epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE of the

THE DEPARTMENT OF HOMELAND SECURITY

[DHS Docket No. DHS-2013-0016]

Agency Information Collection Activities:

Office of Biometric Identity Management (OBIM)

Biometric Data Collection at the Ports of Entry

June 14, 2013

By notice published on April 15, 2013, in compliance with the Paperwork Reduction Act, the Department of Homeland Security ("DHS") published a request for comments regarding the Office of Biometric Identity Management ("OBIM") collection of biometric data at ports of entry to the United States.[1] The Paperwork Reduction Act mandates that, in connection with federal information collections, agencies "assume responsibility and accountability" for Privacy Act compliance and enforce privacy, confidentiality, and security "policies, procedures, standards, and guidelines."[2]

Pursuant to the DHS notice of April 15, 2013, and consistent with the purposes of the Paperwork Reduction Act, EPIC submits these comments to address the privacy and security issues the OBIM's data collection raises. EPIC recommends that DHS cease all data collection activity until these privacy concerns are addressed and rectified. Specifically, EPIC recommends that DHS: (1) impose strict

[1] Agency Information Collection Activities: Office of Biometric Identity Management (OBIM) Biometric Data Collection at the Ports of Entry, 78 Fed. Reg. 22274-75 (Apr. 15, 2013).
[2] 44 U.S.C. § 3506 (g).

information security safeguards on its biometric information collection and limit its dissemination of biometric information; (2) conduct a comprehensive privacy impact assessment on the OBIM Program; (3) grant individuals Privacy Act rights before collecting additional biometric information; and (4) adhere to international privacy standards.

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving privacy safeguards established by Congress, including the Privacy Act of 1974, and routinely comments in public rulemakings on agency proposals.[3]

The OBIM program was formerly known as the United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") program. EPIC commented extensively on DHS's US-VISIT program and the collection of biometric data. During the program's introduction in 2004, EPIC urged DHS to ensure that the US-VISIT program complied with the Privacy Act and international privacy standards.[4] EPIC also encouraged DHS not to exempt biometric databases from Privacy Act protection, and to reduce the time records are stored within DHS databases.[5] In 2005, EPIC objected to the expansion of the US-VISIT Program[6] and the introduction of radio frequency identification ("RFID") tags into traveler forms.[7] EPIC has also submitted numerous *amicus* briefs concerning privacy, including to the

[3] *See, e.g.*, EPIC et al., *Comments Urging the Department of Homeland Security To (A) Suspend the "Automated Targeting System" As Applied To Individuals, Or In the Alternative, (B) Fully Apply All Privacy Act Safeguards To Any Person Subject To the Automated Targeting System* (Dec. 4, 2006), *available at* http://epic.org/privacy/pdf/ats_comments.pdf; EPIC, *Comments on Automated Targeting System Notice of Privacy Act System of Records and Notice of Proposed Rulemaking, Docket Nos. DHS-2007-0042 AND DHS-2007-0043* (Sept. 5, 2007), *available at* http://epic.org/privacy/travel/ats/epic_090507.pdf. See also, EPIC: Automated Targeting System, https://epic.org/privacy/travel/ats/.
[4] EPIC, *Comments of the Electronic Privacy Information Center* (Feb. 4, 2004), http://epic.org/privacy/us-visit/us-visit_comments.pdf.
[5] EPIC, *Comments of the Electronic Privacy Information Center* (Jan. 11, 2004), http://epic.org/privacy/us-visit/ADIS_comments.pdf.
[6] EPIC, *Comments of the Electronic Privacy Information Center* (Nov. 5, 2004), http://epic.org/privacy/us-visit/us-visit_comments2.pdf.
[7] EPIC, *Comments of the Electronic Privacy Information Center* (Aug. 4, 2005), http://epic.org/privacy/us-visit/comments080405.pdf; EPIC, *Comments of the Electronic Privacy Information Center* (Oct. 3, 2005);

Supreme Court in *Hiibel v. Sixth Judicial District Court of Nevada*, which discussed the US-VISIT program in the context of the proliferation of personal information in government databases.[8]

Scope of the OBIM Program and Proposed Data Collection

DHS started the US-VISIT program, presently known as the OBIM program, in 2004 as a result of measures included in the Homeland Security Act of 2002.[9] According to the Department, the purpose of the system is to allow the U.S. Government to track aliens and prevent fraud by recording biometric information at points of entry to the United States.[10]

The program initially captured only two fingerprints.[11] It has since expanded to include all ten fingerprints, as well as photographs.[12] A 2010 DHS report on biometric standards requirements for the US-VISIT program indicates that additional biometric data is being contemplated for capture, including DNA.[13] Information released by Accenture, a contractor responsible for much of the technology behind the US-VISIT program, indicates that biometric data such as iris scans, palm prints, scars, marks, tattoos, and DNA are being developed for use.[14]

Biometric data obtained upon entry to the United States is stored in the Arrival and Departure Information System ("ADIS").[15] In 2009, DHS issued a final rule exempting portions of the ADIS system

[8] Brief for Electronic Privacy Information Center (EPIC) and Legal Scholars and Technical Experts as Amici Curiae, *Hiibel v. Sixth Judicial District Court of Nevada*, 542 U.S. 177 (2004) (No. 03–5554), *available at* http://epic.org/privacy/hiibel/epic_amicus.pdf.
[9] CNN, *Program to fingerprint U.S. visitors starts* (Jan. 5, 2004), http://www.cnn.com/2004/US/01/04/visit.program/.
[10] Department of Homeland Security, *US-VISIT Traveler Information*, http://www.dhs.gov/us-visit-traveler-information (last visited Jun. 5, 2013).
[11] Lawrence M. Wein and Manas Baveja, *Using fingerprint image quality to improve the identification performance of the U.S. Visitor and Immigrant Status Indicator Technology Program*, 102:21 PROCEEDINGS OF THE NATIONAL ACADEMY OF SCIENCES OF THE UNITED STATES OF AMERICA 7772, May 13, 2005, *available at* http://www.pnas.org/content/102/21/7772.full.pdf.
[12] Department of Homeland Security, *What to Expect when Visiting the United States*, http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_traveler_brochure_english.pdf (last visited Jun. 5, 2013).
[13] Department of Homeland Security, *Biometric Standards Requirements for US-VISIT* (March 15, 2015), http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_biometric_standards.pdf.
[14] Accenture, *U S Department of Homeland Security: Security Management and Biometrics*, http://www.accenture.com/us-en/Pages/success-improved-homeland-security-management-biometrics.aspx (last visited Jun. 5, 2013).
[15] Privacy Act of 1974; Department of Homeland Security National Protection and Programs Directorate--001 Arrival and Departure Information System, System of Records, 78 Fed. Reg. 31955-58 (May 28, 2013).

from the Privacy Act of 1974[16] "because of criminal, civil, and administrative enforcement requirements."[17] Recently, DHS has published notice of its intention to continue exempting the ADIS system from various parts of the Privacy Act.[18]

Biometric data collected from the US-VISIT program is shared with numerous other government entities, including the Department of Defense, Department of Justice, and state and local law enforcement.[19] Currently, 30,000 individuals from federal, state, and local governments access the data contained in the US-VISIT program every day.[20] Biometric data is also shared with foreign governments, including Canada, Australia, and the United Kingdom.[21]

In January 2009, DHS issued a final rule that expanded the class of persons subject to the US-VISIT program to include almost all aliens, including lawful permanent residents ("LPRs").[22] In March 2013, OBIM took over various functions of the US-VISIT Program.[23]

In DHS's information collection Federal Register notice, the agency states that OBIM will collect and disseminate "biometric information (digital fingerprint images and facial photos) from individuals during their entry into the United States."[24] DHS states the collection will take 35 seconds.[25]

With this proposed information collection, DHS is "particularly interested in comments that":

> 1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; 2. Evaluate the accuracy of the agency's estimate of the burden of the

[16] 5 U.S.C. § 552a.
[17] Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/National Protections and Programs Directorate/U.S. Visitor and Immigrant Status Indicator Technology--001 Arrival and Departure Information System of Records, 74 Fed. Reg. 63944-46 (Dec. 4, 2009).
[18] *See* Privacy Act of 1974; Department of Homeland Security National Protection and Programs Directorate--001 Arrival and Departure Information System, System of Records, 78 Fed. Reg. 31955-58 (May 28, 2013).
[19] DHS, *Government Agencies Using US-VISIT*, http://www.dhs.gov/government-agencies-using-us-visit (last visited Jun. 5, 2013).
[20] *Id.*
[21] CBC News, *U.S., Canada will share refugee fingerprints* (Nov. 24, 2009), http://www.cbc.ca/news/canada/story/2009/11/24/biometrics-refugees024.html.
[22] United States Visitor and Immigrant Status Indicator Technology Program ("US-VISIT"); Enrollment of Additional Aliens in US-VISIT; Authority To Collect Biometric Data From Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 73 Fed. Reg. 77473-01 (Dec. 19, 2008).
[23] Department of Homeland Security, *Office of Biometric Identity Management*, http://www.dhs.gov/obim (last visited Jun. 5, 2013).
[24] 78 Fed. Reg. 22275.
[25] *Id.*

> proposed collection of information, including the validity of the methodology and assumptions used; 3. Enhance the quality, utility, and clarity of the information to be collected; and 4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.[26]

EPIC's recommendations pertain to points 3 and 4 above because by protecting privacy and information integrity, DHS can enhance the quality of information, as well as minimize the burden on respondents.

1. DHS Should Impose Strict Information Security Safeguards on its Biometric Information Collection and Limit its Dissemination of Biometric Information

Information security is a critical consideration for any organization that collects digital records and data, and it is even more important when government agencies collect sensitive and personally identifying information. Government agencies must make every effort to safeguard sensitive information. Without proper safeguards, individuals and groups with malicious intent to intrude, access, and obtain sensitive information may disrupt operations or launch attacks against computer systems and networks. This concern has become even more important given the increasing number of security incidents and ease of obtaining hacking tools.[27]

The OBIM program "relies extensively on computerized networks and systems to collect, access, and process a significant amount of personal and sensitive information on foreign visitors, immigrants, and legal permanent residents."[28] Consequently, substantial information security safeguards are essential to prevent data breaches, manipulation, and malicious attacks.

The U.S. Government Accountability Office ("GAO") has previously reported that the US-VISIT program contained significant information security weaknesses.[29] In a 2007 report, GAO noted that

---

[26] *Id.*
[27] U.S GOV'T ACCOUNTABILITY OFFICE, GAO-07-870, Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program 3 (2007); *See also* Tech News Daily, *How to Hack an iPhone With a USB Charger* (June 3, 2013) http://www.technewsdaily.com/18241-iphone-malicious-charger.html; The Nation, *Spear phishing: How the non-nerds hack into you* (June 14, 2013), http://www.nationmultimedia.com/opinion/Spear-phishing-How-the-non-nerds-hack-into-you-30208233.html; The Sydney Morning Herald, *The fly-by, Wi-Fi Hacking Machine* (May 24, 2013) http://www.smh.com.au/it-pro/security-it/the-flyby-wifi-hacking-machine-20130524-2k5xg.html.
[28] U.S GOV'T ACCOUNTABILITY OFFICE, GAO-07-870, Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program 16 (2007);
[29] *Id.* at 18.

despite DHS access requirements, Customs and Border Protection ("CBP") "did not control access to its restricted information technology spaces since its physical access systems were controlled by local authorities."[30]

While the GAO reports that the DHS has complied with its recommendations concerning information security in the US-VISIT Program, the OBIM program still raises substantial privacy risks. The GAO recommendations, for example, did not include any measures to ensure adequate physical safety of critical information spaces. Because the OBIM program will disseminate biometric information to other federal agencies, state and local law enforcement agencies, downstream protection of this information is incredibly important. Because of inherent difficulty in maintaining adequate safeguards after such information is disseminated, DHS should limit biometric information as much as possible and restrict access to only those agencies that have proven an ability to safely protect the information.

These concerns are significant. Government actors from local law enforcement to federal and state agencies have consistently proven unable to properly safeguard sensitive information. In October 2012 South Carolina announced that an "international hacker had stolen 3.6 million Social Security numbers and 387,000 credit and debit card numbers."[31] Former state senator John Hawkins said that "the state had failed to protect taxpayers and had not reported the attack promptly."[32] Also, the TSA suffered significant security problems with its passenger redress website when the TSA failed to secure the website; large amounts of personal information were leaked, exposing hundreds of travelers to identity theft.[33] Moreover, later that year, the TSA reported that an external hard drive containing Social Security numbers, payroll information, and bank data for about 100,000 TSA employees was stolen from

[30] *Id.* at 21.
[31] New York Times, *Hacking of Tax Records Has Put States on Guard*, (Nov. 5, 2012) http://www.nytimes.com/2012/11/06/us/south-carolina-tax-hacking-puts-other-states-on-alert.html.
[32] *Id.*
[33] U.S House, Committee On Oversight And Government Reform. *Information Security Breach at TSA, The Traveler Redress Website* (January 2008). http://web.archive.org/web/20080131043651/http://oversight.house.gov/documents/20080111092648.pdf

a "secure area."[34] And from January 1, 2009 to May 31, 2012, there have been 268 breach incidents in government agencies exposing more than 94 million records containing personally identifiable information.[35]

Furthermore, DHS itself has had issues securing personal and sensitive information of its employees as recently as last month. Tens of thousands of DHS employees and contractors who submitted background investigation information were at risk of having their personal data stolen, exposing them to identify theft. An internal DHS notice sent to employees noted that "[a]s a result of this vulnerability, information including name, Social Security numbers (SSN) and date of birth (DOB), stored in the vendor's database of background investigations was potentially accessible by an unauthorized user since July 2009."[36]

A report[37] from the Electronic Frontiers Foundation ("EFF") and the Immigration Policy Center ("IPC"), warns that DHS biometric databases raise serious privacy concerns in that "biometrics are not infallible, and databases contain errors. These problems can result in huge negative consequences for U.S. citizens and legal immigrants mistakenly identified."[38] Concerns for effective information security become even more important when combined with possible database errors; not only are breaches of private and sensitive information possible, but also unauthorized exposure of incorrect personal information.

These weaknesses across government agencies collectively increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information, including personally identifiable information, and disrupt the operations of the OBIM program.

---

[34] Washington Post, *TSA Hard Drive With Employee Data Is Reported Stolen* (May 5, 2007). http://www.washingtonpost.com/wp-dyn/content/article/2007/05/04/AR2007050402152.html.
[35] Rapid7, *Data Breaches in the Government Sector* http://www.rapid7.com/docs/data-breach-report.pdf; *See also* Privacy Rights Clearinghouse, www.privacyrights.org.
[36] Federal News Radio, *Data Breach puts DHS employees at Risk of Identity Theft* (May 22, 2013) http://www.federalnewsradio.com/473/3332836/Data-breach-puts-DHS-workers-at-risk-of-identity-theft.
[37] EFF, *From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities*, (May 2012) https://www.eff.org/document/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond.
[38] Think Progress, *Report: Biometric Data Collection And Database Sharing Poses Serious Privacy Concerns* (May 31, 2012) http://thinkprogress.org/security/2012/05/31/492739/biometric-data-privacy/?mobile=nc.

EPIC recommends oversight to ensure DHS and recipients of OBIM data consistently apply the upmost information security safeguards to protect sensitive data. EPIC also recommends that dissemination of OBIM information is strictly limited to only those agencies and government actors that require the information as a necessity and that the information is strictly limited to uses for which it was originally collected.

2. DHS Should Conduct a Comprehensive Privacy Impact Assessment on the OBIM Program

Due to the continued development and expansion of the US-VISIT program, EPIC requests that DHS issue a comprehensive Privacy Impact Assessment ("PIA") for biometric data collection at points of entry in accordance with the E-Government Act of 2002.

Under the E-Government Act of 2002, Federal agencies that are

> (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
> (ii) initiating a new collection of information that—
> (I) will be collected, maintained, or disseminated using information technology; and
> (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government[39]
> must conduct a PIA regarding the collection of the data.[40]

The E-Government Act of 2002 was passed, in part, to "provide increased opportunities for citizen participation in Government . . . [to] make the Federal Government more transparent and accountable . . . [and to] provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy . . ."[41]

The 2003 Office of Management and Budget Guidance for the Implementation of the Privacy Provisions of the E-Government Act of 2002 ("OMB Guidance") includes useful guidance for agencies conducting PIAs. First, "individual" is defined for the purposes of the E-Government Act as a US citizen

[39] E-Government Act of 2002, Pub. L. No 107-347, §208(b)(1)(A) (2002).
[40] *Id.*
[41] *Id.* §2(b).

or an alien lawfully admitted for permanent residence.[42] Second, the OMB Guidance directs agencies that "*In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks.*"[43] This includes, but is not limited to, instances when government databases that hold identifiable information are merged, centralized, or matched with other databases, and when new identifiable information is added to a collection that raises the risks to personal privacy.[44]

> DHS policy regarding PIAs states that where a DHS program involves multiple systems:
>
> it may be more appropriate to conduct a single PIA than to conduct a separate PIA on each of the information technology systems. Such a PIA provides a more holistic view of the privacy concerns related to a program, rather than a specific IT system, particularly where an individual may be interacting with multiple IT systems and the privacy concerns arise not from a specific system but from its use in combination with other systems.[45]

The Memo also gives another reason why conducing a single, comprehensive PIA is better than multiple narrow PIAs: "[t]o ensure greater transparency and help build trust in DHS operations . . . a single PIA provides the public with a comprehensive view of a program's privacy impact and how the privacy concerns have been addressed."[46]

In regards to the current DHS request for comments related to the OBIM biometric data collection, EPIC requests that a complete and comprehensive PIA be issued before the program proceeds. As a threshold matter, the E-Government Act applies to the OBIM's collection of biometric data because it has been expanded to cover permanent legal residents.[47] While there have been many incremental PIAs regarding the US-VISIT and IDENT programs[48] that were necessary under the E-Government Act, it is

---

[42] Joshua B. Bolten, Memorandum for Heads of Executive Departments and Agencies (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda_m03-22/#b.
[43] *Id.* (emphasis in original).
[44] *See id.*
[45] Hugo Teufel III, Privacy Policy Guidance Memorandum (Dec. 30, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf.
[46] *Id.*
[47] United States Visitor and Immigrant Status Indicator Technology Program ("US-VISIT"); Enrollment of Additional Aliens in US-VISIT; Authority To Collect Biometric Data From Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 73 Fed. Reg. 77473-01 (Dec. 19, 2008).
[48] *See, e.g.*, DHS, *US-VISIT Program, Increment 1 Privacy Impact Assessment* (Dec. 18, 2003), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_inc1.pdf; DHS, *US-VISIT Program, Increment 2 Privacy Impact Assessment* (Sept. 14, 2004), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit.pdf; DHS, *Privacy Impact Assessment Update for*

time for DHS to re-assess the entirety of the US-VISIT program as it is taken over by OBIM for several reasons.

First, there have been numerous developments in the DHS's collection of biometric data. The US-VISIT program has dramatically expanded the amount of biometric data it is collecting,[49] and there is continuing development of new biometric collection technologies for use such as iris and DNA.[50] There has been an expansion of classes of persons that are subject to the US-VISIT program.[51] There is widespread sharing of biometric data obtained through the US-VISIT program with other federal, state, and local agencies and law enforcement[52], and with foreign governments.[53] The development of new technologies and the merging of databases storing biometric data are precisely the type of situations that the OMB Guidance defines as necessitating a PIA. To date, no comprehensive PIA has been issued by DHS covering the entirety of these developments. When viewed as a whole, it is highly likely that additional privacy concerns not previously considered will come to light.

This is precisely what former Chief Privacy Officer Teufel stated in his Memorandum where a DHS data collection program uses multiple systems, a single PIA may be more appropriate.[54] Using

---

the US-VISIT Program In Conjunction with the Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Ports of Entry (Jul. 1, 2005), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisitupd1.pdf; DHS, *Privacy Impact Assessment Update for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program in conjunction with the Notice of Proposed Rulemaking on the Authority to Process Additional Aliens in US-VISIT* (Jul. 12, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_addaliens.pdf; DHS, *Privacy Impact Assessment Update for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program In conjunction with the Final Rule (73 FR 77473), Enrollment of Additional Aliens in US-VISIT* (Feb. 10, 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_addl%20aliens.pdf; DHS, *Privacy Impact Assessment for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program Comprehensive Exit Program: Air Exit Pilot* (May 20, 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_air_exit.pdf; DHS, *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)* (Dec. 7, 2012), *available at* http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_usvisit_ident_appendixj_jan2013.pdf.

[49] DHS, *What to Expect when Visiting the United States*, http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_traveler_brochure_english.pdf (last visited Jun. 5, 2013).

[50] *See* Department of Homeland Security, *Biometric Standards Requirements for US-VISIT* (March 15, 2015), http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_biometric_standards.pdf.

[51] DHS, *supra* note 22.

[52] DHS, *Government Agencies Using US-VISIT*, http://www.dhs.gov/government-agencies-using-us-visit (last visited Jun. 5, 2013).

[53] CBC News, *U.S., Canada will share refugee fingerprints* (Nov. 24, 2009), http://www.cbc.ca/news/canada/story/2009/11/24/biometrics-refugees024.html.

[54] Hugo Teufel, *supra* note 45.

multiple technologies in conjunction with one another is different from isolated use of single technologies. Disclosing information to many other entities on the international, national, state, and local levels differs from only sharing information with one level. A comprehensive PIA for the OBIM would rectify these concerns, and for the first time consider the entire privacy implications of biometric data collection.

Second, a comprehensive PIA is necessary in light of the new security concerns raised by DHS data breaches. As noted above, there have been numerous data breaches of DHS and TSA computer systems over the last several years,[55] and as recently as last month.[56] As the data collected under the OBIM/US-VISIT programs have unique privacy concerns, a PIA addressing the potential consequences of a data breach is necessary.

Third, because part of the E-Government Act's purpose is to enable greater citizen participation and to increase government program transparency,[57] a single, updated, comprehensive PIA for the OBIM/US-VISIT program will significantly further these goals. As noted in Teufel's Memorandum, a single PIA "provides the public with a comprehensive view of a program's privacy impact and how the privacy concerns have been addressed."[58] Anyone attempting to piece together the myriad of different PIAs regarding US-VISIT, ADIS, OBIM, and other DHS initiatives would find it almost impossible to ascertain all of the privacy issues presented by the many facets of the current program. EPIC recommends that DHS issue a new comprehensive PIA to remedy this problem.

3. Before Collecting Additional Biometric Information, DHS Should Grant Individuals Privacy Act Rights

EPIC urges DHS to withdraw the proposed Privacy Act exemptions for the OBIM biometric data collection program. As noted above, DHS exempts the record system that stores biometric data collected

[55] *See supra*, notes 29-36.
[56] *See supra*, note 36.
[57] Pub. L. No 107-347, §2(b).
[58] Hugo Teufel, *supra* note 45.

from visitors to the US, ADIS, from several provisions of the Privacy Act.[59] These include subsections (c)(3) and (4) (Accounting for Disclosures), (d) (Access to Records), (e)(1) (Relevancy and Necessity of Information), (e)(2) (Collection of Information from Individuals), (e)(3) (Notice to Subjects), (e)(4)(G) and (H) and (f) (Agency Requirements), (e)(5) (Collection of Information), (e)(8) (Notice on Individuals), and (g) (Civil Remedies).[60]

EPIC has previously commented on DHS proposals to exempt data collection efforts from the Privacy Act.[61] As part of the purpose of the Paperwork Reduction Act is to ensure data collection efforts by federal agencies conform to all laws related to "privacy and confidentiality . . . "[62], EPIC renews its objections to the newly proposed DHS's exemptions. In particular, EPIC requests DHS and OBIM to justify its exemptions to the Privacy Act for the collection of biometric data. This is of special concern in regards to Legal Permanent Residents ("LPR"), who are covered by the Privacy Act[63] and yet are subject to the US-VISIT program.[64]

Additionally, all persons, regardless of their status as US citizens or LPR have privacy rights under international law and guidelines.[65] DHS should not contravene internationally established norms regarding the collection of personal data, especially particularly sensitive biometric data. EPIC urges DHS to reconsider its exemptions to the Privacy Act for all persons subject to the US-VISIT/OBIM program.

4. DHS's OBIM Should Adhere to International Privacy Standards

Since January 2003, DHS has collected personal information and biometric identifiers of thousands of travelers entering this country every day. Given the extensive disclosure of US-

[59] *See* Privacy Act of 1974; Department of Homeland Security National Protection and Programs Directorate--001 Arrival and Departure Information System, System of Records, 78 Fed. Reg. 31955-58 (May 28, 2013).
[60] DHS, Privacy Act of 1974: Implementation of Exemptions, 72 Fed. Reg. 46921-22 (Aug. 22, 2007), *available at* http://www.gpo.gov/fdsys/pkg/FR-2007-08-22/pdf/E7-16461.pdf.
[61] *See* EPIC, *Comments of the Electronic Privacy Information Center* (Jan. 12, 2004), http://epic.org/privacy/us-visit/ADIS_comments.pdf.
[62] 44 U.S.C. § 3501(8)(A).
[63] 5 U.S.C. § 552a(a)(2).
[64] United States Visitor and Immigrant Status Indicator Technology Program ("US-VISIT"); Enrollment of Additional Aliens in US-VISIT; Authority To Collect Biometric Data From Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 73 Fed. Reg. 77473-01 (Dec. 19, 2008).
[65] *See infra* Part 4.

VISIT/OBIM information from DHS to other law enforcement entities, there is a high likelihood that this information will be used for purposes beyond the legal authority by which US-VISIT was created.

To further the important objective of guarding against mission creep, EPIC urges DHS to consider the application of international privacy standards to the collection and use of personal information obtained for non-U.S. citizens. The international community has recognized time and time again that all individuals have rights in their personal information, regardless of nationality. A number of countries, including Brazil, Japan, and China,[66] have objected to DHS's collection and use of biometric and personal information about their citizens. As it expands OBIM, DHS should recognize the danger of continuing to disregard international human rights standards, and strive to align its practices with the principles articulated by international guidelines for protecting privacy.

The Universal Declaration of Human Rights ("Universal Declaration") provides that no individual "shall be subjected to arbitrary interference with his privacy," and that "[e]veryone has the right to protection of the law against such interference or attacks."[67] Furthermore, "no distinction shall be made on the basis of the political, jurisdictional, or international status of the country or territory to which a person belongs."[68] The United States was a key architect of the Universal Declaration and one of the original signatories. It is thus surprising to find our nation deploying a system that violates the Universal Declaration by encroaching upon the privacy of individuals based on their lack of U.S. citizenship, and failing to provide them rights in their personal information held by the United States.

Similarly, the OECD Privacy Guidelines of 1980 ("OECD Privacy Guidelines") apply to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and

---

[66] *See* New York Times, *Brazil Seeks to Bypass Fingerprinting*, (Jan. 14, 2004); Mainichi Daily News, *Japan to Demand U.S. Erase Fingerprints, Photos After Visitors Leave Country*, (Sept. 29, 2004) *available at* http://www12.mainichi.co.jp/news/mdn/search-news/916107/US2dVISIT-0-1.html; China Daily, *US Urged Not to Fingerprint Chinese* (March 24, 2004) available at http://www.chinadaily.com.cn/english/doc/2004-03/24/content_317687.htm.

[67] United Nations, Universal Declaration of Human Rights, G.A. Res. 217A(III), U.N. GAOR, 3d Sess., U.N. Doc. A/810 (1948), art. 12, reprinted in M. ROTENBERG ED., THE PRIVACY LAW SOURCEBOOK 2003 318 (EPIC 2003) (emphasis added) [hereinafter PRIVACY LAW SOURCEBOOK].

[68] *Id.* art. 2 at 318.

individual liberties."[69] The OECD Privacy Guidelines require, among other things, that there should be limitations on the collection of information; collection should be relevant to the purpose for which it is collected; there should be a policy of openness about the information's existence, nature, collection, maintenance and use; and individuals should have rights to access, amend, complete, or erase information as appropriate.[70] OBIM, as currently designed, will deny non-U.S. citizens the fundamental protections of these internationally recognized standards.

The United Nations Guidelines for the Regulation of Computerized Personal Files of 1990 ("UN Privacy Guidelines") recognize many of the same rights in information as the OECD Privacy Guidelines provide, providing in addition that "data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, philosophical and other beliefs . . . should not be compiled."[71] The OBIM program may collect and use information of this nature to evaluate whether visitors may enter the United States, a use that would clearly violate the UN Privacy Guidelines.

In addition, the European Union Data Protection Directive ("EU Directive") recognizes a right to privacy in personal information and establishes protections for information collected from all individuals, regardless of nationality.[72] Like both sets of Guidelines, the EU Directive recognizes an individual's right to access information and requires that information be kept accurate and timely.[73] The EU Directive also requires that information be relevant to the purpose for which it is collected.[74] By neglecting to give non-U.S. citizens rights in information about them used in the OBIM program, the United States has failed to comply with this widely recognized legal regime for privacy protection. Moreover, the proposed General

[69] Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data, OECD Doc. 58 final (Sept. 23, 1980), art. 3(a), reprinted in PRIVACY LAW SOURCEBOOK at 330.
[70] *Id.* Basic Principles of National Application at 331.
[71] United Nations, G.A. Res. 45/95, Guidelines for the Regulation of Computerized Personal Files (Dec. 14, 1999) prin. 5, reprinted in PRIVACY LAW SOURCEBOOK at 368.
[72] Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, reprinted in PRIVACY LAW SOURCEBOOK at 371.
[73] *Id.* art. 6 at 384.
[74] *Id.*

Data Protection Regulation (GDPR)[75], which will supersede the current EU Directive, expands on privacy and data protection safeguards related to new technological developments such as cloud computing. DHS should take affirmative steps in ensuring safeguards evolve alongside new technologies.

The United States is a signatory of the Universal Declaration, the OECD Privacy Guidelines, and the UN Privacy Guidelines. The United States' collection and use of personal information of non-U.S. citizens through the OBIM program violates these guidelines, as well as the EU Directive, and suggests a disregard for international privacy laws and human rights standards. As it expands OBIM, DHS should recognize the danger of continuing to disregard international human rights standards, and strive to align its practices with the principles articulated by international guidelines for protecting privacy.

Conclusion

For the aforementioned reasons, EPIC opposes DHS's collection of biometrics and urges the agency to cease collecting biometric information without proper privacy safeguards in place. EPIC recommends that, at a minimum, DHS: (1) impose strict information security safeguards on its biometric information collection and limit its dissemination of biometric information; (2) conduct a comprehensive privacy impact assessment on the OBIM Program; (3) grant individuals Privacy Act rights before collecting additional biometric information; and (4) adhere to international privacy standards.

Respectfully submitted,

Marc Rotenberg, EPIC President and Executive Director
Khaliah Barnes, EPIC Administrative Law Counsel
Christopher Boone, EPIC Law Clerk
Adam Marshall, EPIC Law Clerk

Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue, NW Suite 200
Washington, DC 20009
(202) 483-1140 (tel)
(202) 483-1248 (fax)

[75] European Commission, Proposal for the EU General Data Protection Regulation. European Commission (Jan. 25, 2012).