Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC

Hearing on

"Passport Files: Privacy Protection
Needed For All Americans"

Before the

United States Senate,
Committee on the Judiciary

July 10, 2008
Room 226, Dirksen Senate Office Building
Washington, DC

Mr. Chairman, Members of the Committee, thank you for the opportunity to testify today on the privacy of passport records. My name is Marc Rotenberg and I am Executive Director of the Electronic Privacy Information Center. EPIC is a public interest research organization in Washington, DC. We have a particular interest in the enforcement of the federal Privacy Act and the protection of privacy by federal agencies that collect personal information. We appreciate the work of the Judiciary Committee on these issue and the legislative proposals that have been introduced to help safeguard the privacy rights of Americans.

As recent news stories and the Inspector General's report make clear, the personal information in the passport files of Americans is not adequately protected.[1] More alarming is that the reports of poor privacy controls at the State Department comes at a time when federal agencies are turning over their responsibilities to private contractors and the Administration is pushing to extend data collection and dissemination across the federal government.

It is not simply the passport information of Presidential candidates or celebrities that is at risk; it is the privacy of any person who obtains a state drivers license, works in the federal government, travels across the border to Canada, or seeks employment.

The experience of the passport breaches and the increased information collection efforts at agencies show that new privacy protections are necessary to safeguard the rights of the American public. The Personal Data Privacy and Security Act, S. 495, which has already passed this Committee, would help address the problem. EPIC also recommends limiting employee and contractor disclosures; increasing accounting

[1] *See* EPIC, Passport Privacy, http://epic.org/privacy/travel/pass/.

requirements; and the creation of an independent privacy agency. Further, the State department should be more open about its information security practices.

I. Breaches in the Passport Record System Show That the State Department and Private Contractors Inadequately Protect Personal Information.

Personal information of American citizens in their passport files is inadequately protected. This conclusion is confirmed by the Inspector General. The State Department grants contractors access to citizen's personal information under multimillion dollar contracts, and these contractors have been implicated in these breaches.

The problem of improper access to passport records stretches back at least as far as the 1992 Presidential campaign. Three U.S. State Department officials conducted a search of Presidential candidate William Clinton's passport file during that presidential election. In October 1992, the F.B.I. investigated whether Clinton's passport file was accessed illegally after it was discovered that several pages of his passport file were missing.[2] The State Department concluded that Clinton's file was accessed purposefully to influence the outcome of the presidential election.[3] The investigation led to the resignation of one State Department official and the dismissal of the Assistant Secretary of State for Consular Affairs.

It is because of the 1992 episode that alarm bells literally went off when there was improper access to the passport files of the Presidential canidates earlier this year. In March of 2008, the State Department announced that on three different dates Senator

---

[2] David Johnston, *F.B.I. Investigating Possible Gaps in File On Clinton Passport*, NEW YORK TIMES, October 7, 1992, *available at* http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DC1531F934A35753C1A964958260.

[3] Robert Pear, *State Dept. Official Who Searched Clinton's Passport Files Resigns*, NEW YORK TIMES, November 18, 1992, *available at* http://query.nytimes.com/gst/fullpage.html?res=9E0CE5D71F39F93BA25752C1A964958260.

Obama's passport records were accessed by three different contract employees who had no legitimate reason to access the records.[4] Two of the employees were terminated, while the third was disciplined.[5] Spokesman Sean McCormack stated that the State Department requires all government and contract employees who log onto the system to access passport records to acknowledge "that the records are protected by the Privacy act and that they are only available on a need-to-know basis".[6] Sen. Obama's passport file breach was detected by a monitoring system.[7] The monitoring system is "tripped" when an employee accesses the record of a high-profile individual.[8] Later, the State Department revealed that Senator Clinton and Senator McCain's files had also been improperly accessed.

All three Presidential candidates expressed their concern about the privacy of passport records. Senator Barack Obama said that the breaches were "deeply disturbing" and while he appreciated Condoleeza Rice's apology, he said he expected a "full and thorough investigation". He further said, "One of the things that the American people count on in their interactions with any level of government is that if they have to disclose personal information, that it stay personal and stay private."[9]

Senator Hillary Clinton's office released a statement saying that "Senator Clinton will closely monitor the State Department's investigation into this and the other breaches

---

[4] Teleconference with Patrick F. Kennedy, Under Secretary for Management and Sean McCormack, U.S. Department of State, Spokesman (March 20, 2008), http://www.state.gov/m/rls/102460.htm.
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] Obama urges inquiry into passport snooping" (March 21, 2008), http://us.cnn.com/2008/POLITICS/03/21/obama.passport/index.html#cnnSTCVideo

of private passport information."[10] Senator John McCain said that "If anyone's privacy was is breached, then they deserve an apology and a full investigation. I believe that will take place. . . . The United States of America values everyone's privacy and corrective action should be taken."[11] His office also released a statement: "The U.S. government has a responsibility to respect the privacy of all Americans. It appears that privacy was breached and I expect a thorough review and a change in procedures as necessary to ensure the privacy of all passport files."[12]

The Inspector General's July 2008 Report.

Subsequent to these events, the Inspector General undertook an investigation of improper access to passport files at the State Department. Although the report is heavily redacted, the Inspector General found that 127 politicians, athletes and entertainers' records had been excessively accessed between September 2002 and March 2008.[13] The IG's report founds numerous problems in the system used to protect confidentiality of passport records and made 22 recommendations to improve it.[14] The report further noted a general lack of policies, procedures, guidance, and training regarding the prevention

[10] Statement on Breach of Senator Clinton's Passport File, (March 21, 2008), http://www.clinton.senate.gov/news/statements/details.cfm?id=295036&&.
[11] CNN Video (March 21, 2008), http://www.cnn.com/video/#/video/politics/2008/03/21/america.votes.friday.cnn?iref=videosearch
[12] Helene Coooper, *State Department Investigating Breach of Candidates' Passport Files,* THE NEW YORK TIMES, Mar. 21, 2008, http://thecaucus.blogs.nytimes.com/2008/03/21/state-dept-punishes-aides-for-obama-passport-breach/.
[13] United States Department of State and the Broadcasting Board of Governors Office of Inspector General, *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records Systems (PIERS),* Appendix A, AUD/IP-08-29 (July, 2008), *available at* http://www.govexec.com/pdfs/070308n2.pdf [hereinafter, *OIG Report*].
[14] *Id.* at 4.

and detection of unauthorized access to passport and applicant information.[15] Also, the subsequent response and disciplinary processes taken in response to breaches was found to be inadequate.[16]

II. The Use of Private Contractors at the State Department Contributed to the Privacy Problem.

Part of the problem at the State Department, which is also a problem at other federal agencies, is that the agency turns over its record management responsibilities to private contractors who feel little obligation to protect the privacy interests of Americans. The Department of State hires contract staff to assist with processing passport applications.[17] Contractors assist "government employees by answering customer service enquiries, printing and mailing issued passports, and entering data."[18] Contractors comprised between 40-45% of the total employees at passport agencies and centers since 2001.[19] An estimated 800 of the 2,635 contractors currently work in the National Passport Information Center. Those 800 contractors assist with current applications and are not granted access to the PIERS. [20] In addition, third parties identified as routine users are "allowed access to PIERS based upon agreements with those agencies as to how they will use this data and protect it within the Privacy Act."[21]

The contract employees who gained unauthorized access to the passport files of Senator Obama, Senator Clinton, and Senator McCain were employed by Stanley, Inc.

---

[15] *Id.* at 1-4; *See also id.* at 39-42.
[16] *Id.* at 1-4.
[17] Office of the Department of State Spokesman, "Questions Taken at the March 24, 2008 Daily Press Briefing", March 24, 2008, *available at* http://www.state.gov/r/pa/prs/ps/2008/mar/102569.htm.
[18] *Id*.
[19] *Id*.
[20] *Id.*
[21] *Id*.

and The Analysis Corporation.[22] On March 17, 2008, just days before the public learned of the breaches if passport records, the State Department awarded Stanley, Inc. a five-year $570 million contract to continue to oversee the printing, quality control, and mailing of U.S. passports and other travel documents.[23]

III. Increasing Identification Requirements and Information "Sharing" Initiatives Exacerbate Poor Privacy Protections.

Recent news of poor privacy controls at the State Department comes at a time when Americans are being asked to provide more and more personal information to federal agencies. Security breaches, such as access to passport records at the State Department, are alarming in isolation. However they are much more significant given recent trends to increase identification mandates and information collection and dissemination.

The National Strategy for Information Sharing Increases Privacy Risks.

Over the last several years, the Administration has pursued an aggressive plan for information collection and dissemination across the federal government, but with little regard for privacy protection. In October 2007, the President released the "National Strategy for Information Sharing."[24] The strategy describes information "sharing" between state and local governments, the private sector, and foreign countries. The strategy encourages information sharing related to broad and undefined categories

[22]U.S. Department of State, Daily Press Briefing (March 21, 2008), *available at* http://www.state.gov/r/pa/prs/dpb/2008/mar/102485.htm.
[23] Stanley, Inc. Home Page, "Stanley Awarded $570 Million Contract to Continue Support of Passport Program", http://investor.stanleyassociates.com/phoenix.zhtml?c=198762&p=irol-newsArticle&ID=1119161
[24] The White House, National Strategy for Information Sharing, October, 2007, *available at* http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf.

including "terrorism, homeland security or law enforcement information related to terrorism."[25] Participation in this program is not conditioned on successful implementation of privacy principles. The strategy refers to recently implemented or expanded federal programs that collect citizens' personal information, including the "Information Sharing Environment," fusion centers, a "terrorist screening center," and the "Homeland Security Information Network."[26]

Privacy protections are lacking from this strategy. The strategy declares that information needs of state and local entities will grow as they incorporate homeland security into their day-to-day crime fighting activities.[27] Fusion centers are the "primary focal points" for sharing of terrorism related information.[28] Private sector information sharing focuses on sharing with operators and owners of "critical infrastructure."[29] In receiving foreign information the "guiding objective" is to ensure that the US can disseminate the information "as broadly as possible."[30] Meanwhile, privacy is to be protected by a "Privacy Guidelines Committee" chaired by the Attorney General and the Director of National Intelligence.[31] The committee will consist of the privacy officers of the departments and agencies of the Information Sharing Council.[32]

Basic security and fairness considerations require that increased personal data collection must be balanced by strong privacy safeguards. As the federal government collects and shares more personal data, it increases the risk that Americans' privacy will

[25] *Id*. at 27.
[26] *Id*. at 7-8,
[27] *Id.* at 17.
[28] *Id.* at 20.
[29] *Id.* at 21.
[30] *Id.* at 25.
[31] *Id.* at 28.
[32] *Id.*

be breached by snoops, identity thieves, or others. Greater collection also increases the damage that results from privacy violations. Breaches involving large amounts of personal information are generally greater threats than those concerning smaller amounts of data. Recent federal surveillance efforts have increased the likelihood that an American will become a victim of a privacy breach, and heightened the risks associated with a breach. These measures have not been accompanied by stronger privacy protections.

Increasing Requirements for Americans to Use Passports and Other Identification Documents Exacerbate Poor Privacy Protections.

Increasing requirements for individuals to use identification systems should be matched by increasing privacy safeguards for these systems. The Intelligence Reform and Terrorism Prevention Act required the Department of Homeland Security to enact requirements for a passport or other document denoting citizenship for all travel into the United States by American citizens.[33] Homeland Security subsequently created the Western Hemisphere Travel Initiative.[34] Air travelers were required to present a passport or secure travel documents beginning on January 23, 2007.[35] Land and Sea entry requirements will be fully implemented by June 2009.[36] These requirements have led to

[33] Pub. L. No. 108-458, § 7209(b), 108 Stat. 3637, 3823
[34] Department of Homeland Security, Western Hemisphere Travel Initiative, http://www.dhs.gov/xprevprot/programs/gc_1200693579776.shtm.
[35] Department of Homeland Security, *Documents Required for Travelers Departing From or Arriving in the United States at Air Ports-of-Entry From Within the Western Hemisphere*, 71 Fed. Reg. 68411 (Nov. 24, 2006) (to be codified at 8 CFR Parts 212 and 235; 22 CFR Parts 41 and 53).
[36] Department of Homeland Security, *Documents Required for Travelers Departing From or Arriving in the United States at Sea and Land Ports-of-Entry From Within the Western Hemisphere*, 73 Fed. Reg. 18383 (April 3, 2008) (to be codified at 8 CFR Parts 212 and 235; 22 CFR Parts 41 and 53).

an increase in the demand for passports[37] and should be matched by an increase in passport privacy.

The REAL ID Act increases the requirement for driver's licenses and indirectly increases the demand for the use of passports. The REAL ID Act sets minimum standards for driver's licenses for federal purposes.[38] A passport can be used to meet one of these standards for getting a driver's license. [39] Further, DHS Secretary Michael Chertoff has advised that a passport will serve the same federal purposes as a REAL ID compliant driver's license.[40] These increased identification requirements should be matched by increased privacy protections.

IV. Strong Privacy Protections are Needed to Reduce Privacy Risks.

The experience of the passport breaches and the increased information collection efforts at agencies show that several new privacy protections are necessary. The use of contractors and permissive disclosures threaten privacy, and these should be curtailed. Stronger accounting within agencies will help to detect and investigate breaches. These recommendations improve on the ones made by the Inspector General. Further, the creation of an independent privacy authority will improve privacy protections.

The Federal Privacy Act Is Undermined by The Use of Contractors.

---

[37] Molly Hennesy-Fiske, *Federal Officials Admit They Weren't Ready for High Passport Demand*, LOS ANGELES TIMES, June 20, 2007, *available at* http://travel.latimes.com/articles/la-trw-passports20jun20.

[38] Pub. L. No. 109-13, 119 Stat. 231 (2005).

[39] Department of Homeland Security; *Minimum Standards for Drivers Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes: Final Rule*, 73 Fed. Reg. 5271, 5333 § 37.11(c)(1)(i) (Jan 29, 2008).

[40] Department of Homeland Security, *Remarks by Homeland Security Secretary Michael Chertoff at a Press Conference on REAL ID*, (Jan 11, 2008), http://www.dhs.gov/xnews/speeches/sp_1200320940276.shtm.

A specific purpose of the Privacy Act is that data collectors should provide adequate safeguards for personal information that they have collected. When Congress enacted the Privacy Act in 1974, it declared that:

> The Purpose of this act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal Agencies, except as otherwise provided by law, . . . (4) to collect, maintain, use or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that *adequate safeguards are provided to prevent misuse of such information*.[41]

In line with this purpose, agencies are required to:

> establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.[42]

These mandates are undermined when agencies allow contractors to operate and access systems of records. The Privacy Act requires the agency to cause a contractor to follow the obligations of the Privacy Act.[43] The Privacy Act requirements apply "when an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function."[44] For the purposes of the criminal liability provisions, employees of the contractor are considered to be agency employees.[45]

Contractors are less accountable to agency oversight. The OIG recommended determining the feasibility of guidelines to discipline those engaged in unauthorized

[41] Pub. L. No. 93-579, § 2(b), 88 Stat. 1896 (1974).
[42] 5 U.S.C. § 552a (e)(10).
[43] 5 U.S.C. § 552a (m).
[44] *Id.*
[45] *Id.*

access, including contractors and outside agencies.[46] Bureaus within the department disagreed, stating that they had no jurisdiction to engage in disciplinary action against outside agencies and contractors.[47]

Broad disclosures Within Agencies and to Contractors Undermine Privacy Act Purposes.

Limiting agency disclosures will limit the risk of unauthorized access and other data breaches. Routine use and other disclosure rules allow broad access by contractors and agency employees. The Privacy Act permits disclosures to be made according to "routine uses."[48] The only requirements are that the disclosure of the record be "for a purpose which is compatible with the purpose for which it was collected"[49] and that a description of the disclosure be published in the Federal Register.[50] For its passport system, the State Department permits routine use disclosures of passport information to "contractor personnel conducting data entry, scanning, corrections and modifications."[51] This effectively gives contractors access to read and edit personal information in the passport system of records.

The Government Accountability Office has recently reported on how broad disclosures, including "routine use" definitions by agencies may undermine the Privacy Act's goals to limit uses to specified purposes.[52] The report notes:

---

[46] *OIG Report*, *supra* note 13, at 30.
[47] *OIG Report*, *supra* note 13, at 30-31.
[48] 5 U.S.C. § 552a (b)(3).
[49] 5 U.S.C. § 552a (a)(7).
[50] 5 U.S.C. § 552a (e)(4)(D).
[51] Department of State; *Privacy Act of 1974; System of Records*, 73 Fed. Reg. 1660, 1662 (January 9, 2008).
[52] Government Accountability Office, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 (May 2008).

> According to generally accepted privacy principles of purpose specification, collection limitation and use limitation principles, the collection of personal information should be limited and its use should be limited to a specified purpose. Yet current laws and guidance impose only modest requirements for describing the purposes for collecting and using personal information, and limiting how that information is collected and used.[53]

The Privacy Act permits wide disclosure of records within Agencies. Disclosure is permitted "to those officers and employees of the agency . . . who have a need for the record in the performance of their duties."[54] The GAO calls these only "modest limits" on the use of information for multiple purposes within an agency.[55] Wide disclosures within agencies undermine privacy protections by making unauthorized disclosures more likely. For example, State Department officials described trainees as having access to production data, rather than a dummy training records.[56] Officials also described that trainees are recommended to look up their relatives during training -- it was during one of these lookups that a trainee viewed Hillary Clinton's information.[57] These are unnecessary disclosures of information, which go beyond the purpose for which passport records are collected.

EPIC recommends that these disclosures be limited to those that are "for the purposes for which the data was collected." Such a limit would prevent trainee uses of data. More importantly, limiting disclosure limits the risk of a data breach and unauthorized disclosures because it limits the potential sources of breaches. For example, the Federal Communications Commission recently tightened the rules under which

---

[53] *Id.* at 5.
[54] 5 U.S.C. § 552a (b)(1).
[55] Government Accountability Office, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536, 39 (May, 2008).
[56] U.S. Department of State, Daily Press Briefing (March 21, 2008), *available at* http://www.state.gov/r/pa/prs/dpb/2008/mar/102485.htm.
[57] *Id.*

telecommunications companies could share customer records with joint venture and independent contractors.[58] The FCC specifically noted that the risk of breaches increases when new parties gain access to personal information.[59] Once there has been a disclosure of data, the collector "no longer has control over it and thus the potential for loss of this data is heightened."[60]

Stronger Accounting Helps to Detect, Prosecute Unauthorized Access.

Congress should require accounting for all record access. Audit trails help to investigate breaches as well as serve as the raw data that can proactively detect misuse. While investigating the passport database, the OIG found "many control weaknesses -- including a general lack of policies, procedures, guidance and training -- relating to the prevention and detection of unauthorized access to passport and applicant information …."[61] More robust accounting requirements could have prevented and detected the breaches in the passport records.

The Privacy Act requires that accounting be made which includes the "date nature and purpose of each disclosure" and the "name and address of the person or agency to whom the disclosure is made."[62] Excepted from this accounting are disclosures made under § 552a(b)(1) -- "to those officers and employees of the agency which maintains the records who have a need for the record in the performance of their duties."[63] This

---

[58] *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carrier's Use of Customer Proprietary Network Information and Other Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115, WC Docket No. 04-36, 22 (March 13, 2007) *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf.
[59] *Id.* at 25.
[60] *Id.* at 23.
[61] *OIG Report*, *supra* note 13, at 1.
[62] 5 U.S.C. § 552a (c)(1).
[63] 5 U.S.C. § 552a (c)(1) (excepting disclosures made under § 552a (b)(1)).

significant gap in accounting means that misuse goes undetected, and breaches are difficult to investigate. The OIG found that while the passport system logged user access, it did not log what activities were conducted or why the system was being accessed.[64] Further, the OIG found that this data is accessed via a Consular Consolidated Database web portal by other agencies.[65] The report did not indicate whether this access was appropriately accounted.

EPIC recommends that robust accounting requirements be applied to intra-agency disclosures. The exception for (b)(1) disclosures in § 552a(c)(1) should be removed.

OIG Recommendations Are Insufficient to Protect Privacy.

The OIG's recommendations do not go far enough to protect personal privacy, neither in the State Department nor throughout the federal government. Clear mandates are necessary, and limits on disclosure and tougher accounting will protect privacy better than more detailed information sharing agreements.

The OIG review focused on the unauthorized access of passport data and the response to incidents of unauthorized access.[66] After redactions, 6 of 22 recommendations made by OIG remained accessible to varying degrees.[67] In the 6 visible recommendations, the OIG made recommendations that the CA "consider," "determine the feasibility of," and "evaluate"[68] potential programs and policy amendments without specifics or mandates. Clear agency mandates which are effectively implemented are needed to protect privacy beyond these recommendations.

[64] *OIG report*, *supra* note 13, at 32.
[65] *Id.* at 33.
[66] *Id.*
[67] *Id.* at 40-42.
[68] *Id.*

Other recommendations include items such as evaluating the accuracy of Privacy Impact Assessments;[69] conducting vulnerability and risk assessments;[70] addressing third party disclosure and breaches;[71] and altering the agreements with agencies and entities that access PIERS data.[72] These recommendations have not yet been implemented. They do not address the root cause of the privacy problem -- that too many individuals have access to data and that insufficient systems detect improper access.

Further, these recommendations only affect the Department of State. Changes in federal law would broadcast these changes throughout the federal government.

Creation of an Independent Privacy Authority Will Improve Privacy Protections.

Improved privacy protection will be achieved by the creation of an independent privacy agency. Such an entity would have the authority and the expertise to ensure that agencies are complying with the Privacy Act and to help agencies anticipate new challenges involving rapidly changing technology and privacy issues. The organization should be independent of the executive branch. The correct model would be an independent agency, similar to the Federal Trade Commission or the Federal Communications Commission.

In 1973 the Department of Health, Education and Welfare established a special panel to study privacy issues arising from the growing use of automated date processing equipment.[73] That report led to the development and passage of the Privacy Act of

---

[69] *Id.* at 33.
[70] *Id.* at 34.
[71] *Id.* at 37.
[72] *Id.* at 36-7.
[73] US Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens*, (July 1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm.

1974.[74] But that report also made clear that the cornerstone of an effective federal policy is a permanent privacy agency.[75]

In countries across the world, efforts are underway to address these privacy concerns. The European Union has implemented extensive privacy directives that establish legal rights for all citizens in the European Union countries.[76] Non-EU countries, from Canada[77] to Hong Kong,[78] are pursuing comprehensive privacy agendas led by privacy agencies. These government agencies routinely report on the handling of privacy complaints,[79] the emergence of new privacy issues, and proposed measures to protect privacy. These reports help the public and the government understand the status of privacy protection in their country and develop new approaches to replace old ones.

But there is still no privacy agency in the United States. In many respects, this is surprising. It is clear that the absence of a privacy agency in the federal government remains a critical problem. Having announced numerous programs that hinge on the collection and dissemination of Americans' personal information, some institutional balance must be established to ensure that these proposals receive adequate review. This would be a small investment in what many Americans consider their number one concern about our nation's infrastructure – the protection of personal privacy.

The State Department Should be More Open About Its Information Security Practices.

---

74 5 U.S.C. § 552a (1974).
75 HEW Report, *supra* note 73, at § 3.
76 European Commission, Data Protection – European Commission, http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.
77 Office of the Privacy Commissioner of Canada, Mandate and Mission of the OPC, http://www.privcom.gc.ca/aboutUs/index_e.asp.
78 Office of the Privacy Commissioner for Personal Data, Hong Kong, Homepage, http://www.pcpd.org.hk/.
79 Office of the Privacy Commissioner of Canada, http://www.privcom.gc.ca/i_i/index_e.asp.

The OIG should remove the redactions in its report due to substantial interest that citizens have in the security of their passport information. Several recommendations in the report are redacted under FOIA exemption 2. Exemption 2 allows agencies to withhold information that is "related solely to the internal personnel rules and practices of an agency."[80] The recommendations the OIG has made relate also to security of the personal information in passport records, not "solely for internal personnel rules and practices of an agency." The purpose of Exemption 2 is to "relieve agencies from the burden of assembling and maintaining for public inspection matter in which the public could not reasonably be expected to have an interest."[81] Exemption 2 can be overcome if the documents in question relate to "substantial matters which might be the subject of legitimate public interest".[82]

The relevant Exemption 2 test for this report is the "High 2," examining whether the disclosure risks circumvention of agency regulations and statutes. This standard was established in *Founding Church of Scientology of Wash. v. Smith*, where the court held, "[i]f withholding frustrates legitimate public interest, however, the material should be released unless the government can show that disclosure would risk circumvention of lawful agency regulation."[83] In *Crooker v. Bureau of Alcohol, Tobacco & Firearms*, the court held "[t]here can be little doubt that citizens have an interest in the manner in which they may be observed by federal agents."[84] In the case of electronic passport records, the files can be accessed not only by government employees, but also private contractors.[85]

---

[80] 5 U.S.C. § 552 (b)(2).
[81] *Dep't of Air Force v. Rose*, 425 U.S. 352, 369-370 (1976).
[82] *Id.* at 365.
[83] *Founding Church of Scientology of Wash. v. Smith*, 721 F.2d 828, 831 (D.C. Cir. 1983).
[84] *Crooker v. Bureau of Alcohol, Tobacco & Firearms,* 635 F.2d 887, 888 (D.C. Cir. 1980).
[85] *OIG Report*, *supra* note 13, at 1.

The Inspector General's report on the breaches of State Department passport files qualifies as the subject of a legitimate public interest, yet most of the "Results" sections of the IG's report was withheld under Exemption 2. This section is highly relevant to the public because it details exactly what kinds of breaches were discovered and how prevalent these breaches are. This information is similar to the information in *Dep't of Air Force v. Rose*. In *Rose*, the Supreme Court considered whether Exemption 2 applied to case summaries of hearings concerning violations of the Air Force Academy's Honor and Ethics code.[86] The Court ruled that, although the summaries clearly related to internal personnel matters, the public's interest in the integrity of its armed forces removed this information from the category of matters of internal significance.[87] In the case of passport records, the public's interest in the security of personal information and State Department compliance with the Privacy Act, is certainly as important.

The PIERS database contains records on 192 million passport files of 127 million passport holders,[88] and because these records can be viewed without automatic internal agency notification, the potential security breaches constitute a legitimate privacy and security concern for the public. According to the executive summary of the report, the passport records contain personally identifiable information, including the applicant's name, gender, social security number, date and place of birth, and vital records.[89] Unauthorized access to this information creates a high risk for the public, and the report describes a multitude “weaknesses and data vulnerabilities” in the PIERS system.[90]

---

[86] *Dep't of Air Force v. Rose*, 425 U.S. 352 (1976).
[87] *Id.*
[88] *OIG Report*, *supra* note 13, at 1.
[89] *Id*.
[90] *Id*. at 33.

It is our recommendation that the Inspector General release a more complete report, with, at a minimum, the titles of each of the individual recommendations so that the public can adequately gauge their effectiveness in protecting privacy.

V. Need for Comprehensive Privacy Legislation.

The problems with passport records are not unique to the State Department. Across the federal government, there are growing risks to personal privacy. Technology has marched and left the law behind. But the protection of privacy remains a central concern for Americans as it was for the Presidential candidates who learned that their personal information, which they were required to provide to the federal government, had been improperly accessed by private contractors.

It is for this reason that EPIC strongly supports passage of S. 495, the Personal Data Privacy and Security Act. This Act would effectively handle this problem by putting in place high standards for business entities that deal with sensitive personally identifiable information. These standards and practices would assist in prevention and disciplinary action in situations like the passport information breach. One of the most relevant provisions requires that the entity "adopt measures that… detect actual and attempted… unauthorized access… of sensitive personally identifiable information, including by employees and other individuals otherwise authorized to have access."[91] This provision and the institution of the program as a whole directly provide for prevention and detection that did not exist at the State Department at the time of the passport breaches.

[91] S. 495, 110th Cong. § 302(4)(B)(ii).

Disciplinary action, the other issue brought up by the OIG, is provided for in § 303, Enforcement, which provides for penalties for offending entities. Although the bill does not address disciplinary actions against specific employees, it allows for penalties of up to $1 million per intentional violation.[92] This provides incentives to these organizations to prevent violations and enact disciplinary measures against employees who put the entities in danger of liability.

The bill also addresses contractor relationships, one of the major issues in the passport breaches. Under the provisions in § 401, the data privacy and security programs of potential contractors, as well as any history of breaches and their response to such breaches, would be evaluated by the government before any contracts would be awarded. Additionally, § 402 provides for evaluation and auditing of contractors already affiliated with government agencies. These provisions would ensure that government agencies, which often retain some of the most sensitive personally identifiable information about US persons, would only contract with and allow access to this information to entities that have proven their commitment to the high standards required by the other portions of the Act.

Finally, § 331 of the bill provides for the creation of a new office in the Federal Trade Commission called the Office of Federal Identity Protection. This office would assist consumers in prevention of identity theft and personal privacy information violation as well as providing assistance after a violation has occurred. Requiring the FTC to "help consumers restore their stolen or otherwise compromised personally identifiable information quickly and inexpensively,"[93] not only serves those betrayed by

[92] *Id*. at § 303(a).
[93] *Id*. at § 331(c)(9)

entities who have failed to meet the requirements of the Act, but also provides incentive to the FTC to see to the strict enforcement of the Act thus minimizing the cost of operating the Office of Federal Identity Protection.

We understand that the Committee has already reported this bill favorably. We hope the full Senate will move quickly on S. 495 so that it can become law this year. Further delay, particularly in light of the recent problems at the State Department and other similar incidents, leaves the privacy of all Americans at risk.

VI. Conclusion.

Recent news of poor privacy controls at the State Department comes at a time when Americans are being asked to provide more of their personal information to federal agencies and to produce more identification documents. The experience of the passport breaches and the increased information collection efforts make clear that new privacy protections are necessary. EPIC recommends limiting employee and contractor disclosures; increasing accounting requirements; and the creation of an independent privacy agency. Further, the State Department should be more open about its information security practices. Finally, EPIC supports passage of S. 495, the Personal Data Privacy and Security Act.

Thank you again for the opportunity to appear before the Judiciary Committee today. I will be pleased to answer your questions.