina	Biometric data collected includes fingerprints and photographs.[1]	Criminal investigation; national security[2]	Federal Police, Border Patrol, Coast Guard, Airport Security Police, National Registry of Individuals, and National Directorate of Migration[3]	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]
Australia	The Australian Passport Database stores information about passport applicants, including digitized photographs. Digitized	Passport applicant photographs are compared to images from any previously held Australian travel document. This includes digitally matching	Information held in the Australian Passport Database, including photographs,[7] may only be disclosed to "a person specified in a Minister's	Relevant legislation does not specify timeframes for data storage but passport applicants' personal information is subject to the Australian Privacy

	photographs are the only biometric information collected from applicants and are also contained in an Integrated Circuit Chip embedded in ePassports, which have been issued since October 2005.[5]	photographs against facial biometric information held in the Australian Passport Database to "ensure that the person has not applied for a travel document in another name."[6]	determination" for the purposes of performing functions under the Australian Passports Act 2005 (Cth).[8] Particular disclosure purposes are set out in the Act[9] and relevant persons to whom information may be disclosed for each purpose are specified in a Determination.[10]	Principles contained in the Privacy Act 1988 (Cth).[11] That Act provides that, where personal information is no longer needed for any purpose for which it may be used or disclosed, the relevant entity must "take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified."[12]
Brazil	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.[13]	Processing of passports and record keeping[14]	Federal Police, and possibly other official institutions that may enter into an agreement with the Federal Police[15]	Deletion date unspecified[16]
Canada	Canada maintains a facial recognition database that uses biometric data to	The purpose of the facial recognition database is to match the photo submitted	Data from the facial Recognition Database is accessed and used by	Unspecified

	help screen passport or travel document applicants.[17] The Office of the Privacy Commissioner (OPC) is working with the Passport Office to "avoid the development of centralized databases containing biometric information."[18]	by passport applicants against facial biometric information held in the Passport Database.[19]	Passport Canada. No policy or legislative framework was identified regarding "use, disclosure, retention, [or] disposal of biometric identifiers"[20] in accordance with privacy protections under the *Canadian Charter of Rights and Freedoms*[21] and the *Privacy Act.*[22]	
France	Biometric and civil status data related to passport applications is kept in a national database called TES.[23]	The principal purpose of the TES database appears to be the processing of passport applications, deliverances and renewals, and the prevention of passport falsification.[24]	The ETS database may be accessed by authorized government personnel for the purpose of processing passport applications and issuing passports.[25] 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.[26] Specially authorized law enforcement and intelligence personnel may access the national TES database for antiterrorism purposes.[27]	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.[28]

Germany	The German Passport Act states that Germany will not have a federal database of biometric passport data. [29]According to the same Act, the Passport Register contains photographs and relevant personal data of passport holders and nothing else.[30] Fingerprints may not be stored after a passport is issued.[31]	Biometric data contained in the passport may be used only to verify the identity of document and holder.[32] The Passport Register serves to issue passports and verify their authenticity, identify persons possessing or holding a passport, and to implement the Passport Act.[33]	Passport and law enforcement agencies may access biometric data contained in individual passports to verify the identity of the holder of the passport by comparing the biometric data stored in the passport with the biometric data observed in the holder.[34] Access to Passport Register limited to passport agencies for passport-related purposes[35] and to other agencies, as authorized by law.[36]	Biometric data used to verify authenticity of an individual passport or identity of its holder must be erased after this examination is concluded.[37] Personal data contained in the Passport Register must be stored until new passport is issued, but no longer than five years after expiration of passport.[38]
Hong Kong	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.	N/A	N/A	Retention of immigration records is generally subject to the Personal Data (Privacy) Ordinance, which provides only general rules on data protection.
Israel	On a trial basis: Biometric identification data of facial characteristics and of	Identification and verification of ID and travel documents.[42]	According to the Law, the Registry will be maintained by the Agency for Biometric Databank	Preliminary implementation of the Law from Jan. 1, 2013–Dec. 31, 2014, is designed to

	fingerprints[39] are being collected and stored on a voluntary basis during a test period[40] from Jan. 1, 2013 to Dec. 31, 2014.[41]		Management in the Ministry of Interior (MOI).[43] Data will be accessible by authorized MOI employees for purposes of issuing ID documents;[44] 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.[45]	examine its impact on volunteers and the utility of maintaining and using the biometric databank.[46] Biometric data used to verify authenticity of an individual passport or identity of its holder must be erased after this examination is concluded.[47]
Japan	Japan has a database that stores application forms for passports, which include applicants' photos.[48] There is no separate database to store the biometric data of all passport applicants.	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.	Not specified
South Korea	The Ministry of Foreign Affairs has a database on names, dates of births,	To carry out passport operations	Data is only for passport operations. Specifically, fingerprints cannot be	The period of keeping and management of fingerprints cannot exceed

	photos, fingerprints, addresses, passport issuance records, etc., of passport holders. There is no separate database to store passport applicants' biometric data.[49]		collected, kept, and managed for any purpose other than that of confirming the applicants themselves in the process of issuing the passport.	three months. Storage time for other personal information is not specified.
Mexico	The website of Mexico's Department of Foreign Relations (DFR) indicates that biometric data (fingerprints and photograph) are collected from passport applicants.[50] Mexico's Passport Regulation[51] and a website maintained by the DFR[52] briefly mention a passport database but do not provide details.	N/A	N/A	N/A
New Zealand	Since 1998, electronic passport application files, including photographs, have been stored in a secure database.[53] Since 2005, biometric photographic information has been stored in chips embedded in ePassports.[54]	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	The passport office may disclose passport information, including photographs,[56] to "any appropriate agency, body, or person to aid border security, facilitate the processing of passengers, verify the identity of a	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

		database in order to prevent fraud.[55]	holder of a travel document, or determine whether a person is a New Zealand citizen."[57] Formal written agreements with requesting organizations must be entered into by the passport office.[58]	for which the information may lawfully be used."[59] 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."[60]
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.[61]	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."[62] 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).[63] The Swedish National Police Board in turn is required to keep a central record of the passports.[64]	The photographs may not be used during automated searches.[65] A search for the photo using the passport holder's ID number or name is still permissible.[66] The passport registry may only be accessed by Rikspolisstyrelsen and the passmyndigheten.[67] 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.[68]	Biometric information is not kept.[69] 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.[70] 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.[71] Biometric data includes the passport applicant's digital photograph, digital signature, and fingerprints.[72]	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.[73] Migration control and issuance of documents for migrants and alien residents is another purpose for collecting personal information in the Registry.[74]	The Registry is maintained by the Ukraine's National Migration Service, which is a part of the Ministry of Internal Affairs (police).[75] 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.[76] 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.[77]	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."[78] Because most of the documents based on data stored in the Registry require renewal every ten years,[79] 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.[83]

	things, biometric data such as fingerprints and facial images.[80]	outside federal agencies.[81]	of Investigation, DHS Terrorist Screening Center, US Citizenship and Immigration Services, and others.[82]	

[1] Decreto 1766/2011 Créase el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) [Decree 1766/2011 Creating the Federal System of Biometric Identification for Security] art. 2, BOLETÍN OFICIAL [B.O.], Nov. 8, 2011,http://www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm.

[2] *Id*. art. 1.

[3] *Id*. art. 3.

[4] Ley 25326 Protección de Datos Personales [Law on Personal Data Protection], B.O. Nov. 2, 2000, http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm.

[5] *ePassport*, DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, https://www.passports.gov.au/web/epassport.aspx (last visited Mar. 12, 2014).

[6] *Id*. *See also* Australian Passports Act 2005 (Cth) s 47, http://www.comlaw.gov.au/Details/C2012C00135; Australian Passports Determination 2005 (Cth) r 7.6, http://www.comlaw.gov.au/Details/F2013C00149.

[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.

[10] Australian Passports Determination 2005 (Cth) rr 7.4 & 7.5. The relevant persons to whom information may be disclosed for particular purposes are set out in schedule 3 of this determination. *See also Protection and Release of Information*, DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, http://www.dfat.gov.au/publications/passports/Policy/ProtectionReleaseofInformation/index.htm (last visited Mar. 12, 2014).

[11] *See* notes to sections 46 and 47 of the Australian Passports Act 2005 (Cth) and rule 7.6 of the Australian Passports Determination 2005 (Cth). These notes have been amended to refer to the Australian Privacy Principles contained in amendment legislation that came into effect on March 12, 2014. Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) sch 5 cls 17–20, http://www.comlaw.gov.au/Details/C2012A00197. *See also Protecting Your Privacy*, DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, https://www.passports.gov.au/Web/ProtectingPrivacy.aspx (last visited Mar. 12, 2014).

[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).

[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}.

[14] Information provided over the phone by a Brazilian official.

[15] *Id.*

[16] *Id.*

[17] *Criticisms of E-passports and Facial Recognition Projects*, *in* SARA A. LEVINE, B.C. CIVIL LIBERTIES ASSOCIATION, PRIVACY HANDBOOK (2014), http://bccla.org/privacy-handbook/main-menu/privacy6contents/privacy6-10/. The statutory authority for creating the database appears to be; Canadian Passport Order, SI/81-86, http://laws-lois.justice.gc.ca/eng/regulations/SI-81-86/FullText.html. According to section 8.1(2) of the Order "[t]he Minister may convert an applicant's photograph into a biometric template for the purpose of verifying the applicant's identity, including nationality, and entitlement to obtain or remain in possession of a passport."

[18] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, DATA AT YOUR FINGERTIPS BIOMETRICS AND THE CHALLENGES TO PRIVACY 5, https://www.priv.gc.ca/information/pub/gd_bio_201102_e.pdf (last updated Nov. 1, 2011).

[19] *Facial Recognition Application Project – Passport Canada*, FOREIGN AFFAIRS, TRADE AND DEVELOPMENT CANADA, http://www.international.gc.ca/department-ministere/atip-aiprp/publications/facial-faciale.aspx?lang=eng (last updated Aug. 12, 2013).

[20] *Facial Recognition Project Privacy Impact Assessment Report*, PASSPORT CANADA, http://www.ppt.gc.ca/publications/facial.aspx?lang=eng (last modified May 5, 2006).

[21] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act, 1982, c. 11 (U.K.), http://laws-lois.justice.gc.ca/eng/charter/.

[22] Privacy Act, R.S.C., 1985, c. P-21, http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html.

[23] Décret No. 2005-1726 du 30 décembre 2005 relatif aux passeports [Decree No. 2005-1726 of December 30, 2005, Regarding Passports], *as modified by* Décret No. 2008-426 du 30 avril 2008 [Decree No. 2008-426 of April 30, 2008] , arts. 18–19, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000018763666&dateTexte=vig.

[24] *Id.* art. 18.

[25] Décret No. 2005-1726 art. 20.

[26] Décret No. 2005-1726 art. 21, *as modified by* Décret No. 2008-426.

[27] Décret No. 2005-1726, *as modified by* Décret No. 2012-1490 du 27 décembre 2012 [Decree No. 2012-1490 of December 27, 2012] art. 21-1, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000018763666&dateTexte=vig.

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

[29] Passgesetz [Passport Act] Apr. 19, 1986, BUNDESGESETZBLATT [BGBL.] I at 537, *as amended*, § 4 (3)),http://www.gesetze-im-internet.de/pa_g_1986/BJNR105370986.html. §4(3) was introduced in 2007, in implementation of EU Regulation 2252/204 and it provides also that passport are

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).

[39] Inclusion of Biometric Identification Means and Biometric Identification Data in Identification Documents and in a Databank, Law, 5770-2009 (hereinafter IBI Law), § 2, SEFER HAHUKIM No. 2217 p. 256.

[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).

[48] *Ryoken kanri masutafairu* [*Passport Management Master File*], E-GOV, MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS, http://gkjh.e-gov.go.jp/servlet/Ksearch?CLASSNAME=KJNMSTDETAIL&seqNo=0000001597&fromKJNMSTLIST=true (last visited Mar. 14, 2014).

[49] Passport Act, Act No. 8990, Mar. 28, 2008, *amended by* Act No. 11774, May 22, 2013, arts 7 & 8.

[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).

[51] Reglamento de Pasaportes y del Documento de Identidad y Viaje [Passport Regulation, as amended], art. 24, DIARIO OFICIAL DE LA FEDERACIÓN [D.O.], Aug. 5, 2011, available on the website of Mexico's Department of Foreign Relations, *at* http://www.sre.gob.mx/images/stories/marconormativodoc/redgpasa031213.pdf.

[52] *Apellidos de casada* [*Last Name of Married Women*], SECRETARIA DE RELACIONES EXTERIORES, http://embamex.sre.gob.mx/japon/index.php/es/pasaportes/92-si-va-a-tramitar-pasaporte-esto-es-importante (last visited Mar. 13, 2014).

[53] *Passport Data Protection Methods*, DEPARTMENT OF INTERNAL AFFAIRS, http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Legal-Privacy-Births-Deaths-Marriages-Civil-Unions-Name-Changes-Passports-and-Citizenship-Privacy-Notice?OpenDocument#data3 (last visited Mar. 13, 2014).

[54] Press Release, Hon. Rick Barker, NZ Passports to Contain Security Chip (Nov. 3, 2005), http://www.beehive.govt.nz/node/24492; Press Release, Department of Internal Affairs, E-Passport Boosts Security for All New Zealanders (Nov. 3, 2005), http://www.dia.govt.nz/press.nsf/d77da9b523f12931cc256ac5000d19b6/87b380d5390e3b1fcc2570ae00114c3f!OpenDocument.

[55] *Questions and Answers on Passport Fee Changes and Passport Online Renewal Service*, PASSPORTS.GOVT.NZ, http://www.passports.govt.nz/Questions-and-answers-on-the-passport-fee-changes-and-the-Passport-Online-Renewal-Service (last visited Mar. 13, 2014).

[56] Passports Act 1992, s 37(1)(g), http://legislation.govt.nz/act/public/1992/0092/latest/DLM277433.html.

[57] *Your Privacy*, PASSPORTS.GOVT.NZ, http://www.passports.govt.nz/Your-privacy (last visited Mar. 12, 2014); Passports Act 1992, s 36(1).

[58] Passports Act 1992, s 36(2). Disclosure arrangements currently exist with the New Zealand Customs Service, New Zealand Department of Labour, Australian Department of Immigration and Citizenship, Australian Customs Service, US Department of Homeland Security (only when a person travels to the US), and New Zealand Police for Interpol (only details of documents reported lost, stolen, or otherwise invalid). *Births, Deaths, Marriages, Civil Unions, Name Changes, Passports and Citizenship Privacy Notice*, DEPARTMENT OF INTERNAL AFFAIRS, http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Legal-Privacy-Births-Deaths-Marriages-Civil-Unions-Name-Changes-Passports-and-Citizenship-Privacy-Notice?OpenDocument (scroll to "Travel Document Disclosures") (last visited Mar. 12, 2014).

[59] Privacy Act 1993, s 6, Principle 9, http://legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

[60] Passports Act 1992, s 27H.

[61] 6a § § PASSLAG [PASSPORT ACT] (Svensk Författningssamling [SFS] 1978:302), http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/sfs_sfs-1978-302/.

[62] *See* Proposition [Prop.] 2004/05:119 p. 50.

[63] 22 § PASSFÖRORDNING [PASSPORT INSTRUCTION] (Svensk Författningssamling [SFS] 1979:664).

[64] 23§ PASSPORT INSTRUCTION.

[65] 6b § PASSPORT ACT.

[66] Prop. 2004:05:119 p. 51.

[67] 23 § PASSPORT INSTRUCTION.

[68] 23 § PASSPORT INSTRUCTION.

[69] *See* Sweden's second column.

[70] 6§ p. 7, SFS 2009:641, as provided for by ch. 22;1 § OFFENTLIGHETS- OCH SEKRETESSLAGEN [PUBLIC INFORMATION AND SECRECY ACT] (Svensk Författningssamling [SFS] 2009:400).

[71] Law of Ukraine on Unified State Demographic Registry and Documents that Confirm Citizenship of Ukraine or Individual's Special Status (Registry Law), VIDOMOSTI VERKHOVNOI RADY [VVR] [official gazette] (in Ukrainian) 2013, No. 51, Item 716, art. 7, *available at* http://zakon4.rada.gov.ua/laws/show/5492-17 (official parliamentary website, last visited March 13, 2014).

[72] *Id*.

[73] *Id*. art. 4.

[74] *Id*. art. 13.

[75] *Id*. art. 2

[76] *Id*. art. 11.

[77] Law of Ukraine on Protection of Personal Data, VVR 2010, No. 34, Item 481, art. 9, at http://zakon4.rada.gov.ua/laws/show/2297-17 (official parliamentary website, last visited March 13, 2014).

[78] *Id*. art. 19 (translation by GLRD staff).

[79] *Id*. art. 21.

[80] U.S. DEP'T OF STATE, CONSULAR CONSOLIDATED DATABASE (CCD) PRIVACY IMPACT ASSESSMENT (PIA) 2 (Mar. 22, 2010), http://www.state.gov/documents/organization/93772.pdf.

[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.