

**PASSPORT FILES: PRIVACY PROTECTION NEEDED  
FOR ALL AMERICANS**

---

---

**HEARING**  
BEFORE THE  
**COMMITTEE ON THE JUDICIARY**  
**UNITED STATES SENATE**  
**ONE HUNDRED TENTH CONGRESS**

SECOND SESSION

---

JULY 10, 2008

---

**Serial No. J-110-105**

---

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

44-368 PDF

WASHINGTON : 2008

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

|                                  |                                   |
|----------------------------------|-----------------------------------|
| EDWARD M. KENNEDY, Massachusetts | ARLEN SPECTER, Pennsylvania       |
| JOSEPH R. BIDEN, Jr., Delaware   | ORRIN G. HATCH, Utah              |
| HERB KOHL, Wisconsin             | CHARLES E. GRASSLEY, Iowa         |
| DIANNE FEINSTEIN, California     | JON KYL, Arizona                  |
| RUSSELL D. FEINGOLD, Wisconsin   | JEFF SESSIONS, Alabama            |
| CHARLES E. SCHUMER, New York     | LINDSEY O. GRAHAM, South Carolina |
| RICHARD J. DURBIN, Illinois      | JOHN CORNYN, Texas                |
| BENJAMIN L. CARDIN, Maryland     | SAM BROWNBACK, Kansas             |
| SHELDON WHITEHOUSE, Rhode Island | TOM COBURN, Oklahoma              |

BRUCE A. COHEN, *Chief Counsel and Staff Director*

STEPHANIE A. MIDDLETON, *Republican Staff Director*

NICHOLAS A. ROSSI, *Republican Chief Counsel*

# CONTENTS

## STATEMENTS OF COMMITTEE MEMBERS

|                                                                                                 | Page |
|-------------------------------------------------------------------------------------------------|------|
| Feingold, Hon. Russell D., a U.S. Senator from the State of Wisconsin, prepared statement ..... | 43   |
| Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont .....                          | 1    |
| prepared statement .....                                                                        | 52   |
| Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania .....                        | 3    |

## WITNESSES

|                                                                                                        |    |
|--------------------------------------------------------------------------------------------------------|----|
| Duda, Mark W., Assistant Inspector General for Audits, Department of State, Washington, D.C. ....      | 6  |
| Geisel, Harold W., Ambassador and Acting Inspector General, Department of State, Washington, D.C. .... | 4  |
| Raul, Alan Charles, Partner, Sidley Austin, LLP, Washington, D.C. ....                                 | 17 |
| Rotenberg, Marc, Executive Director, Electronic Privacy Information Center, Washington, D.C. ....      | 13 |
| Schwartz, Ari, Vice President, Center for Democracy & Technology, Washington, D.C. ....                | 15 |

## QUESTIONS AND ANSWERS

|                                                                                                    |    |
|----------------------------------------------------------------------------------------------------|----|
| Responses of Ambassador Geisel to questions submitted by Senators Specter, Leahy and Kennedy ..... | 21 |
| Responses of Alan Charles Raul to questions submitted by Senator Specter ....                      | 27 |
| Responses of Marc Rotenberg to questions submitted by Senators Specter and Feingold .....          | 31 |
| Responses of Ari Schwartz to questions submitted by Senators Feingold and Specter .....            | 36 |

## SUBMISSIONS FOR THE RECORD

|                                                                                                                    |    |
|--------------------------------------------------------------------------------------------------------------------|----|
| Duda, Mark W., Assistant Inspector General for Audits, Department of State, Washington, D.C., statement .....      | 38 |
| Geisel, Harold W., Ambassador and Acting Inspector General, Department of State, Washington, D.C., statement ..... | 45 |
| Kennedy, Patrick F., Under Secretary of State for Management, Department of State, Washington, D.C., letter .....  | 50 |
| Raul, Alan Charles, Partner, Sidley Austin, LLP, Washington, D.C., statement .....                                 | 54 |
| Rotenberg, Marc, Executive Director, Electronic Privacy Information Center, Washington, D.C., statement .....      | 57 |
| Schwartz, Ari, Vice President, Center for Democracy & Technology, Washington, D.C., statement .....                | 79 |



## **PASSPORT FILES: PRIVACY PROTECTION NEEDED FOR ALL AMERICANS**

**THURSDAY, JULY 10, 2008**

U.S. SENATE,  
COMMITTEE ON THE JUDICIARY,  
*Washington, D.C.*

The Committee met, pursuant to notice, at 10:03 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Cardin, and Specter.

### **OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT**

Chairman LEAHY. Good morning. Today, the Committee is going to hold an important hearing on the unauthorized access of Americans' passport files. Millions of Americans, including, I expect, every member of this Committee, entrust their personal information to the State Department in order to obtain passports and other services. We give a great deal of information, but we trust our Government to protect the private information of its citizens. But, sadly, the State Department has failed to honor this duty. They have left millions of ordinary Americans vulnerable to not only privacy violations but to identity theft that could come from that and other crimes.

Now, last week—while Americans were celebrating Independence Day—the State Department's Acting Inspector General issued a report finding that State Department workers and contractors repeatedly accessed the passport files of entertainers, athletes, and other high-profile Americans without proper authorization. Now, I do not care whether it is a well-known person or someone we have never heard of. Either way it is wrong. And this revelation of passport snooping comes after press reports in March that the passport files of three Presidential candidates—Senators Obama, Clinton, and McCain—were improperly accessed. Somebody running for office, as they do, give up enough of their privacy as it is. They ought to be able to count on their own Government protecting it.

The Inspector General's findings raise serious concerns about possible violations of the Privacy Act and other Federal laws. And according to the report, 85 percent of the passport records included in a sample of high-profile Americans had been searched at least once—and many files were searched multiple times—during a 5½-year period. In fact, one individual's passport records were searched 356 different times by 77 different people.

(1)

The Inspector General's report reveals that the records of millions of ordinary Americans are also vulnerable to privacy breaches. There are no checks in the system to even determine if the passport files of the average American are accessed. Now, these files, just so we fully understand, contain name, date and place of birth, and Social Security numbers. As some of the experts on the Internet and data privacy know these are the kinds of facts somebody wants when they want to steal your identity. But the State Department does not have a general lack of policies, procedures, guidance, and training to stop it. According to the report, the Department's Passport Information Electronic Records System—PIERS—contains the passport records for approximately 127 million passport holders. Now that our Government is requiring us to have passports even to go into a friendly country, like Canada, the number of passport files to protect grows.

The State Department could not readily identify the universe of Government workers and contractors who have access to this information. The Inspector General estimates that this figure exceeds 20,000 Government employees from various agencies and outside contractors. We might as well just post this stuff on billboards all over the country. And the tip of the iceberg in this report is the fact that passport information is shared with other agencies, and we have no idea what procedures are followed to protect information once it leaves the State Department. So here, sure, take all this information, bring it back someday. It has got to be better than that. The State Department Inspector General has referred this serious matter to the Justice Department. I made it very clear to the Attorney General yesterday that I hope the Department's Criminal Division will investigate this thoroughly. If criminal violations have occurred, people ought to go to jail.

The lax data security at the State Department is not unique. A week does not go by without reports of personal data privacy breaches at Government agencies and private businesses. Just recently, we had front-page headlines with news about the theft of sensitive medical information from the National Institutes of Health, and earlier reports of data breaches have involved virtually every branch of our Federal Government. I just cannot imagine this. You might as well just open up the files and leave them out on the street corner and say, "Here, help yourself."

The Inspector General's report is just the latest example of why we should have swift action on the Leahy-Specter Personal Data Privacy and Security Act. Senator Specter and I put this together. It is a comprehensive privacy bill that would help to prevent data security breaches and provide further protections in the handling of American's private data. And I hope that the Senate will promptly pass it.

Data privacy and security at our Federal agencies is a serious and growing problem. We have to address it. So we have to understand not only what went wrong at the State Department but elsewhere. And I am glad the Department's Acting Inspector General and Assistant Inspector General for Audits are here to share their findings. And we have a distinguished panel of privacy experts. And then I hope we will end up passing the Leahy-Specter bill.

[The prepared statement of Senator Leahy appears as a submission for the record.]

With that, I will turn to Senator Specter.

**STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA**

Senator SPECTER. Thank you. Mr. Chairman, I commend you on calling this hearing so promptly. The Inspector General's report was issued on July 7th. This is July 10th. That is pretty unusual for an oversight committee to move into a field. But I think the implications of this matter warrant it.

On every turn, we find that privacy is in jeopardy. Yesterday we enacted followup legislation on the Foreign Intelligence Surveillance Act, which goes further than we had in the past. And when you deal with national security, there are very weighty factors. But where you have snoopers, there is absolutely no justification for what they are doing. And, regrettably, when you take a look at all of the snoopers, it is sort of overwhelming.

Just last month, sensitive information on about a thousand patients at Walter Reed Army Medical Center exposed a security breach. Last year, thieves stole a Transportation Security Administration computer containing information on some 100,000 current and former employees. The Department of Agriculture 2 years ago exposed 26,000 employees, contractors, and retirees to an invasion of privacy. Also in 2006, hackers stole data from the Defense Department system on 14,000 active-duty and retired servicemembers' independents. And the list goes on and on. There is obviously a great interest in personalities and high-profile people, but we have to do something very forceful to stop it.

I was intrigued by one of the statistics in the IG's report, Inspector General's report, that the records of one individual were accessed a total of 356 times by 77 users between 2002 and 2008. I would like to know who that was. Maybe I would be interested in that myself.

[Laughter.]

Senator SPECTER. There must be something very fascinating, perhaps even lurid, about that particular individual.

But one of the great values in our society is privacy, and vigilance is the cost of being effective at protecting it. So I am glad to see our Committee moving ahead, Mr. Chairman, and I am glad to cooperate with you in expediting this important hearing.

Chairman LEAHY. Well, it would be impossible to move forward on this without you, and you have been so good on the privacy bill. You know, in Vermont, we tend to respect our privacy a great deal, and I will put this story in perspective. I live on a dirt road, an old 1850s farmhouse we have had for over 50 years, a lot of land, fields, and whatnot. And adjoining farmers hayed the fields and so on since I was a teenager. And this was a story in the New York Times. It is the only thing I think was ever written about me that I have actually saved, even framed, and it goes almost this way.

It was a Saturday morning. A little farmer was standing on the porch. A reporter in an out-of-State car pulls up and says, "Does Senator Leahy live up this road?" He said, "Are you a relative of his?" He said, "No. No, I am not." He said, "Well, are you a friend

of his?” “Well, not really.” “Is he expecting you?” “No.” “Never heard of him.”

[Laughter.]

Chairman LEAHY. So we love our privacy.

Senator SPECTER. Well, Senator Leahy, as I understand it, the “fahrm”—also know as the “farm”—is expansive enough so that you can hide.

Chairman LEAHY. That it is.

We are fortunate this morning. Our first witness is Ambassador Harold Geisel. Ambassador Geisel currently serves as the Acting Inspector General for the Department of State. He assumed the duties of Deputy Inspector General for the Department of State and the Broadcasting Board of Governors in June of this year. He is a career Department of State foreign service officer. He has dedicated more than 20 years to the Department. In 1994, Ambassador Geisel was assigned as Acting Inspector General of the State Department. He held the position of Deputy Assistant Secretary of State for Information Management from 1995 to 1996, during which he directed the development of the Department’s first IT strategy plan. He served as our Ambassador to Mauritius in 1996 to 1999, received his bachelor’s degree in liberal arts from Johns Hopkins University and his master’s degree in finance from the University of Virginia. And I saw Senator Cardin of Maryland smile when I mentioned Johns Hopkins.

Please go ahead, Ambassador.

**STATEMENT OF AMBASSADOR HAROLD W. GEISEL, ACTING INSPECTOR GENERAL, DEPARTMENT OF STATE, WASHINGTON, D.C.**

Ambassador GEISEL. Chairman Leahy, Ranking Member Specter, Senator Cardin, thank you for inviting me to discuss with you the privacy concerns reported in the results of our review of controls over access to passport records in the Department of State’s Passport Information Electronic Records System, or PIERS. The full report has been provided to the Committee.

In March 2008, media reports surfaced that the passport files maintained by the Department of State of three U.S. Senators, who were also Presidential candidates, had been improperly accessed by Department employees and contractors. On March 21, 2008, the Office of Inspector General, Office of Audits, initiated a review of Bureau of Consular Affairs controls over access to passport records and issued the final report 1 week ago, on July 2nd. The OIG made 22 recommendations to address the control weaknesses, and the Department concurred with 19 of them, partially agreed with one, and did not agree with two recommendations.

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 and the subsequent response and disciplinary processes when a potential unauthorized access is substantiated.

As of April 2008, PIERS contained records on about 192 million passports for about 127 million passport holders. These records include personally identifiable information, or PII, as it is known, such as the applicant’s name, gender, Social Security number, date

and place of birth, and passport number. PIERS also contains additional information, such as previous names used by the applicant, citizenship status of the applicant's parents or spouse, and scanned images of passport photos. PIERS offers users the ability to query information pertaining to passports and vital records, as well as to view and print original copies of the associated documents. As a result, PIERS records are protected from release by the Privacy Act of 1974. Unauthorized access to PIERS records may also constitute a violation of the Computer Fraud and Abuse Act.

At the time of the publicized breaches, neither Consular Affairs nor the Department had implemented breach notification policies, procedures, or other criteria for reporting incidents of unauthorized access of passport records when they were detected. However, between March and May 2008, Consular Affairs and the Bureau of Administration took a number of corrective actions, including issuing interim guidance on the various steps to be followed and decisions to be made in response to a potential incident of unauthorized access to passport records and applicant personally identifiable information, and they issued a Department-wide PII breach response policy.

While these immediate actions taken are commendable, OIG has recommended that the Department conduct the necessary vulnerability and risk assessments of all passport systems given the weaknesses and data vulnerabilities identified in this review of PIERS. Accordingly, OIG believes that the Department should make resources available to conduct the assessments as quickly as possible.

OIG also recommended that CA ensure the accuracy of its Privacy Impact Assessments for PIERS and for all other passport systems to accurately reflect security controls for and risks to personally identifiable information.

I would like to introduce Mr. Mark W. Duda, Assistant Inspector General for Audits, who led this review, and he will provide a summary of the findings.

Thank you for the opportunity to present this timely information to you today. Following Mr. Duda's remarks, we would be happy to answer any questions you may have.

[The prepared statement of Ambassador Geisel appears as a submission for the record.]

Chairman LEAHY. Thank you, Ambassador. And, of course, Mr. Duda, prior to being at the Department of State, was senior evaluator in the Department of Treasury Office of Inspector General, as well as auditor in charge at the Smithsonian Institution's Office of Inspector General. And, Senator Cardin, you will be interested in known he received a bachelor of science degree in accounting from the University of Maryland and a master of business administration from the University of Baltimore.

Senator CARDIN. I am glad to see that we are getting the best talent in the Nation working for us.

[Laughter.]

Chairman LEAHY. Mr. Duda, why don't you go ahead, and then we will start with the questions.

**STATEMENT OF MARK W. DUDA, ASSISTANT INSPECTOR GENERAL FOR AUDITS, DEPARTMENT OF STATE, WASHINGTON, D.C.**

Mr. DUDA. Chairman Leahy, Ranking Member Specter, members of the Committee, thank you for the opportunity to discuss the results of our review of controls over access to passport records in the Department of State's Passport Information Electronic Records System, which is also known as PIERS. I will be referring to that acronym periodically.

On March 21, 2008, following the first reported breach of a Presidential candidate's passport records and at the direction of the former Acting Inspector General, the Office of Inspector General, Office of Audits, initiated this review of the Bureau of Consular Affairs controls over access to passport records in PIERS. Specifically, this review focused on determining whether the Department: one, adequately protects passport records and data contained in PIERS from unauthorized access; and, two, responds effectively when incidents of unauthorized access do occur.

During fiscal year 2007, the Department issued about 18.4 million passports domestically and participated or assisted in the issuance of about 365,000 passports overseas.

According to Consular Affairs officials, there were about 20,500 users with active PIERS accounts as of May 2008, and about 12,200 of these users were employees or contractors of the Department. PIERS is also accessed by users at other Federal departments and agencies, including the Department of Homeland Security, the Federal Bureau of Investigation, and the Office of Personnel Management, to assist in conducting investigations, security assessments, and analyses.

In our review, 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 and the subsequent response and disciplinary processes when a potential unauthorized access is substantiated.

In some cases, Department officials stated that the lack of resources contributed to the lack of controls and to the Department's ability to assess vulnerabilities and risk. OIG described some security and management practices utilized by both the Internal Revenue Service and the Social Security Administration as examples where similar improvements could be made by the Department.

OIG made 22 recommendations to address the control weaknesses found with safeguarding passport records. We did not verify instances of unauthorized access, but we did conduct a judgmentally determined study to identify the frequency with which the records for 150 high-profile individuals were accessed in PIERS between September 2002 and March 2008. Our results revealed several patterns that raised serious concerns about the potential for undetected unauthorized access to passport records. Of the 150 names included in the study, OIG found that the records of 127 individuals, or 85 percent, had been accessed at least one time. The results showed a total of 4,148 hits to the passport information for these 150 individuals. OIG made no determination as to whether the hits represented authorized or unauthorized access.

Additionally, although an 85-percent hit rate appears to be excessive, the Department currently lacks any criteria to determine whether this is an unusually high rate.

As stated by the Acting Inspector General, following the publicized passport record breaches, the Department implemented a number of corrective actions and has other efforts planned, as we have detailed in the report.

Based on the responses from Department officials, of the 22 recommendations made the Department has agreed with 19 of those recommendations; they partially agree with one recommendation; and they disagreed with two recommendations. To ensure adequate and timely action, OIG will conduct a full compliance followup review of the Department's implementation of the recommendations in this report, as well as Consular Affairs' process for reviewing possible unauthorized accesses by users as identified in our study.

Thank you for the opportunity to appear before you today. I would be happy to answer any questions you have.

[The prepared statement of Mr. Duda appears as a submission for the record.]

Chairman LEAHY. Well, thank you. As I sort of indicated before, I will start with you, Ambassador. I know the State Department has placed a number of celebrities on a special watchlist, and dignitaries watch out for that. I am just as concerned by the person we do not know the name of who lives down the street, works in a store, or whatever else, because they have also given all this information up. And it is one thing with a watchlist. They are not on that watchlist. Isn't it virtually impossible to know if the passport files of ordinary American citizens have been improperly accessed?

Ambassador GEISEL. Senator, that is really the key question. The answer is we have the ability to know if they have been accessed. We do not at this time know if they have—whether the access is authorized or unauthorized, and a crucial part of our recommendations is that we have to know that.

Chairman LEAHY. Yes, because it is one thing to go and look back and say, OK, pick out passport number 2936000 or whatever and find that. But I am thinking of—for example, if somebody wants to—well, I will check on my neighbor or my former boyfriend or girlfriend, or somebody may have a more nefarious thing, I want to get this information, I know where this person lives, they are fairly wealthy, I want to get this information and sell it to somebody who will probably pay a lot of money for it because they are going to use it to clean out their bank account. I mean, there is nothing to ring alarm bells when that happens. Is that correct?

Ambassador GEISEL. As it stands right now, Senator, that is absolutely correct, and that is why I think one of our most important recommendations is that the Department take a look at software that does work, such as is used currently by the Internal Revenue Service or the Social Security Administration.

Chairman LEAHY. And we know in the past that the Internal Revenue Service had a problem with this. People were looking at the tax returns of movie actors and all, and usually it was just because it is kind of fun to find out. But if they can do that, they can also get the person who runs the local grocery store.

Mr. Duda, the State Department has brought in a lot of contractors for this surge capacity in processing passport applications, especially when it decided that our neighbor to the north, Canada, the most friendly country we have ever been involved with, poses such a threat that we have all got to start having passports to go there. That is a political comment to the aside only because I think the policy is ridiculous. But as a result, a lot of outside people were hired.

Is there a greater vulnerability to snooping if you are using outside contractors because you do not have the kind of leverage that you might have in the State Department? If you find a State Department employee doing it, they can be disciplined. They can be fired. They can be whatever else. But is there greater concern because we have had to rely so much on outside contractors?

Mr. DUDA. There could be, but there are actually controls you can put in place. Obviously, if the Department is soliciting the services of a contractor, they are entering into a contract with a vendor, you know, the Department is paying the vendor. The Department writes the contracts. The Department can put whatever, you know, is legally feasible into a contract. And one of the things that can be put in the contracts is adequate controls to ensure that contractors have access to this data.

Chairman LEAHY. Has that been done?

Mr. DUDA. Partially.

Chairman LEAHY. Partially. And shouldn't we make sure that if we are going to have penalties, criminal or otherwise, that they be the same whether you are somebody in the State Department or somebody in a private contractor?

Mr. DUDA. Absolutely.

Chairman LEAHY. Thank you. And in that regard, Ambassador, the Attorney General suggested that DOJ will open a criminal investigation into the passport breaches involving the three Presidential candidates based upon the referral from your office. Are there going to be more referrals from your office?

Ambassador GEISEL. We don't comment on investigations, but there will certainly be referrals where we feel that a case can be made to the Justice Department and that the Justice Department has reasonable probability of achieving a good prosecution.

Chairman LEAHY. Both Senator Specter and I are former prosecutors, as are a number of the people on this Committee, and, frankly, in this kind of thing, I think some well-placed prosecutions with the use of the criminal code may be as much of a deterrent as you can imagine.

Senator Specter?

Senator SPECTER. Thank you, Mr. Chairman.

Has anybody been caught?

Ambassador GEISEL. Yes, sir. Those were the referrals that were made.

Senator SPECTER. And what happened as a result of their being identified, apprehended, and caught?

Ambassador GEISEL. Excuse me, sir.

[Pause.]

Ambassador GEISEL. If these people have actually been referred to Justice, I—

Senator SPECTER. No, I don't want to know "ifs." I want to know if you have apprehended people and they have been caught. That is what I want to know.

Ambassador GEISEL. The answer is yes, sir.

Senator SPECTER. And how many?

Ambassador GEISEL. Five so far, but it is very much of an ongoing investigation, and I am sure—

Senator SPECTER. Only five.

Ambassador GEISEL. So far.

Senator SPECTER. And have there been prosecutions against those individuals?

Ambassador GEISEL. I am not aware of what Justice is doing with those referrals.

Senator SPECTER. Well, Ambassador, you ought to be. You ought to followup as to what the Department of Justice is doing. We would like to know that.

Let me talk to the witness, if I may. I only have 5 minutes. What is the motivation behind this, if you know? Is it just curiosity? Is it just snooping? Why so many invasions of privacy here?

Ambassador GEISEL. Well, I hope it is just snooping. I suspect—

Senator SPECTER. No, no. I don't want to know what you hope. What evidence do you have as to what motivates people to do this?

Ambassador GEISEL. I don't think we know yet what motivated these particular people to snoop.

Senator SPECTER. Well, have they been questioned? Obviously, they have been. What has the interrogation of these people disclosed?

Ambassador GEISEL. So far it is snooping, sir.

Senator SPECTER. So far what?

Ambassador GEISEL. It is snooping, just as you said. It is snooping. It is peeping. We don't have any evidence that the—which is what I worry about, that someone would do this, for instance, for the purpose of perpetrating identity fraud.

Senator SPECTER. Well, is the Department of State making a real effort to push prosecutions? Prosecutor Leahy might say to you that if you get a conviction, you deter some people from doing it. I certainly would say that.

Ambassador GEISEL. Amen, Senator. I cannot think of a better way—I think there are two—

Senator SPECTER. So what have you done to pursue prosecutions to try to have some deterrence?

Ambassador GEISEL. We have referred them to the Justice Department.

Senator SPECTER. Have you followed up? We write lots of letters to the Department of Justice. Senator Leahy had a whole portfolio of them yesterday talking to the Attorney General. There has to be followup. This is a primary responsibility of the Department of State, and the Department of State ought to pursue it.

Ambassador GEISEL. I absolutely agree with you, Senator.

Senator SPECTER. Well, what do you plan to do about it?

Ambassador GEISEL. I think the best answer is that we, A, intend to followup but, B, intend to put in a much better system or recommend—

Senator SPECTER. Well, a better system we have talked about, but where you have the specific cases, would you give a report to the Committee within 30 days on the issue of followup and what has happened?

Ambassador GEISEL. Absolutely, sir.

Senator SPECTER. I note that the penalty for looking for commercial advantage or financial gain is increased to 5 years. It is 1 year otherwise. Has there been any showing that any of these invasions of privacy were motivated by commercial advantage or financial gain?

Ambassador GEISEL. Not yet, sir, but as I said, that is our greatest worry.

Senator SPECTER. Have you pursued the issue as to whether somebody is looking for financial gain?

Ambassador GEISEL. Yes, sir, but as I said, so far it appears to be peeping.

Senator SPECTER. When you have the evidence of unauthorized disclosure, do you go to the individuals whose files have been tampered with to see if they have any indication that they have been prejudiced in any way by what has happened?

Ambassador GEISEL. That is part of an ongoing investigation, and I am sure you understand that I—

Senator SPECTER. I understand. I am not asking you about specific cases. I am asking about procedures. I am not asking you about a specific case.

Ambassador GEISEL. Yes, sir.

Senator SPECTER. I would not intrude on that.

Ambassador GEISEL. I understand. I don't know that we have—let me ask our people. Have we gone to specific individuals?

The answer is—as you advised, I will not discuss it in detail, but the answer is yes, we have done so.

Senator SPECTER. The answer is yes to which question?

Ambassador GEISEL. The answer is yes, we have spoken with individuals to see if they were affected by the—

Senator SPECTER. I am not asking you about any specific individuals. Have you found any individuals who have been prejudiced aside from—just an invasion of privacy is a prejudice all by itself. But beyond that, have they lost financially? Have they had anything specific happen as a result of the unauthorized disclosure or snooping on their records?

Ambassador GEISEL. We have not—that is a negative, sir. So far, no one has advised that they have been adversely affected in a financial sense by the snooping.

Senator SPECTER. Well, as a final comment—my red light is on—I would urge you to get tough about it and to followup.

Ambassador GEISEL. Absolutely.

Senator SPECTER. And reports are not sufficient. When Congress is providing criminal penalties, you have a real hammer, and you ought to be using it. If you would supply in writing any recommendations you have for modifications of the statute, I think the Committee would appreciate that.

Thank you very much, Ambassador. Thank you, Mr. Duda.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Senator Cardin?

Senator CARDIN. Thank you, Mr. Chairman. I certainly agree with your comments and Senator Specter's comments, and I want to followup on Senator Specter's points.

First of all, I want to thank both of you for what you are doing in helping us to put in the right procedures to make sure this never happens again. But I just want to underscore the point that Senator Specter has made. When we had similar problems in other agencies—I think about laptops that were taken out of offices and that contained sensitive data that went missing—we were not clear as to what was being done with that sensitive information, which included Social Security numbers. We know that identity theft is one of the largest criminal problems we have in our community today. We know that the information contained in passport files would be very valuable for people who want to participate in identity theft. As Senator Leahy has said, we know that the information could be valuable for criminals who want information about potential targets. So the vulnerability is there with the information, and that is why it is particularly sensitive.

I think your testimony has raised a lot more questions than we have the answers to. Obviously, someone who does this for curiosity to peep in someone else's records is wrong and needs to be disciplined. But if they are doing it for financial reward, if it is part of criminal activities, then that is a much more serious issue, and we want to know about that also.

I also believe—and I know there is a large volume of people whose records have been unauthorized access. But I think to a certain degree those individuals are entitled to know that. And although in a criminal investigation you may be looking at a specific number of cases in order to get the cooperation of the individuals whose records were unauthorized accessed, but I do think if someone looked at my passport records, I have a right to know that.

So are any steps being taken in order to notify the individuals whose records were unauthorized accessed so that they are on record, first, that that was done and, second, to be alerted to potentially being a victim to other types of activities such as identity theft?

Ambassador GEISEL. To date, Senator, the work that we have done, we are not yet at the point, as Mr. Duda explained, that we are certain that the access was unauthorized, although obviously when you are talking about numerous breaches, it seems a sure shot.

The problem will be—well, we cannot notify anyone until we know that the access was unauthorized. In many cases, it would have been authorized. For example, someone who often crosses the border, the Homeland Security person will have a very good reason for going back to that file. But we have a lot more work to do.

Mr. DUDA. One of the things I wanted to point out is that, you know, management's responsibility is obviously to have a system in place, have the controls to prevent unauthorized access to, you know, PII information for all Americans. OIG's role obviously is to oversee that and do testing and so forth.

In this review that we did, we identified such a large number of potential unauthorized accesses and a control environment that

was limited, at best. We made significant recommendations which the Department largely agree with and is in the process of implementing. And one of the things they are doing right now, they have told us—CIA officials have told us that they are looking into all of the potential unauthorized accesses from our case study, and then once the determination that the Department makes, they will then make referrals to the Office of Inspector General.

Senator CARDIN. Let me make a recommendation. To the extent that you determine that someone's passport records were accessed, unauthorized, will you recommend that that individual be notified that his or her records were inappropriately accessed?

Mr. DUDA. Yes, absolutely. I don't know whether that will be a management responsibility, but OIG definitely—

Senator CARDIN. Will you let us know whether that recommendation is followed by the agency so that we know whether, in fact, those who were victimized are at least aware that they were victimized?

Mr. DUDA. Yes. One of the corrective actions the Department has already implemented is drafting a breach response policy, and I don't recall the exact specifics, but—

Senator CARDIN. I just want to make sure that we know whether the victims, those whose records were accessed inappropriately, will be notified, and whether you will be able to follow up to let us know whether that, in fact, was carried out by the agency.

Ambassador GEISEL. We will make that recommendation, Senator.

Senator CARDIN. I appreciate it.

The second point, Mr. Chairman, just very quickly, we just finished acting on the FISA statute, and it just raises a question to me as to whether agencies are accessing passport records for mass data collections. Is any of this involved in a data collection system where there is routine information gathered on our passport records as part of homeland security or intelligence operations that you are aware of?

Mr. DUDA. Not that I am aware of, but one of our concerns in this review or any potential plans of sharing the data in PIERS or any of the other passport systems with other agencies for any purpose, we want to make sure that there are adequate controls in place.

Senator CARDIN. Will you also report back to us if your review shows that there is mass data collections from the passport records that are questionable from the point of view of whether they are authorized by statute?

Mr. DUDA. Absolutely.

Senator CARDIN. Thank you.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much, and if we have other questions, we will submit them for the record. There is going to be a roll call vote fairly soon, so if we seem to be speeding along, that is why. But thank you both very, very much. It helps us highlight the concern that we have here.

The next panel, if we could arrange to bring them up. This panel of people are certainly known to this Committee. Marc Rotenberg is the Executive Director of the Electronic Privacy Information

Center, EPIC, in Washington, D.C. He teaches information privacy law at Georgetown University Law Center, an excellent school, having graduated from there. He has testified before Congress on such topics as encryption policy, consumer protection, computer security, communications privacy. He chairs the ABA Committee on Privacy and Information Protection. He has served on several national and international advisory panels, including expert panels in cryptography policy and computer security for the OECD, legal experts in cyber space law for UNESCO. He is a founding board member and former chair of the Public Interest Registry, which manages the .org domain. He also served as counsel, in full disclosure, an invaluable member of my staff on the Senate Judiciary Committee. He is a graduate of Harvard and Stanford Law School, the recipient of more awards than I could even name, but that includes the World Technology Award in Law.

Mr. Rotenberg, please go ahead.

**STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR,  
ELECTRONIC PRIVACY INFORMATION CENTER, WASHINGTON, D.C.**

Mr. ROTENBERG. Thank you very much, Mr. Chairman, Senator Cardin. I appreciate the opportunity to be here today.

We have a particular interest in the privacy of personal information collected by Federal agencies, and as the recent news stories and the report from the Inspector General have made clear, the passport information that we are required to provide to the Government is not adequately protected. And we are particularly concerned about this because there are growing demands on personal information by the Federal Government, and with the increasing use of identification documents.

So it is not simply the passport information of Presidential candidates or celebrities that is at issue. It is the personal information of people who apply for a driver's license, work in the Federal Government, or travel to Canada. And for these reasons, we think that more needs to be done to protect personal privacy, not only at the State Department but also across the Federal Government.

Now, I think it is helpful to understand the background of the particular incident at the State Department to put in context what the Inspector General uncovered. It was back in 1992 when State Department officials were found to be going through the passport files of then Presidential candidate Bill Clinton to try to find embarrassing information. And there was an investigation. The State Department subsequently dismissed employees who were engaging in this activity. This is precisely the concern about information that individuals provide to the Federal Government that will be misused, that will be obtained by identity thieves, or that will be used in ways that are simply not appropriate.

So it was because of that 1992 incident that alarm bells literally went off this spring at the State Department when it was determined that the passport files of Senators Obama, McCain, and Clinton had been improperly accessed. And I think it is worth noting that all three Senators made statements at the time about the importance of protecting the privacy of personal information. In fact, Senator Obama himself 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.”

Now, the Inspector General’s report, which was undertaken pursuant to the March release of the passport information, provides some useful information and some useful recommendations. But I should point out that much of the report has been redacted, that is to say, of the 22 recommendations contained in the IG’s report, only six, in fact, are available for public review. There are many sections of the report that have literally been blacked out. If I may show the Committee, we have a few pages here from the report.

[Displays documents.]

This is a page labeled “Sensitive but unclassified.” The top half of the page references the FOIA exemption (b)(2) as the basis for withholding the information. The bottom does not even bother with the (b)(2) designation. It just blacks out the entire section of the report. This is problematic because, of course, to evaluate the adequacy of the recommendations made by the Inspector General, it is important to see the whole report.

Now, we have made—and it is included in my complete statement—a series of recommendations. We do think there should be auditing so that whenever there is access, those access events will be recorded. We do think there should be improved oversight. We think there needs to be some independent evaluation of the privacy safeguards within the Federal agencies, including the State Department. But I think most importantly, the legislation S. 495, which you, Mr. Chairman, cosponsored along with Senator Specter and was favorably reported by this Committee, contains several very important provisions that, if in force, might have actually prevented this from occurring, because a big problem today at the State Department is that a lot of the information processing is being done by private contractors. The agency turns over to a private company the responsibility for producing the passports, for collecting the information for the passports, for inspecting the information. And it is in that process of outsourcing the Government function that the privacy concern arises. And so this legislation, S. 495, actually puts in place disciplinary requirements so that if these kinds of problems occur, people can be held accountable, opportunities to review the contractor relationship so that an agency can make a determination if the contractor is doing enough to protect personal privacy.

One of the remarkable facts here is that just a few days before the State Department revealed that three Presidential candidates had their passport files improperly accessed, the agency had renewed its contract with Stanley, the privacy company, a 5-year deal for \$570 million. I think if a company cannot protect the personal information of American citizens that it obtains, the agencies need to rethink some of those contracts.

So thank you very much for the opportunity. I would be pleased to answer your questions.

[The prepared statement of Mr. Rotenberg appears as a submission for the record.]

Chairman LEAHY. Thank you very, very much.

Ari Schwartz is the Vice President and Chief Operating Officer of the Center for Democracy and Technology, CDT. He works to promote privacy protection in the Digital Age while expanding access to Government information through the Internet. He is the leader of the Anti-Spyware Coalition, in 2006 was awarded the RSA Award for Excellence in Public Policy for his work in building the Anti-Spyware Coalition and other efforts against spyware. He has been named to the top five Influential IT Security Thinkers of 2007 by Secure Computing magazine, served as a member of the Department of Commerce National Institute of Standards and Technology Information, among others.

So, Mr. Schwartz, I am delighted you are here because I am a bit of a bug or nag in my office on keeping spyware off our computers.

**STATEMENT OF ARI SCHWARTZ, VICE PRESIDENT, CENTER  
FOR DEMOCRACY & TECHNOLOGY, WASHINGTON, D.C.**

Mr. SCHWARTZ. Thank you very much, Senator Leahy, and Senator Cardin as well. Thank you for holding this important public hearing and for inviting me to participate.

I would especially like to commend you, Mr. Chairman, on how you opened this hearing. While the news reporting on the subject of passport breach has focused on whether Presidential candidates or other celebrities had their passport records snooped through, the privacy and security of the passport records of average individuals has received considerably less attention, and you raised that in your opening statement and I appreciate that.

As we heard earlier, there seems to be little to no protection on how to prevent or detect the truly nefarious activities which passport records such as stalking or identity theft that we could see with this kind of browsing.

To address this problem, CDT suggests that Congress take the same approach that it did 11 years ago when it was found that IRS employees were browsing tax records. Congress should increase oversight and civil and criminal penalties on passport records. Just to send you to the right place, that is the Taxpayer Browsing Protection Act of 1997 that I know the Chairman and many other people on this Committee worked on.

The illegal browsing of passport records of Americans by Government employees should be a major concern not only to the millions of passport holders but to all Americans as it suggests an inability of Government to protect privacy at the highest levels.

The Inspector General's report pointed to many flaws in the State Department's ability to protect privacy. CDT has raised many of these same concerns over the past 3 years with the State Department. For example, the Inspector General found that the Privacy Impact Assessment for the passport data base was just inaccurate. CDT wrote to Secretary Rice over a year ago to raise concerns about Privacy Impact Assessments at the State Department, and particularly the E-Passport program. We never received a reply, and no changes to the PIAs were ever made. CDT has since found incomplete and inaccurate information in several other Privacy Impact Assessments on the Department of State website.

The State Department must be held accountable for the failures of its privacy program and encouraged to provide resources and leadership so that it can be ensured that our privacy is being protected when held by the State Department.

To prevent other serious breaches of public trust Congress will need to address the roots of the problem by more closely monitoring the State Department's collection of personal data.

While the State Department has clearly been a failing agency across the board on privacy, there are several other failing agencies as well. For example, one agency that CDT spoke to told us that a privacy audit revealed that they had lost track of half of their Privacy Act system of records. They simply do not know where millions of personal records were that were originally brought in by this agency. One retiring security official from the Department of Interior explained publicly, while discussing that agency's constant failures in privacy and security reporting, "We are promiscuous with our data. We don't know where our data is."

You can call this a privacy concern. You can call this a security concern. You can call it a data management concern. But to the American taxpayer, it is certainly called a failure.

CDT agrees with GAO's recent analysis suggesting that the way to ensure privacy protection at agencies is through improvement in existing Government privacy laws, oversight, and leadership. To solve these problems beyond our initial State Department specific suggestions, CDT recommends that Congress work with the executive branch in the four following areas:

No. 1, expanding Privacy Act coverage and closing Privacy Act loopholes.

No. 2, improving the quality of Privacy Impact Assessments by Government agencies. This would also include Privacy Impact Assessments for Government use of commercial data, as required in the Leahy-Specter data breach bill, S. 495 as referenced earlier.

No. 3, improving privacy leadership. This would include a permanent Chief Privacy Officer position at the Office of Management and Budget written into law, Chief Privacy Officers at all major component agencies, and the creation of an independent Chief Privacy Officer Council with a similar structure to the CIO and CFO councils.

And, No. 4, increasing and improving privacy reporting and audits. I detail all these suggestions in my written testimony.

In general, we believe that there is now consensus around a set of sound recommendations for action by Congress and executive branch to fill the gaps and loopholes in privacy law and policy. CDT urges the Committee and the Senate to work quickly so that the next President can have the right tools in place upon taking office and can get started immediately on strengthening privacy in the Federal Government.

I look forward to working with you, and we thank you for your leadership on these important issues. Thank you for your attention, and I look forward to your questions.

[The prepared statement of Mr. Schwartz appears as a submission for the record.]

Chairman LEAHY. Thank you very much.

Alan Raul is a partner in the Washington, D.C., office of the international law firm Sidley Austin. He chairs Sidley's Information Law Privacy Practice Group, served as Vice Chairman of the White House Privacy and Civil Liberties Oversight Board from March 2006 through January 2008. He was the Associate Counsel to President Reagan from 1986 to 1988, where he represented the White House in connection with the Iran-contra investigation. He served as General Counsel to the Office of Management and Budget in the Executive Office of the President. He was nominated by President George H.W. Bush and confirmed by the Senate to the position of General Counsel at the U.S. Department of Agriculture from 1989 to 1993. He is a graduate of Harvard College, Harvard University's Kennedy School of Law, and to show there is no rivalry, the Yale School.

Please go ahead.

**STATEMENT OF ALAN CHARLES RAUL, PARTNER, SIDLEY  
AUSTIN, LLP, WASHINGTON, D.C.**

Mr. RAUL. Thank you, Chairman Leahy, Senator Specter, Senator Cardin. Thank you for inviting me to testify on protecting the privacy of passport files maintained by the U.S. Department of State. It is an honor to appear before you this morning.

I am testifying today in a personal capacity. As you noted, I am currently engaged in private law practice in Washington where I focus on privacy, data security, and Internet law. And until recently, I also served in a part-time capacity as Vice Chairman of the White House Privacy and Civil Liberties Oversight Board.

This hearing arises because of a recent investigation and report by the State Department's Inspector General indicating that the passport files of high-profile individuals, including the files of three Presidential candidates—namely, Senators McCain, Obama, and Clinton—may have been improperly accessed by State Department employees and contractors. The State Department announced this week that it had terminated around five contractors in connection with what appear to be serious violations of personal privacy, Federal law, and internal controls.

While the investigation continues, if the facts turn out to be as they now appear, there is no question that the standards of the Privacy Act of 1974 were not satisfied. To the extent agency employees and contractors accessed passport files with no official need to do so, they disrespected the privacy of affected passport holders and applicants and brought substantial disrepute upon their agency.

The Privacy Act, the e-Government Act of 2002, and the Federal Information Security Management Act of 2002—FISMA—all require Government agencies to adopt and implement effective controls to prevent just the sort of invasion of personal information that occurred here.

Moreover, each of these Acts authorizes the Director of the Office of Management and Budget to assist, guide, and oversee Federal efforts in the realm of privacy and information security. Congress and the White House should continue to support and encourage OMB's leading role in the field of privacy and information security.

With regard to the specific incident at hand, it is not clear at this point whether any of the individuals whose files were accessed experienced any pecuniary losses or other actual damages that would support claims of civil liability under the Supreme Court's *Doe v. Chao* decision of 2004. However, if any agency employee or contractor "willfully disclose[d] the material in any manner to any person or agency not entitled to receive it," or "knowingly and willfully request[ed] or obtain[ed] any record concerning an individual from an agency under false pretenses," then they would be guilty of a criminal misdemeanor and fined up to \$5,000.

It is perfectly clear now, however, that existing law and applicable guidance should have prevented State Department employees and contractors from engaging in frolics and detours—or worse—through the passport files of politicians, prominent figures, or indeed, of any Americans. The fact that these files were subject to access for no good reason is highly troubling. We all expect the Government to do much better in safeguarding our personal information.

Plainly, the State Department must redouble its efforts to conduct privacy impact and risk assessments, to communicate binding privacy policies to all parties handling personal information—both employees and contractors—provide its employees and contractors with meaningful privacy and data security training so they take these issues seriously, and ensure effective audit trails for accessing personal information, as well as establishing clear guidelines for disciplining and terminating employees and contractors who transgress. The State Department should also revisit its administrative, technical, and physical safeguards to prevent future abuse of passport files and other personal records.

At the same time, care must be taken to avoid unduly restricting proper access to information that is essential for national security purposes. As the 9/11 Commission recommended, and Congress enacted, the country has a critical need to promote an "information sharing environment" that transcends traditional governmental boundaries in order to help prevent future terrorist attacks. But the relevant Government agencies, including the State Department, must effectively integrate protections for privacy and other civil liberties into this new information-sharing environment.

In any event, if the executive branch wishes to hold the private sector, State governments, and foreign nations to high standards for information privacy and security, it needs to be a consistently good role model for privacy itself. To that end, the Government obviously has plenty of room for improvement under existing privacy laws and standards for information security.

Thank you for considering my views.

[The prepared statement of Mr. Raul appears as a submission for the record.]

Chairman LEAHY. Thank you. The vote has started. I want to ask one question, and then we will recess for a couple minutes to see if others are coming back.

Mr. Rotenberg, last year Senator Specter and I introduced our Personal Data Privacy and Security Act. Now, this has a specific requirement that the General Services Administration has to evaluate the privacy security practices of potential Government

contractors, but then put penalty provisions in if they fail to follow and fail to protect data privacy. Would this help?

Mr. ROTENBERG. Absolutely, Senator. As I was thinking about the legislation, which I believe you introduced in 2007, it occurred to me this was actually an example where the legislation was ahead of the problem. In other words, if these requirements had been put in place back in 2007, I believe the State Department would have been much more careful in its relationship with the private contractor, and I think the private contractor would have been much more diligent about the activities of its employees. And it was the failure to pass that legislation earlier that very well may have made possible this recent breach.

So I hope the Senate—and the House, of course—act on this. I think it would prevent a lot of damage going forward. It is a very sensible approach to a real problem.

Chairman LEAHY. Mr. Schwartz, Mr. Raul, how do you feel about that?

Mr. SCHWARTZ. I strongly agree with that statement. It would definitely help privacy and security to have that kind of review, and the Government needs to ensure that their security efforts and the security efforts of their contractors are the best that there are. And I would actually take it a step further and say that the entire title of that bill, S. 495, Title 4, would have helped in this case. It has better auditing capability in that section, assuming that was not done in this case, and improvement of Privacy Impact Assessments, something that the Inspector General specifically pointed out in this case was a failure.

Chairman LEAHY. Mr. Raul?

Mr. RAUL. Chairman Leahy, due diligence of potential contractors with regard to their information security systems and processes is essential. I think that is recognized in other legislation like Gramm-Leach-Bliley, HIPAA, regulations under those statutes. I think there is existing guidance that Federal agencies should be doing it now.

I think the message really need to be effectively communicated to the various departments and agencies that they need to take this seriously. So I would support strongly sending that message to all agencies.

Chairman LEAHY. Well, you know, my concern is we know how much there are attacks from outside our borders into all our different computer banks, and a lot of this has been reported in the press, and I will not go into some aspects of it for obvious reasons in an open session. So we have to guard against that, and we should, of course, for the obvious reasons—national security and everything else.

I hate to have to think we have to guard against our own people, and yet it seems possible. The Inspector General's report included 22 recommendations for improvements in the Consular Affairs Bureau of the State Department.

We have that the Department is going to implement most of the recommendations. Is that going to be enough? Again, I am thinking about what we do with our own people. It is a whole different subject what happens when we have countries, not just bad actors out-

side but actually state-sponsored efforts to penetrate our computer systems.

Mr. ROTENBERG. Senator, I think the Inspector General's report is helpful, but I don't think it will be enough. It has recommendations to the agencies, some of which apparently the bureaus are disputing. I think there needs to be here a clear mandate about how the practices are going to change so that this does not happen in the future. And I think there needs to be a comprehensive approach that prevents this from happening in other Federal agencies.

One of the realities right now is that security breaches are on the increase in the Federal Government, and without adequate safeguards to ensure particularly with private contractor access to personal data, I think this problem will continue to get worse.

Mr. SCHWARTZ. Mr. Chairman, I would say that the external security and the internal security are actually tied together and that you cannot really separate the two. It seems in this case, from what we know from the public reports, that the State Department did not know all the people that had access to it, and did not even list all the agencies that have access to it.

Chairman LEAHY. That really frosted me when I saw that.

Mr. SCHWARTZ. And then we also see—and I just said from other agencies, we know that agencies are losing systems. If they do not know where it is, that makes it more vulnerable to outside attack. You cannot secure something if you do not know where it is.

These are all systems that have personal information of Americans in them, so I think that it is a major concern both for the internal threat that comes from this and the external threat as well.

Mr. RAUL. One of the critical components, Chairman Leahy, in any information security program is the conduct of a risk assessment, either incorporated in a Privacy Impact Assessment as required by the Federal Government, or in vulnerability assessments.

From my review of the redacted version of the Inspector General's report, it is not clear whether the State Department had conducted sufficient risk assessments in this area. And it sounds like they were not sure who had access, what information they had. You know, that is unacceptable because risks, as you say, Mr. Chairman, can be either internal or external, and for various different motivations. And if an agency does not know what is at risk, it cannot possibly protect against it.

Chairman LEAHY. We will stand in recess. I keep looking up here. You are probably wondering what I am looking at. It is those five lights in the back which went on some time ago. That is the 5-minute warning. I am heading to the floor. Take care.

We will stand in recess.

[Whereupon, at 11:09 a.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

## QUESTIONS AND ANSWERS

Sensitive, but Unclassified – Law Enforcement Sensitive

### Questions obtained during the Judiciary Committee Hearing of July 10, 2008

*From Senator Specter*

**1. Would you report back to us in 30 days with a progress report on the investigation of those alleged to have opened passport files without authorization or used information in the commission of crime?**

Response: OIG/INV has been referred approximately 70 allegations of unauthorized access concerning PIERS from the Department and from the OIG's audit review of the PIERS system. As we find potential violations of law, we will refer and have referred them to the Department of Justice for prosecutorial determination. To date, OIG/INV has conducted approximately 40 subject interviews and 50 witness interviews. (SBU-LES)

Our investigations have revealed that an overwhelming majority of those interviewed have reinforced the findings of the OIG Audit report released in July 2008. That is, those interviewed claim that they were never given guidance regarding their individual responsibility as a user. In addition they were given initial training on the PIERS database by searching famous celebrities. (SBU-LES)

To date, we have found no evidence that information improperly accessed was used in additional criminal activity or for any other purposes. (SBU-LES)

According to the Department, there have been some persons punished administratively (including removals) but this information is available by contacting the Bureau of Legislative Affairs. The point of contact for this part of the responses is Steve Zate at the Bureau of Legislative Affairs. His contact number is (202) 647-8734. On behalf of the appropriate bureau, HR may have taken action against other individuals and HR would provide that information via the Bureau of Legislative Affairs.

Normally, at the completion of an investigation we would refer our reports of investigation to the bureau of Human Resources (HR/ER) and to the office of Personnel Suitability and Security (DS/PSS) for independent adjudication and action (as they deem appropriate). We would also request results of any action they take concerning the matter investigated.

**2. Please let us know if you would recommend changes in the statutes on penalties or any matter that would assist in the process of corrective action.**

Response: The Department of State Office of Inspector General (OIG) supports the provision in S.495 providing for review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information. Prompt Departmental implementation of recommendation 17 would also assist in the corrective action process. Recommendation 17 recommends that the Department determine the feasibility of developing and implementing specific disciplinary guidelines and a table of disciplinary actions and penalties to address unauthorized access to passport information.

Sensitive, but Unclassified – Law Enforcement Sensitive

*From Senator Cardin*

**3. Does the Department plan to send alerts to individual victims who have had their passport records opened by anyone in the user base in an unauthorized manner? If not, why not?**

Response: We have forwarded this query to The Bureau of Legislative Affairs as this question was not a part of our initial quick-response review. We understand that Department bureaus, which were not part of the July 10, 2008 hearing, are prepared to respond to these committee questions upon receipt from the committee. The response to this query will be reviewed by the OIG for possible inclusion in compliance reporting or future reviews of this system. The point of contact for these responses is Steve Zate at the Bureau of Legislative Affairs. His contact number is (202) 647-8734.

**4. Does the Department plan to send a broadcast-type message all passport holders regarding the unauthorized breached to reassure them regarding corrective action? If not, why not?**

Response: We have forwarded this query to the Bureau of Legislative Affairs as this question was not a part of our initial quick-response review. We understand that Department bureaus, which were not part of the July 10, 2008 hearing, are prepared to respond to these committee questions upon receipt from the committee. The response to this query will be reviewed by the OIG for possible inclusion in compliance reporting or future reviews of this system. The point of contact for these responses is Steve Zate at the Bureau of Legislative Affairs. His contact number is (202) 647-8734.

*Judiciary Committee Staff Questions (majority)*

**Increased Passport Demand**

**5. Much of the expansion in the number of people who can access passport records is due to the huge increase in passport applications. The State Department estimates that 29 million passport applications will be processed this year alone -- and that between 30 and 36 million applications will be processed in fiscal year 2009. As the State Department develops more automated systems to respond to increased passport demand, what controls should be put into place to ensure that the privacy of American citizens is adequately protected?**

Response: OIG made 22 recommendations to the Department that address corrective actions needed to improve controls. Specifically, for number 19, the OIG recommended that vulnerability and risk assessments be conducted of all passport systems within 120 days after the issuance of the OIG report. This recommendation also requires the results of these assessments identify corrective actions needed and a timetable to address weaknesses and vulnerabilities. It

Sensitive, but Unclassified – Law Enforcement Sensitive

is important that these assessments be conducted as soon as possible to determine the proper controls needed.

The Department concurred with this recommendation for system wide reviews in systems containing personally identifiable information, and agreed to ensure a comprehensive evaluation and where necessary, create mitigation strategies to address vulnerabilities. The primary organizations participating in these assessments are the Bureau of Administration, Bureau of Consular Affairs, and the Office of Information Resources.

Scope of Privacy Concerns

**6. Your report focused on the “Passport Information Electronic Records Systems” or PIERS because it is the largest of all data systems and happened to be the subject of several breaches in March of this year. However, the State Department is responsible for several other data systems, which also include Americans’ personal private information. Based upon your findings with respect to PIERS, do you believe that there may be similar privacy vulnerabilities in other State Department databases?**

Response: Yes. Specifically, for recommendations number 18 and 19, OIG recommended that Privacy Impact Assessments be reviewed and vulnerability and risk assessments be conducted for all passport systems within 120 days after the issuance of the OIG report.

Access to Passport Records

**7. I was shocked to learn that more than 20,000 government workers and outside contractors have access to the Department’s passport records. In addition to improving data privacy controls, should the number of people who can access passport records be limited, or monitored, to reduce the risk of improper passport snooping?**

Response: Yes. Ten of the 22 recommendations in the report relate to these concerns. OIG recommended that access to passport records be limited to authorized users with a verifiable business need, and that the amount of information available be based on the business role of the user (i.e. tiered user access). OIG also recommended that only active users have access, that inactive users’ user IDs and passwords are deleted from the system, and that periodic monitoring be conducted to validate users and their access needs. This applies to all users, whether internal or external to the Department.

**8. According to the OIG report discussed in the July 10, 2008 hearing, Consular Affairs officials indicated that, “...there were about 20,500 users with active PIERS accounts as of May 2008 and about 12,200 of these users were employees or contractors of the Department....PIERS is also accessed by users at other federal agencies to assist in conducting investigations, security assessments, and analyses. These other federal entities are located across the United States and include the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Office of Personnel Management (OPM).” (p. 7)**

**a. Please provide a list of all federal agencies that have users with PIERS access.**

Sensitive, but Unclassified – Law Enforcement Sensitive

- b. Please provide a list of all contractors of the Department with PIERS access. (If a comprehensive list is not possible, please provide a list of all known contractors.) (H/CA))
- c. Approximately how many of the 12,200 “employees and contractors” you mentioned are employees, and how many are contractors?
- i. What sort of oversight of these contractors currently takes place in relation to privacy issues (if any)?
  - ii. Are these contractors subject to any disciplinary actions by the Department for privacy breaches?
  - iii. When these contractors enter into contracts with the Department, are they required to follow that same policies and procedures as Department employees?

Response: We have forwarded this query to the Bureau of Legislative Affairs as this question was not a part of our initial quick-response review. We understand that Department bureaus, which were not part of the July 10, 2008 hearing, are prepared to respond to these committee questions upon receipt from the committee. The response to this query will be reviewed by the OIG for possible inclusion in compliance reporting or future reviews of this system. The point of contact for these responses is Steve Zate at the Bureau of Legislative Affairs. His contact number is (202) 647-8734.

**9. What is the timeline for follow-up on the recommendations made in the OIG report? What consequences (if any) will there be if these changes from the report are not implemented?**

Response: OIG’s compliance policy requires each agency to provide a written response for each recommendation within 30 calendar days from the date the report was issued (July 2), at which time OIG will evaluate the agencies’ responses. Any disagreements that cannot be resolved, and for which OIG determines that an impasse has been reached, will be referred to the Under Secretary for Management for adjudication, pursuant to Department policy. In such instances, OIG will inform the Committee of the Under Secretary’s actions. In addition, OIG will conduct a follow-up review of corrective actions taken or planned by the Department, and the Department’s process for reviewing potential unauthorized accesses as identified in OIG’s study.

On July 3, Senator Biden sent a letter to Secretary Condoleezza Rice urging the Secretary to take all appropriate measures to promptly implement OIG’s recommendations and requesting a progress report from the Department within 90 days. Additionally, on July 17, the Senate Appropriations Committee approved a funding measure that would withhold 20 percent of the funds generated from fees collected from issuing passports and other services that would be made available to the Department in 2009 until the Department follows recommendations for improving the security of personal information contained in passport files.

**10. Recommendation 17 in the OIG report reads as follows: “OIG recommends that the Bureau of Consular Affairs, in coordination with the Bureau of Human Resources, determine the feasibility of developing and implementing specific disciplinary guidelines and a table of disciplinary actions and penalties to address unauthorized access to passport information. Consideration should be given to addressing all passport system users, including contractors, within the Department of State and with other agencies.” Consular**

Sensitive, but Unclassified – Law Enforcement Sensitive

**Affairs and Human resources did not concur with the recommendation, and it remains unresolved.**

**a. Please describe why you made this recommendation and what makes these sorts of guidelines so important?**

Response: OIG made this recommendation because existing guidelines for disciplinary actions cited by the Department were inadequate for the following reasons:

- a) They did not adequately address both Civil Service and Foreign Service employees;
- b) They were not readily available and conveyed to staff and managers to ensure that these individuals were aware of the possible penalties their unauthorized access could incur and that disciplinary actions for unauthorized access met some minimum standards that applied to all; and
- c) They were not communicated to other agencies and contractors (whether informally or as part of a Memorandum of Agreement or contract) to ensure that disciplinary actions for unauthorized access by their employees were both appropriate and consistent when compared to those applied to Department personnel.

Both the Internal Revenue Service and the Social Security Administration have tables and guidelines that are provided to employees and that define and clarify the penalties individuals may be subject to if they inappropriately access privacy data. OIG believes that having and communicating such information reinforces the seriousness of unauthorized access and can serve as a deterrent to inappropriate access.

**11a. What do you recommend Congress do to ensure that the Bureau of Consular Affairs is held accountable for implementing the OIG's recommendations?**

Response: As mentioned in response to Question 9, Congress has initiated actions to ensure that the Department is held accountable for implementing the OIG's recommendations. In addition to this, OIG will follow up on the Department's implementation of the report's recommendations as part of the normal compliance process. In addition, OIG will conduct a follow-up review of corrective actions taken or planned by the Department, and the Department's process for reviewing potential unauthorized accesses as identified in OIG's study.

**11b. What should Congress do to ensure general accountability on the issue of passport privacy protection?**

Response: OIG believes that if the report's recommendations are properly implemented, and that existing federal requirements related to protection of privacy data to include the Federal Information Security Management Act of 2002 and Office of Management and Budget's M-06-16 (June 2006) and M-07-16 (May 2007), are followed, that Congress can ensure general accountability on the issue of passport privacy protection.

Sensitive, but Unclassified – Law Enforcement Sensitive

**Judiciary Committee Staff Questions (minority)**

**12. To the extent Privacy Act violations are obviously a systemic problem afflicting numerous agencies, what do you think the OMB Director should do on a government-wide basis to make sure that other agencies are making improvements similar to the ones you have already undertaken?**

Response: We support the findings in the June 18, 2008 Government Accountability Office Report (GAO-08-795T) on personally identifiable information, which identified alternatives that the Congress should consider, including revising the scope of privacy laws to cover all personal information, requiring that the use of such information be limited to a specific purpose, and revising the structure and publication of privacy notices. We understand that OMB commented on this report, saying that the Congress should consider these alternatives in the broader context of existing privacy and related statutes.

**13. Have you asked the leadership of the PCIE and ECIE to help you apprise other agencies' Inspectors' General that it behooves them to go to school on the mistakes and, hopefully, lessons learned at the State Department?**

Response: No. However, we will raise this at the next PCIE / ECIE meeting.

**14. Have you secured the cooperation of the other agencies (e.g., DOJ, DHS, and OPM) that share access to PERS to ensure that they mirror the reforms under way at the State Department?**

Response: We have forwarded this query to the Bureau of Legislative Affairs as this question was not a part of our initial quick-response review. We understand that Department bureaus, which were not part of the July 10, 2008 hearing, are prepared to respond to these committee questions upon receipt from the committee. The response to this query will be reviewed by the OIG for possible inclusion in compliance reporting or future reviews of this system. The point of contact for these responses is Steve Zate at the Bureau of Legislative Affairs. His contact number is (202) 647-8734.

ALAN CHARLES RAUL  
1501 K STREET, NW  
WASHINGTON, DC 20005  
202-736-8477 (OFFICE)  
ARAUL@SIDLEY.COM

August 11, 2008

The Honorable Patrick J. Leahy  
Chairman, Committee on the Judiciary  
United States Senate  
152 Dirksen Senate Office Building  
Washington, DC 20510

The Honorable Arlen Specter  
Ranking Member, Committee on the Judiciary  
United States Senate  
224 Dirksen Senate Office Building  
Washington, DC 20510

Dear Chairman Leahy and Senator Specter:

As requested, I am providing my responses to the Questions for the Record propounded to me by Senator Specter following the Committee's July 10 hearing on "Passport Files: Privacy Protection Needed For All Americans." I was pleased to be able to testify at that hearing, and to provide the responses attached to this letter. (The views expressed here are my own, and do not represent the views of my law firm, or any of its partners, personnel or clients.)

In brief, though I have not comprehensively reviewed, and thus cannot subscribe to all aspects of the bill, I support the basic thrust of the Leahy-Specter legislation, S. 495, the "Personal Data Privacy and Security Act." I believe that federal standards in this area can offer necessary and appropriate substantive protections, while ensuring that privacy and data security standards in the United States develop in a rational, nation-wide manner. National leadership in this area is particularly important given the global, indeed largely non-territorial, nature of digital communications and databases.

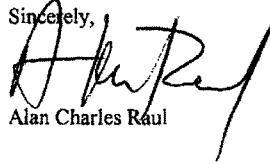
In addition, based on my experience in the private practice of Information and Privacy Law, as former General Counsel of the Office of Management and Budget, and former Vice Chairman of the White House Privacy and Civil Liberties Oversight Board, I would support the statutory designation of a lead federal privacy office. I recommend that the federal privacy office should have a clear legislative mandate, and should be placed in the Office of Management and Budget, perhaps by creating an Office of Privacy and Information Policy.

The Honorable Patrick J. Leahy  
 The Honorable Arlen Specter  
 August 11, 2008  
 Page 2

The OMB privacy office could coordinate all federal Chief Privacy Officers, and consult closely with the Federal Trade Commission, banking agencies, the Justice Department, Departments of Homeland Security and Health and Human Services, Federal Communications Commission, etc., regarding enforcement matters, and with respect to privacy and cyber-security in particular regulatory sectors. OMB is highly conversant with privacy and data security issues based on its responsibilities for helping develop Privacy Act policies, and policies and practices to secure personal information held by the federal government. OMB is fundamentally a policy development and coordination operation, and already plays a coordinating role with federal Chief Information and Privacy Officers.

Federal privacy and data security leadership will help establish a higher national priority for these important issues, and will allow the United States to address these issues more effectively with the European Union and other international jurisdictions.

Again, thank you for the opportunity and honor to testify before you and other members of the Senate Judiciary Committee. I would be pleased to work further with the Committee, if I can be of assistance.

Sincerely,  
  
 Alan Charles Raul

Attachment:  
 "Privacy and the Digital State: Balancing Public  
 Information and Personal Privacy"

Responses of Alan Charles Raul to Questions for the Record

1. The mens rea requirements applicable to criminal violations of the Privacy Act do not necessarily seem inappropriate. Privacy Act violations can also be sanctioned and deterred with civil remedies (including damages against non-compliant agencies) and with employment actions (including termination and other administrative discipline against malfeasant agency personnel).
2. It should be clear that unauthorized access to or use of protected personal information constitutes a prohibited disclosure for purposes of the Act's penalties (i.e., clarify that such conduct is prohibited to the extent such unauthorized access or use is not already covered in the prohibition against requesting or obtaining records under "false pretences," *see* 5 U.S.C. § 552a(i)(3)).
3. I have not conducted an in depth review of the literature and reports regarding possible updating of the Privacy Act for electronic records since I completed writing "Privacy and the Digital State: Balancing Personal Privacy and Public Records," in 2001 (Kluwer Academic Publishers, 2001). Accordingly, I will defer to my prior publication, copies of which are being forwarded for the Committee's consideration. (Copies provided to Chairman Leahy and Senator Specter).
4. In general, I support the thrust of the draft Leahy-Specter Personal Data Privacy and Security Act. I believe that rational federal privacy and data security legislation can help assure the public that their personal information will be adequately protected and also provide coherent and predictable national standards for the entities that collect, process, use and transfer such information. Reasonable national standards are particularly important in an area described by Judge Loretta A. Preska, in *American Library Association v. Pataki* (969 F. Supp. 160 (S.D.N.Y. 1997)) as "a national preserve" where "users [must be protected] from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether." In addition, federal legislation will help combat the erroneous impression *au courant* among some EU officials that the United States does not offer robust privacy protection. That is not true at all, but the absence of cross-sector federal legislation has allowed the misimpression to take root.
  - a. I have not undertaken to date a comprehensive, detailed review of S. 495. I would be happy to work further with the Committee if that would be of value.
  - b. In general, I would recommend that where the draft legislation can be rendered more general and less prescriptive, compliance burdens can be made more reasonable without sacrificing substantive protections. The bill should, quite simply, be streamlined and made shorter.
  - c. In my opinion, the legislation should designate a primary federal agency with responsibility for administering and interpreting the legislation and helping

develop government-wide privacy and data security policy; that agency should be an office within the Office of Management and Budget, which is already responsible for privacy and data security for information held by the government information. The OMB privacy office should be directed to consult and coordinate with other federal agencies on enforcement matters, especially the FTC, banking agencies, HHS, Justice Department, Homeland Security, FCC, and other agencies responsible for privacy and cyber-security in different sectors.

DC1 1245183v.1

August 28, 2008

Chairman Patrick Leahy  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Dear Senator Leahy,

Enclosed please find answers to the questions submitted by Senator Spector and Senator Feingold, following the July 10, 2008 hearing before the Judiciary Committee on "Passport Files: Privacy Protection Needed for All Americans."

Thank you again for the opportunity to participate in this important hearing.

Sincerely,

Marc Rotenberg  
EPIC Executive Director

Enclosure

## Question from Senator Specter

*Why do you think the OMB has failed to do its job of ensuring that all agencies enforce and comply with the Privacy Act? Is there a single agency that might be better suited to discharge the duties currently executed by the OMB Director?*

Senator, the fundamental reason that the OMB has failed to ensure that all federal agencies comply with the Privacy Act is that the agency lacks the authority and independence to enforce the federal privacy law. As the Privacy Act was originally conceived, an independent privacy agency would have been established for the purpose of overseeing compliance with the law. Unfortunately, the privacy agency was removed from the version of the bill approved by the Congress to obtain the support of the Ford White House. I believe this was done at the urging of President Ford's Chief of Staff Richard Cheney.

Virtually every privacy scholar who has examined the structure of US privacy law since the passage of the Privacy Act has noted that the US lacks an agency that has the authority to oversee and enforce what is otherwise considered a generally good privacy law. I wrote on this issue in the late 1980s and worked with the late Senator Simon on legislation to establish a privacy agency. Unfortunately that bill did not receive enough votes in the Senate for passage.

Over the last several years we have pressed the OMB to play a more active role in the enforcement of the Privacy Act. In 2003, EPIC and almost 100 organizations urged the OMB to reject a proposal from the FBI to exempt the National Crime Information Center from the accuracy requirements of the Privacy Act. We cited concerns that had been expressed by Justice O'Connor in the 1995 case *Arizona v. Evans* that acknowledged the importance of new technology for law enforcement but also emphasized the need to ensure the accuracy and reliability of police databases. The OMB ignored this concern and allowed the FBI to go forward with the Privacy Act exemption. The most recent report from the Bureau of Justice Statistics indicates ongoing problems with the reliability of the NCIC. This is just one example of the OMB's failure to safeguard the interests set out in the Privacy Act.

It is also interesting to note that virtually every other country that has enacted a comprehensive privacy law, similar to the Privacy Act, has also established an independent privacy commission to ensure compliance with privacy laws and to pursue privacy investigations. These "Data Protection Authorities" have provided a bulwark for the privacy rights of citizens against the incursion of both government and the privacy sector and continue to play an important role identifying emerging privacy challenges. The Article 29 Working Group of the European Commission, for example, issues widely respected reports and assessments of new privacy issues. There is nothing comparable in the United States, which is unfortunate and makes policy making on privacy challenges less well informed and privacy solutions more difficult to achieve.

While I believe it was appropriate to designate an individual within OMB responsible for privacy compliance during the administration of President Clinton, the long-term solution and the necessary solution is to establish an independent agency with the authority to ensure compliance with the Privacy Act as was intended originally.

It is conceivable that the newly constituted Civil Liberties and Privacy Oversight Board could play a more significant role in the oversight of the Privacy Act, but that entity was established specifically to address the new surveillance authorities of the federal government established after 9-11 and not the routine privacy issues that arise across the federal government, such as the mishandling of passport records by a private contractor.

## QUESTIONS FROM SENATOR FEINGOLD

1. *It's apparent that many federal agencies are not taking seriously enough their obligation to protect the privacy of the personal information in their custody and control. What's needed here, in addition to a stronger legal framework, is a culture of respect for privacy rights within our federal government. Do you have any thoughts about such a culture could be fostered?*

Senator, I believe that the federal Privacy Act provides the essential framework that makes clear the responsibility that federal agencies have to ensure privacy protection. Compliance with the Privacy Act is the primary measure of agencies willingness to take seriously the obligation to safeguard privacy. Unfortunately, too many agencies seek to exempt themselves from Privacy Act obligations or discharge their legal obligations to private contractors over whom they exercise little control.

Remarkably, the Department of Homeland Security, the agency responsible for many of the most extensive data collection activities in the last several years, has a terrible record for Privacy Act compliance. The agency routinely seeks exemptions from Privacy Act obligations and it has had several notable data breaches, including the loss of information on 100,000 employees including undercover federal air marshals.

I believe that the Congress and the next Administration must send a much clearer message to federal agencies that if they fail to protect the information that they collect, that if they do not comply with the Privacy Act, budgets will be cut and agency staff will be asked to step down. Neither the Congress nor the President should tolerate the mismanagement of personal information by any federal agency.

2. *Accountability is an important part of fostering a culture of respect for privacy. In other words, there must be strict liability and strict consequences for breaches of privacy.*

- a. *Do we know, at this time, whether each and every State Department employee and contractor who was found to have improperly accessed passport files has been removed from his or her State Department duties?*

Senator, I am not aware of the status of these investigations. While I agree that individuals should be held accountable for their acts, since this matter involved the use of a private contractor who conducted work on behalf of the agency, a more effective sanction in this instance may be to simply suspend any further contracts with this company until there is assurance that these incidents will not be repeated. This would send a clear message to other federal contractors that they must take seriously the obligation to safeguard the personal information they obtain.

- b. *The contract employees who gained unauthorized access to the passport files included individuals employed by Stanley, Inc. and the Analysis*

*Corporation. What consequences, if any have, there been for these companies? Do they still hold contracts with the State Department?*

Senator, I understand that subsequent to the Committee hearing on the passport issue in July, there was a provision included in the FY2009 appropriations bill for the Department of State that withholds funds until all of the recommendations of the Inspector General to improve controls over access to passport files are implemented. The practical consequence of this provision may be to suspend future payments to these firms until the privacy concerns are addressed.

Question Submitted by U.S. Senator Feingold to Ari Schwartz:

1. The President released a "National Strategy for Information Sharing" in October 2007. The strategy envisions unprecedented sharing of Americans' personal information among federal, state, local, and foreign governments, as well as the private sector. According to the strategy, the privacy of this information will be safeguarded by a set of privacy guidelines that have been developed by the Attorney General and the Director of National Intelligence. These guidelines are available at:  
<http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf>

a. Do you have any concerns about the content of the guidelines?

CDT prepared a detailed analysis of the privacy guidelines, which were issued in 2006. <http://www.cdt.org/security/20070205iseanalysis.pdf>. We pointed out that these privacy guidelines fail to even define privacy or specify the "other legal rights" or "applicable laws" that ISE participants must follow. Privacy is a broad and widely misunderstood concept, and agencies need more guidance than is included in these guidelines. We have consistently called for the use of Fair Information Practices (FIPs) in cases like these; a checklist or guide using the FIPs would be much more clear and substantial than the guidelines here. Since 2006, the Program Manager's office has issued additional privacy materials for agencies participating in the ISE, <http://www.ise.gov/pages/privacy-overview.html>, most recently compiled in a Privacy and Civil Liberties Implementation Workbook. However, the new material, while providing additional detail, still fails to give adequate direction to agencies. Still, agencies are instructed to "take appropriate steps" with only a list of resources to provide further guidance as to what steps might be appropriate.

b. Aside from the guidelines' content, do they have the force of law?  
 What is the penalty if an agency doesn't adhere to them?

The guidelines have no force of law and, strictly speaking, the ISE Program Manager has no authority to enforce them. While the elements of the ISE are subject to the Privacy Act, that Act is riddled with exemptions, which this Administration has been quick to invoke. One of the problems with the guidelines is that they make no effort to restrain agencies in exempting their data from key sections of the Privacy Act. Under the guidelines, an agency that exempts its records from the Privacy Act is "complying with" the Privacy Act.

Question from Senator Specter to Ari Schwartz:

1. In your testimony, you called for stiffer criminal penalties for Privacy Act violations concerning Passport Records. Is there any reason why those covered records should be treated differently than other covered records maintained by government agencies?

It is true that Privacy Act penalties in general currently lack the force to provide strong protections for Americans. However, we have seen in several cases where stiffer penalties for a certain type of records that have been repeatedly abused have raised privacy awareness instantly in the agencies that hold those records. Laws passed for tax, veterans, census and social security records have clearly led to more resources and innovations in privacy protections at the agencies holding those records. The repeated and egregious violations of passport records suggest that stronger protections will be necessary to immediately change the culture at the State Department. Meanwhile, as I suggested in my testimony, Congress should be working to amend the Privacy Act to ensure that it covers all the types of information and has sufficient enforcement mechanisms and penalties across the board.

SUBMISSIONS FOR THE RECORD

REMARKS OF MARK W. DUDA

ASSISTANT INSPECTOR GENERAL  
FOR AUDITS

U.S. DEPARTMENT OF STATE AND BROADCASTING

BOARD OF GOVERNORS

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

ON

CONTROLS AND NOTIFICATION FOR ACCESS TO  
PASSPORT RECORDS IN THE DEPARTMENT OF STATE'S  
PASSPORT INFORMATION ELECTRONIC RECORDS  
SYSTEM

JULY 10, 2008

Chairman Leahy, Ranking Member Specter, members of the Committee, thank you for the opportunity to discuss the results of our review of controls over access to passport records in the Department of State's Passport Information Electronic Records System, which is known as the PIERS system.

On March 21, 2008, following the first reported breach of a presidential candidate's passport records and at the direction of the former Acting Inspector General, the Office of Inspector General, Office of Audits, initiated this limited review of Bureau of Consular Affairs controls over access to passport records in PIERS. Specifically, this review focused on determining whether the Department:

- (1) adequately protects passport records and data contained in PIERS from unauthorized access and
- (2) responds effectively when incidents of unauthorized access occur.

During Fiscal Year 2007, the Department issued almost 18.4 million passports domestically and participated or assisted in the issuance of about 365,000 passports overseas.

According to Consular Affairs officials, there were about 20,500 users with active PIERS accounts as of May 2008, and about 12,200 of these users were employees or contractors of the Department. PIERS is also accessed by users at other federal departments and agencies, including the Department of Homeland Security, the Federal Bureau of Investigation, and the Office of Personnel Management, to assist in conducting investigations, security assessments, and analyses.

In our review, 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 and the subsequent response and disciplinary processes when a potential unauthorized access is substantiated.

In some cases, Department officials stated that the lack of resources contributed to the lack of controls and to the Department's ability to assess vulnerabilities and risk. OIG described some security and management practices utilized by the Internal Revenue Service and the Social Security Administration as examples where similar improvements can be made by the Department.

OIG made 22 recommendations to address the control weaknesses found with safeguarding passport records. We did not verify instances of unauthorized access, but it did conduct a judgmentally determined study at the initiation of this review to identify the frequency with which the records for 150 high-profile individuals were accessed in PIERS between September 2002 and March 2008. Our results revealed several patterns that raised serious concerns about the potential for undetected unauthorized access to passport records. Of the 150 names included in the study, OIG found that the records of 127 individuals, or 85 percent, had been accessed at least one time. The query results showed a total of 4,148 hits to the passport information for these individuals. OIG made no determination as to whether the hits represented authorized or unauthorized access. Further, although an 85 percent hit rate appears to be excessive, the Department currently lacks criteria to determine whether this is actually an inordinately high rate.

As stated by the Acting Inspector General, following the publicized passport record breaches, the Department implemented a number of corrective actions and has other efforts planned, as detailed in the report.

Of the 22 recommendations made OIG considers 19 recommendations resolved and three recommendations unresolved based on the responses by Department officials. To ensure that adequate and timely progress is achieved, we will conduct a follow-up compliance review of the Department's implementation of the recommendations in this report, as well as Consular Affairs' process for reviewing possible unauthorized accesses by users as identified in our study.

Thank you for the opportunity to appear before you today. I would gladly answer any questions you may have.

**Statement of U.S. Senator Russ Feingold**  
**Senate Judiciary Committee Hearing**  
**“Passport Files: Privacy Protection Needed For All Americans”**  
**July 10, 2008**

Thank you, Mr. Chairman. I think the Report of the Inspector General raises some very important issues, and I’m pleased that you’re putting some much-needed attention on those issues.

It is both shocking and shameful that State Department employees and private contractors were able to access the passport files of Senators Obama, Clinton, and McCain without any legitimate reason. Like all Americans, these Senators have a right to know that their personal information is safe and secure in the hands of the federal government, and will not be subject to unauthorized snooping and prying.

But what’s even more disturbing to me is what the Inspector General’s Report may mean for Americans we didn’t read about in the news. The reason we learned about the unauthorized access to the three candidates’ files is that the State Department has a system for monitoring access to the records of high-profile individuals. But if you’re not on that list of high-profile Americans, your records could be accessed a dozen times a day, and – based on what’s in this Report – it’s likely no one would ever know. I fear that the high-profile cases are just the tip of the iceberg, and that the real victims of the State Department’s failures are ordinary Americans across the country, who had little choice but to entrust their personal information to an agency that wasn’t protecting it.

And there’s an even larger issue at stake. As many of our witnesses have pointed out, a perfect storm of factors has combined in recent years to create an unprecedented threat to the privacy of Americans’ personal information. There has been a dramatic increase in the amount of personal information about Americans that the federal government collects and retains. There has also been a marked increase in information-sharing across government agencies. And the federal government has increasingly relied on private contractors, both to manage this information and to perform jobs that require access to it. Each of these factors carries with it a heightened risk of unauthorized access and disclosure.

Against that backdrop, the Inspector General’s Report is particularly sobering. At a time when the risk of privacy violations is higher than ever before, at least some of our agencies continue to operate without even the most basic privacy protections in place. While federal laws like the Privacy Act of 1974 and the E-Government Act of 2002 provide some protection, they don’t go nearly far enough – and, as the passport incidents show, they are only as effective as the means in place to enforce compliance. We need stronger laws and better implementation –

and we need them before, not after, any significant further expansion in the universe of personal information that the federal government keeps and shares. At a minimum, Congress should act quickly to pass the Personal Data Privacy and Security Act, a bill that we reported out of this committee last year and that I was pleased to cosponsor.

There's another issue that bears mention. The Inspector General's Report was publicly issued in heavily redacted form, although it is not classified. The apparent justification for the redactions was that some of the information relates to internal personnel rules of no real public interest, or that revealing the information could enable the evasion of agency rules. Based on a review of a redacted version and an unredacted version of this report, there appears to be no legitimate justification for many of these redactions. In some cases, it seems clear that the purpose of the redactions was to shield information that could be embarrassing to the government. If only the administration were as intent on protecting the personal information of Americans – information that truly should be private – as it is on shielding information about the workings of government, which every American has a right to know.

I hope that the passport file incidents and the Inspector General's Report serve as a wake-up call, and that we refer back to this hearing and the recommendations of the witnesses before putting our seal of approval on any additional administration proposals to expand federal collection, retention, and sharing of Americans' personal information.

REMARKS OF HAROLD W. GEISEL  
INSPECTOR GENERAL (ACTING)

U.S. DEPARTMENT OF STATE AND BROADCASTING  
BOARD OF GOVERNORS  
BEFORE THE  
UNITED STATES SENATE  
COMMITTEE ON THE JUDICIARY  
ON  
CONTROLS AND NOTIFICATION FOR ACCESS TO  
PASSPORT RECORDS IN THE DEPARTMENT OF  
STATE'S PASSPORT INFORMATION ELECTRONIC  
RECORDS SYSTEM

JULY 10, 2008

Chairman Leahy, Ranking Member Specter, members of the Committee, thank you for inviting me to discuss with you the privacy concerns reported in the results of our review of controls over access to passport records in the Department of State's Passport Information Electronic Records System or PIERS system. The full report has been provided to the Committee.

In March 2008, media reports surfaced that the passport files maintained by the Department of State (Department) of three U.S. Senators, who were also presidential candidates, had been improperly accessed by Department employees and contract staff. On March 21, 2008, the Office of Inspector General, Office of Audits, initiated a limited review of Bureau of Consular Affairs controls over access to passport records, and issued the final report one week ago, on July 2, 2008. The OIG made 22 recommendations to address the control weaknesses and the Department concurred with 19 of them, partially agreed with one and did not agree with two recommendations.

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 and the subsequent response and disciplinary processes when a potential unauthorized access is substantiated.

As of April 2008, PIERS contained records on about 192 million passports for about 127 million passport holders. These records include personally identifiable information or P-I-I , as it is known, such as the applicant's name, gender, social security number, date and place of birth, and passport number. PIERS also contains additional information, such as previous names used by the applicant, citizenship status of the applicant's parents or spouse, and scanned images of passport photos. PIERS offers users the ability to query information pertaining to passports and vital records, as well as to view and print original copies of the associated documents. As a result, PIERS records are protected from release by the Privacy Act of 1974. Unauthorized access to PIERS records may also constitute a violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030).

At the time of the publicized breaches, neither Consular Affairs nor the Department had implemented breach notification policies, procedures, or other criteria for reporting incidents of unauthorized access of passport records when they were detected. However, between March and May 2008, Consular Affairs and the Bureau of Administration took a number of corrective actions, including issuing interim guidance on the various steps to be followed and decisions to be made in response to a potential incident of unauthorized access to passport records and applicant personally identifiable information, and a Department-wide P-I-I breach response policy.

While these immediate actions taken are commendable, OIG has recommended that the Department conduct the necessary vulnerability and risk assessments of all passport systems given the weaknesses and data vulnerabilities identified in this limited review of PIERS. Accordingly, OIG believes that the Department should make resources available to conduct the assessments as quickly as possible.

OIG also recommended that CA ensure the accuracy of its Privacy Impact Assessments for PIERS and for all other passport systems to accurately reflect security controls for and risks to personally identifiable information.

I would like to introduce Mr. Mark W. Duda, Assistant Inspector General for Audits, who led this review and will provide a summary of the findings.

Thank you for the opportunity to present this timely information to you today. Following Mr. Duda's remarks, we would be happy to answer any questions you may have.



United States Department of State  
*Under Secretary of State  
 for Management*  
 Washington, D.C. 20520

July 4, 2008

Dear Mr. Chairman:

Last March, after briefing Secretary Rice, I asked our Inspector General to investigate and report on the improper accessing of passport applications that had come to light. Yesterday we received the report and, regrettably, it confirms our suspicions: there have been numerous improper accesses of passport files and that, while our tracking system records all accesses, there were insufficient procedures and systems in place to oversee and follow-up on abuses.

I can report to you that, while there is more to be done, we have already taken a number of steps to ensure Americans' passport data will be as protected as possible. We have instituted numerous new safeguards, some of which we have already briefed to your staff in the period following the initial revelations. Our reform efforts have not ended and appointments are being scheduled to brief your staff on the actions we have already taken, as well as those we will be implementing to ensure that all access to passport information is appropriate and that should future cases of inappropriate activities arise they will be dealt with immediately.

A new leadership team (Assistant Secretary for Consular Affairs Janice Jacobs and Deputy Assistant Secretary for Passport Service Brenda Sprague) will vigorously implement the recommendations of the Inspector General; and many of them, in fact, parallel actions that we began to put in place after these abuses came to light. A working group, with representatives from throughout the Department, has been meeting regularly to reform our operating procedures, improve our systems, and ensure that any violations are dealt with expeditiously. A number of changes have already been put into place to ensure the protection that each and every passport holder is entitled. And I pledge my own personal attention and oversight.

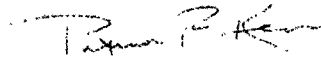
The Honorable Patrick J. Leahy,  
 Chairman,  
 Subcommittee on State, Foreign Operations, and Related Programs,  
 Committee on Appropriations,  
 United States Senate.

We are currently reviewing previous cases of potentially improper access and will refer to the Inspector General any that are determined to be without justification. The results of these OIG reviews will then be forwarded to the Bureau of Human Resources for disciplinary action as appropriate.

Again, let me express my deep regret that the actions of a number of State Department employees and contractors have been improper. The Department takes very seriously its obligation to provide passport services to the American people and to do so in a manner that is fully consistent with law and regulation.

I am at your disposal to meet with you at any time should you so desire.

Sincerely,



Patrick F. Kennedy

**Statement of Senator Patrick Leahy,  
Chairman, Senate Committee on the Judiciary  
Hearing on “*Passport Files: Privacy Protection Needed  
For All Americans*”  
July 10, 2008**

Today, the Committee holds an important hearing on the unauthorized access of Americans' passport files. Millions of Americans entrust their personal information to the State Department in order to obtain passports and other services, and our government has a duty to protect the private information of its citizens. But, sadly, the State Department has failed to honor this duty, leaving millions of ordinary Americans vulnerable to privacy violations, identity theft and other crimes.

Last week -- while Americans were celebrating Independence Day -- the State Department's Acting Inspector General issued a report finding that State Department workers and contractors repeatedly accessed the passport files of entertainers, athletes and other high-profile Americans without proper authorization. This disturbing revelation of passport snooping comes after press reports in March that the passport files of three presidential candidates -- Senators Obama, Clinton and McCain -- were improperly accessed by State Department contractors.

The Inspector General's findings raise serious concerns about possible violations of the Privacy Act and other Federal laws meant to protect Americans' privacy. According to the report, 85% of the passport records included in a sample of high-profile Americans had been searched at least once -- and many files were searched multiple times -- during a five and a half year period. In fact, one individual's passport records were searched 356 different times by 77 different users, according to the report.

More significantly, the Inspector General's report reveals that the records of millions of ordinary Americans are also vulnerable to privacy breaches. There are no checks in the system to even determine if the passport files of ordinary Americans are accessed. Although these passport files contain sensitive personal information, including name, date and place of birth, and Social Security numbers, the Inspector General's report found widespread control weaknesses at the State Department -- including a general lack of policies, procedures, guidance and training -- to prevent and detect the unauthorized access of Americans' passport files. According to the report,

the Department's *Passport Information Electronic Records System* (PIERS) contains the passport records for approximately 127 million passport holders. As more Americans need a passport just to travel to visit family and friends in our neighboring countries, like Canada, due to the Western Hemisphere Travel Initiative, the number of passport files to protect grows.

The State Department could not readily identify the universe of government workers and contractors who have access to this information. The Inspector General estimates that this figure exceeds 20,000 government employees from various agencies and outside contractors. The tip of the iceberg in this report is the fact that passport information is shared with other agencies and we have no idea what procedures are followed to protect information once it leaves the State Department. The State Department Inspector General has referred this serious matter to the Justice Department, and I hope the Department's Criminal Division will investigate this thoroughly.

The lax data security at the State Department is not unique. A week does not go by without reports of personal data privacy breaches at government agencies and private businesses. Just recently, front page headlines have delivered news about the theft of sensitive medical information from the National Institutes of Health, and earlier reports of data breaches have involved virtually every department of our Federal Government. The Inspector General's report is just the latest example of why swift action is needed on the Leahy-Specter *Personal Data Privacy and Security Act* – a comprehensive privacy bill that would help to prevent data security breaches and provide further protections in the handling of Americans' private data by Federal agencies and government contractors. I hope that the Senate will promptly consider and pass this bill, so that we can help make a difference for all Americans.

Data privacy and security at our federal agencies is a serious and growing problem that Congress must address. To do so, we must not only understand what went wrong at the State Department, but also look forward to how best to prevent these kinds of privacy violations in the future. I am pleased that the Department's Acting Inspector General and Assistant Inspector General for Audits are here to share their findings. We also have a distinguished panel of privacy experts to address this issue. I thank all of our witnesses for coming and I look forward to a productive discussion.

#####

**Testimony of**  
**Alan Charles Raul**  
**Before the United States Senate**  
**Committee on the Judiciary**  
**July 10, 2008**

**“Passport Files: Privacy Protection Needed For All Americans”**

Chairman Leahy, Senator Specter, and members of the Committee, thank you for inviting me to testify on protecting the privacy of passport files maintained by the U.S. Department of State. It is an honor to appear before you.

I am testifying today in a personal capacity based on my interest and background in privacy, information security and administrative law. I am currently engaged in private law practice in Washington, D.C., where I focus on privacy, data security and Internet law, as well as on government regulation and enforcement. Until recently, I also served in a part-time capacity as Vice Chairman of the White House Privacy and Civil Liberties Oversight Board. I am author of the book, “Privacy and the Digital State: Balancing Public Information and Personal Privacy” (Kluwer Academic Publishers, 2002), which discusses data protection for public records held by government agencies. I have also previously served as General Counsel of the U.S. Department of Agriculture, General Counsel of the Office of Management and Budget, and Associate Counsel to the President.

This hearing arises because of a recent investigation and report by the State Department’s Inspector General indicating that the passport files of high profile individuals may have been improperly accessed by State Department employees and contractors. The Inspector General’s investigation was triggered by media reports of improper access to the files of three Presidential candidates, namely Senators McCain, Obama and Clinton. Neither the Inspector General nor other State Department officials have suggested that there was any authorized or proper government purpose for rummaging through these files. Accordingly, the State Department announced this week that it had terminated between five and eight contractors in connection with what appear to be serious violations of personal privacy, federal law, and internal controls.

While the investigation apparently continues, if the facts turn out to be as they now appear, there is no question that the standards of the Privacy Act of 1974 were not satisfied. The Privacy Act states that: "No agency shall disclose any record . . . except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be . . . to those officers and employees . . . who have a need for the record in the performance of their duties." To the extent agency employees and contractors accessed passport files with no official need to do so, they disrespected the privacy of affected passport holders and applicants, and brought substantial disrepute upon their agency.

The Privacy Act, the e-Government Act of 2002 and the Federal Information Security Management Act of 2002 ("FISMA"), all require government agencies to adopt and implement effective controls to prevent just the sort of invasion of personal information that occurred here. For example, the Privacy Act mandates that government agencies "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."

Moreover, each of these Acts authorizes the Director of the Office of Management and Budget to assist, guide and oversee federal efforts in the realm of privacy and information security. OMB's coordination of information privacy is reflected in its FY 2005 report to Congress under the e-Government Act. *See* [http://www.whitehouse.gov/omb/egov/documents/Promoting\\_Information\\_Privacy\\_Sec208.pdf](http://www.whitehouse.gov/omb/egov/documents/Promoting_Information_Privacy_Sec208.pdf). Congress and the White House should continue to support and encourage OMB's leading role in the field of privacy and information security.

With regard to the specific incident at hand, it is not clear at this point whether any of the individuals whose files were accessed experienced any pecuniary losses or other actual damages to support claims of civil liability under the Supreme Court's *Doe v. Chao* decision in 2004. However, if any agency employee or contractor "willfully disclose[d] the material in any manner to any person or agency not entitled to receive it," or "knowingly and willfully request[ed] or obtain[ed] any record concerning an individual from an agency under false pretenses," they could be guilty of a criminal misdemeanor and fined up to \$5,000.

It is perfectly clear now, however, that existing law and applicable guidance should have prevented State Department employees and contractors from engaging in frolics and detours – or worse – through the passport files of politicians, prominent figures, or indeed, of any Americans. The fact that these files were subject to access for no good reason is highly troubling. We expect the government to do much better in safeguarding our personal information. Indeed, the State Department Inspector General indicated in his report that other agencies, such as the Treasury Department, IRS, and Social Security Administration are doing better; these agencies, according to State’s IG, “ha[ve] established more controls to prevent and detect unauthorized access than had the [State] Department.”

Plainly, the State Department must redouble its efforts to conduct privacy impact and risk assessments, communicate binding privacy policies to all parties handling personal information, provide its employees and contractors with meaningful privacy and data security training, ensure effective audit trails for accessing personal information, and establish clear guidelines for disciplining and terminating employees and contractors who transgress. The State Department should also revisit its administrative, technical and physical safeguards to prevent future abuse of passport files and other personal records.

At the same time, care must be taken to avoid unduly restricting access to information that is essential for national security purposes. As the 9/11 Commission recommended, and Congress enacted, the country has a critical need to promote an “information sharing environment” that transcends traditional governmental boundaries in order to help prevent future terrorist attacks. But the relevant government agencies, including the State Department, must effectively integrate protections for privacy and other civil liberties into this new information sharing environment.

In any event, if the Executive Branch wishes to hold the private sector, state governments and foreign nations to high standards for information privacy and security, it needs to be a consistently good role model for privacy itself. To that end, the government obviously has plenty of room for improvement under existing privacy laws and standards for information security.

Thank you for considering my views.



**ELECTRONIC PRIVACY INFORMATION CENTER**

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.<sup>1</sup> 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

---

<sup>1</sup> 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.<sup>2</sup> The State Department concluded that Clinton's file was accessed purposefully to influence the outcome of the presidential election.<sup>3</sup> 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 candidates earlier this year. In March of 2008, the State Department announced that on three different dates Senator

<sup>2</sup> 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>.

<sup>3</sup> 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.<sup>4</sup> Two of the employees were terminated, while the third was disciplined.<sup>5</sup> 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".<sup>6</sup> Sen. Obama's passport file breach was detected by a monitoring system.<sup>7</sup> The monitoring system is "tripped" when an employee accesses the record of a high-profile individual.<sup>8</sup> 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 Condoleezza 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."<sup>9</sup>

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

---

<sup>4</sup> 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>.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> Obama urges inquiry into passport snooping" (March 21, 2008), <http://us.cnn.com/2008/POLITICS/03/21/obama.passport/index.html#cn-STCVideo>

of private passport information.”<sup>10</sup> 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.”<sup>11</sup> 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.”<sup>12</sup>

*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.<sup>13</sup> The IG’s report founds numerous problems in the system used to protect confidentiality of passport records and made 22 recommendations to improve it.<sup>14</sup> The report further noted a general lack of policies, procedures, guidance, and training regarding the prevention

<sup>10</sup> Statement on Breach of Senator Clinton’s Passport File, (March 21, 2008), <http://www.clinton.senate.gov/news/statements/details.cfm?id=295036&&>.

<sup>11</sup> CNN Video (March 21, 2008), <http://www.cnn.com/video/#/video/politics/2008/03/21/america.votes.friday.cnn?iref=videosearch>

<sup>12</sup> Helene Cooper, *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/>.

<sup>13</sup> 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*].

<sup>14</sup> *Id.* at 4.

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

## **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.<sup>17</sup> Contractors assist “government employees by answering customer service enquiries, printing and mailing issued passports, and entering data.”<sup>18</sup> Contractors comprised between 40-45% of the total employees at passport agencies and centers since 2001.<sup>19</sup> 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.<sup>20</sup> 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.”<sup>21</sup>

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

<sup>15</sup> *Id.* at 1-4; *See also id.* at 39-42.

<sup>16</sup> *Id.* at 1-4.

<sup>17</sup> 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/t/pa/prs/ps/2008/mar/102569.htm>.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

and The Analysis Corporation.<sup>22</sup> On March 17, 2008, just days before the public learned of the breaches of 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.<sup>23</sup>

### **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.”<sup>24</sup> 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

<sup>22</sup>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>.

<sup>23</sup> 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>

<sup>24</sup> The White House, National Strategy for Information Sharing, October, 2007, *available at* [http://www.whitehouse.gov/nsc/infosharing/NSIS\\_\\_book.pdf](http://www.whitehouse.gov/nsc/infosharing/NSIS__book.pdf).

including "terrorism, homeland security or law enforcement information related to terrorism."<sup>25</sup> 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."<sup>26</sup>

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.<sup>27</sup> Fusion centers are the "primary focal points" for sharing of terrorism related information.<sup>28</sup> Private sector information sharing focuses on sharing with operators and owners of "critical infrastructure."<sup>29</sup> In receiving foreign information the "guiding objective" is to ensure that the US can disseminate the information "as broadly as possible."<sup>30</sup> Meanwhile, privacy is to be protected by a "Privacy Guidelines Committee" chaired by the Attorney General and the Director of National Intelligence.<sup>31</sup> The committee will consist of the privacy officers of the departments and agencies of the Information Sharing Council.<sup>32</sup>

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

---

<sup>25</sup> *Id.* at 27.

<sup>26</sup> *Id.* at 7-8,

<sup>27</sup> *Id.* at 17.

<sup>28</sup> *Id.* at 20.

<sup>29</sup> *Id.* at 21.

<sup>30</sup> *Id.* at 25.

<sup>31</sup> *Id.* at 28.

<sup>32</sup> *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.<sup>33</sup> Homeland Security subsequently created the Western Hemisphere Travel Initiative.<sup>34</sup> Air travelers were required to present a passport or secure travel documents beginning on January 23, 2007.<sup>35</sup> Land and Sea entry requirements will be fully implemented by June 2009.<sup>36</sup> These requirements have led to

<sup>33</sup> Pub. L. No. 108-458, § 7209(b), 108 Stat. 3637, 3823

<sup>34</sup> Department of Homeland Security, Western Hemisphere Travel Initiative, [http://www.dhs.gov/xprevprot/programs/gc\\_1200693579776.shtm](http://www.dhs.gov/xprevprot/programs/gc_1200693579776.shtm).

<sup>35</sup> 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).

<sup>36</sup> 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<sup>37</sup> 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.<sup>38</sup> A passport can be used to meet one of these standards for getting a driver's license.<sup>39</sup> Further, DHS Secretary Michael Chertoff has advised that a passport will serve the same federal purposes as a REAL ID compliant driver's license.<sup>40</sup> 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.*

<sup>37</sup> 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>.

<sup>38</sup> Pub. L. No. 109-13, 119 Stat. 231 (2005).

<sup>39</sup> 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).

<sup>40</sup> 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](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.*<sup>41</sup>

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.<sup>42</sup>

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.<sup>43</sup> 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."<sup>44</sup> For the purposes of the criminal liability provisions, employees of the contractor are considered to be agency employees.<sup>45</sup>

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

<sup>41</sup> Pub. L. No. 93-579, § 2(b), 88 Stat. 1896 (1974).

<sup>42</sup> 5 U.S.C. § 552a (e)(10).

<sup>43</sup> 5 U.S.C. § 552a (m).

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

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

*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."<sup>48</sup> 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"<sup>49</sup> and that a description of the disclosure be published in the Federal Register.<sup>50</sup> For its passport system, the State Department permits routine use disclosures of passport information to "contractor personnel conducting data entry, scanning, corrections and modifications."<sup>51</sup> 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.<sup>52</sup> The report notes:

<sup>46</sup> *OIG Report, supra* note 13, at 30.

<sup>47</sup> *OIG Report, supra* note 13, at 30-31.

<sup>48</sup> 5 U.S.C. § 552a (b)(3).

<sup>49</sup> 5 U.S.C. § 552a (a)(7).

<sup>50</sup> 5 U.S.C. § 552a (e)(4)(D).

<sup>51</sup> Department of State; *Privacy Act of 1974; System of Records*, 73 Fed. Reg. 1660, 1662 (January 9, 2008).

<sup>52</sup> 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.<sup>53</sup>

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."<sup>54</sup> The GAO calls these only "modest limits" on the use of information for multiple purposes within an agency.<sup>55</sup> 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.<sup>56</sup> 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.<sup>57</sup> 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

---

<sup>53</sup> *Id.* at 5.

<sup>54</sup> 5 U.S.C. § 552a (b)(1).

<sup>55</sup> Government Accountability Office, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536, 39 (May, 2008).

<sup>56</sup> 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>.

<sup>57</sup> *Id.*

telecommunications companies could share customer records with joint venture and independent contractors.<sup>58</sup> The FCC specifically noted that the risk of breaches increases when new parties gain access to personal information.<sup>59</sup> 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."<sup>60</sup>

*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 ...."<sup>61</sup> 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."<sup>62</sup> 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."<sup>63</sup> This

---

<sup>58</sup> *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](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf).

<sup>59</sup> *Id.* at 25.

<sup>60</sup> *Id.* at 23.

<sup>61</sup> *OIG Report*, *supra* note 13, at 1.

<sup>62</sup> 5 U.S.C. § 552a (c)(1).

<sup>63</sup> 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.<sup>64</sup> Further, the OIG found that this data is accessed via a Consular Consolidated Database web portal by other agencies.<sup>65</sup> 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.<sup>66</sup> After redactions, 6 of 22 recommendations made by OIG remained accessible to varying degrees.<sup>67</sup> In the 6 visible recommendations, the OIG made recommendations that the CA “consider,” “determine the feasibility of,” and “evaluate”<sup>68</sup> potential programs and policy amendments without specifics or mandates. Clear agency mandates which are effectively implemented are needed to protect privacy beyond these recommendations.

<sup>64</sup> *OIG report*, *supra* note 13, at 32.

<sup>65</sup> *Id.* at 33.

<sup>66</sup> *Id.*

<sup>67</sup> *Id.* at 40-42.

<sup>68</sup> *Id.*

Other recommendations include items such as evaluating the accuracy of Privacy Impact Assessments;<sup>69</sup> conducting vulnerability and risk assessments;<sup>70</sup> addressing third party disclosure and breaches;<sup>71</sup> and altering the agreements with agencies and entities that access PIERS data.<sup>72</sup> 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 data processing equipment.<sup>73</sup> That report led to the development and passage of the Privacy Act of

---

<sup>69</sup> *Id.* at 33.

<sup>70</sup> *Id.* at 34.

<sup>71</sup> *Id.* at 37.

<sup>72</sup> *Id.* at 36-7.

<sup>73</sup> 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.<sup>74</sup> But that report also made clear that the cornerstone of an effective federal policy is a permanent privacy agency.<sup>75</sup>

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.<sup>76</sup> Non-EU countries, from Canada<sup>77</sup> to Hong Kong,<sup>78</sup> are pursuing comprehensive privacy agendas led by privacy agencies. These government agencies routinely report on the handling of privacy complaints,<sup>79</sup> 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.*

<sup>74</sup> 5 U.S.C. § 552a (1974).

<sup>75</sup> HEW Report, *supra* note 73, at § 3.

<sup>76</sup> European Commission, Data Protection – European Commission, [http://ec.europa.eu/justice\\_home/fsj/privacy/law/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm).

<sup>77</sup> Office of the Privacy Commissioner of Canada, Mandate and Mission of the OPC, [http://www.privcom.gc.ca/aboutUs/index\\_e.asp](http://www.privcom.gc.ca/aboutUs/index_e.asp).

<sup>78</sup> Office of the Privacy Commissioner for Personal Data, Hong Kong, Homepage, <http://www.pcpd.org.hk/>.

<sup>79</sup> Office of the Privacy Commissioner of Canada, [http://www.privcom.gc.ca/i\\_i/index\\_e.asp](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."<sup>80</sup> 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."<sup>81</sup> Exemption 2 can be overcome if the documents in question relate to "substantial matters which might be the subject of legitimate public interest".<sup>82</sup>

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."<sup>83</sup> 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."<sup>84</sup> In the case of electronic passport records, the files can be accessed not only by government employees, but also private contractors.<sup>85</sup>

---

<sup>80</sup> 5 U.S.C. § 552 (b)(2).

<sup>81</sup> *Dep't of Air Force v. Rose*, 425 U.S. 352, 369-370 (1976).

<sup>82</sup> *Id.* at 365.

<sup>83</sup> *Founding Church of Scientology of Wash. v. Smith*, 721 F.2d 828, 831 (D.C. Cir. 1983).

<sup>84</sup> *Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 635 F.2d 887, 888 (D.C. Cir. 1980).

<sup>85</sup> *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.<sup>86</sup> 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.<sup>87</sup> 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,<sup>88</sup> 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.<sup>89</sup> 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.<sup>90</sup>

<sup>86</sup> *Dep't of Air Force v. Rose*, 425 U.S. 352 (1976).

<sup>87</sup> *Id.*

<sup>88</sup> *OIG Report*, *supra* note 13, at 1.

<sup>89</sup> *Id.*

<sup>90</sup> *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.”<sup>91</sup> 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.

---

<sup>91</sup> 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.<sup>92</sup> 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,”<sup>93</sup> not only serves those betrayed by

---

<sup>92</sup> *Id.* at § 303(a).

<sup>93</sup> *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.

**Testimony of Ari Schwartz**  
**Vice President of the Center for Democracy & Technology**  
**before the Senate Committee on the Judiciary**  
**on**  
**"Passport Files: Privacy Protection Needed For All Americans"**

**July 10, 2008**

Chairman Leahy, Ranking Member Specter, and members of the Committee, thank you for holding this hearing on the protection of personal information by the federal government. I am Ari Schwartz, Vice President of the Center for Democracy & Technology (CDT).

CDT is a non-profit public interest organization founded in 1994 to promote democratic values and individual liberties for the digital age. CDT works for practical, real-world solutions that enhance free expression, privacy, universal access and democratic participation.

**Summary**

Reports of illegal browsing of passport information by federal employees and contractors highlight concerns that the State Department has neither created adequate controls to protect the personal information of Americans nor enforced the basic privacy laws on these records. Even now, most of the State Department's controls protecting passport privacy focus on flagging the browsing of celebrity passport records. Meanwhile, we simply do not know how often the records of average Americans — including the neighbors, ex-girlfriends or relatives of those with access — have been browsed or for what purposes. Clearly, more must be done to protect the privacy of all passport holders.

However, the privacy issues requiring Congressional attention go beyond passport files and beyond the State Department.

In general, the State Department's privacy program has lacked vision, direction and resources for several years, demonstrating a lack of commitment to privacy protections. However, while the State Department clearly lags behind many other agencies, it is not alone in its failure to protect the information entrusted to it. As the General Accountability Office (GAO) has shown through a number of studies, privacy procedures are weak at many, though not all, of the largest agencies with the most sensitive personal information. This is because law, policy and practice have been allowed to lag behind the government's greater use of technology.

To adequately protect privacy in this digital age, when more information is collected and shared than ever before, Congress and the Executive Branch will need to work together to close the long-recognized gaps in existing laws and policies. At the same time, both branches must foster the leadership and insist upon the measurement capabilities needed

to ensure that existing and new laws and policies are implemented uniformly and diligently.

**Passport Records Browsing Demonstrates Larger Problems in State Department Privacy Program**

The recently released report from the State Department Inspector General (IG), entitled *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS)*, reveals that curious contractors and others accessed the passport files of many "high-profile" individuals. The IG concluded that there are many weaknesses in how the Department tries to prevent and detect the abuse of data in passport records. The IG also found that State Department Privacy Impact Assessments (PIAs) were not accurate in regards to the PIERS system.

The IG report shines a light on only one small part of a larger failing at the State Department. This report was a limited review to determine "whether the Department (1) adequately protects passport records and data contained in PIERS from unauthorized access and (2) responds effectively when incidents of unauthorized access occur." Furthermore, the full extent to which PIERS data has been abused is not apparent because the IG focused much of its report on the records of celebrities and there are incomplete records and little monitoring for what purposes the information was accessed. This leaves open the possibility that those with access to PIERS used it to look up their non-famous acquaintances or use it for nefarious purposes such as stalking or identity theft. Based on the information provided about PIERS privacy controls, it seems unlikely that these invasions would ever be detected.

At CDT, we were not surprised to hear that passport records were not adequately protected, because we have been raising questions about a range of privacy practices at the State Department for several years. Simply put, the State Department has failed to build a comprehensive privacy program despite the fact that the Department holds some of the most sensitive information in the federal government.

On May 2, 2007, CDT wrote a letter to Secretary of State Condoleezza Rice raising major concerns about the process for preparing Privacy Impact Assessments at the State Department.<sup>1</sup> In particular, we raised concerns that the PIAs for the E-Passport and PASS Card program were woefully inadequate, and we urged the Secretary to make more comprehensive analysis available to the public. CDT never received a reply.

Privacy Impact Assessments (PIAs) are mandated by the E-Government Act of 2002. We discuss below how the PIA, when treated seriously, is a valuable tool for identifying and addressing privacy concerns associated with government records systems. While PIAs at some other agencies, such as the Department of Homeland Security (DHS) are 25 to 35 pages long, most State Department PIAs are 1 or 2 pages long and contain only

---

<sup>1</sup> <http://www.cdt.org/security/identity/20070502rice.pdf>

limited information. In reviewing several other PIAs for systems related to PIERS mentioned in the IG report, we found that all were cursory and many were also inaccurate and incomplete. For example, the Consular Consolidated Database PIA, which allows agents Web access to PIERS and several other databases, has a one page PIA that suggests that other agencies that access it include: the Department of Defense, Department of Justice, Federal Bureau of Investigations, Office of Personnel Management and Department of Commerce, but clearly neglects to mention that the DHS has access despite the fact that several DHS components list access to the CCD as a central point in their documents.<sup>2</sup>

Congress must work to address the specific issue of the privacy of passport records. On that score, we suggest that Congress adopt legislation to provide for passport records the same protections and civil and criminal sanctions that have been applied to tax records held by the IRS in the Taxpayer Browsing Protection Act.<sup>3</sup> However, Congress must also work to strengthen privacy protections at the State Department in general through greater oversight and penalties on the agency for failures to meet mandated privacy responsibilities, starting with the timely preparation and public release of meaningful PIAs.

#### **Similar Privacy Problems across the Federal Government**

Just as Congress should not limit its concern to passport records, it should not limit the lessons from this incident to the State Department. Last month, the GAO released a government-wide report finding that agencies “may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles.”<sup>4</sup> While most agencies are not heedlessly violating existing laws as the State Department employees and contractors did in the passport browsing case, many agencies are clearly violating the spirit of the Privacy Act and the E-Government Act.

For years GAO and others have reported that the federal government has not properly implemented or enforced the Privacy Act.

For example, implementation difficulties continue to be found in the following areas:

---

<sup>2</sup> See: <http://www.state.gov/documents/organization/93772.pdf> USVISIT [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_usvisit.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit.pdf); CPB [http://www.cbp.gov/linkhandler/cgov/trade/automated/modernization/ace/quarterly\\_reports/ace\\_status\\_report\\_to\\_congress\\_march\\_2008/ace\\_2ndqtr\\_08.ctt/ace\\_2ndqtr\\_08.pdf](http://www.cbp.gov/linkhandler/cgov/trade/automated/modernization/ace/quarterly_reports/ace_status_report_to_congress_march_2008/ace_2ndqtr_08.ctt/ace_2ndqtr_08.pdf) and several other DHS agencies publicly list their access to the CCD.

<sup>3</sup> PL 105-35.

<sup>4</sup> GAO, “Alternatives Exist for Enhancing Protection of Personally Identifiable Information,” May 2008, GAO-580-36.

- Publishing all required system of records notices;<sup>5</sup>
- Consistency in determining how the “system of records” definition and the disclosure provisions apply;<sup>6</sup>
- Building reliable internal assessment measures to ensure personal data are appropriately collected and safeguarded;<sup>7</sup> and
- Establishing basic rules for federal agencies’ use of personal information obtained from data resellers.<sup>8</sup>

Data security is an important aspect of privacy and another area of broad concern. Many agencies have simply lost the personal data of millions of Americans. For example, the Chief Privacy Officer of a large agency privately reported to CDT that, when the agency did an audit of its Privacy Act systems of records, it found that half of the systems (and all the records involved) were lost. Other cabinet level agencies do not even audit the existence, location or condition of their systems. As one retiring security official from the Department of Interior recently explained, Interior has been “promiscuous with our data... we don’t know anything about our data... we don’t know where our data is.”<sup>9</sup>

### Gaps in the Privacy Act

As GAO and others have noted, the existing structure of the Privacy Act and at least two of its main definitions have become outdated as a result of technology changes.<sup>10</sup> The gaps in the law, combined with lack of enforcement accountability, have allowed agencies to drift further from compliance with the spirit as well as the letter of the

<sup>5</sup> This problem, identified as early as 1987, “Privacy Act System Notices,” November 30 1987, GAO/GGD-88-15BR <http://archive.gao.gov/d29t5/134673.pdf>, is still a major concern today as evidenced in GAO’s report released today. In 1990, a more comprehensive GAO study suggested that only 65% of systems covered by the Privacy Act had proper notice procedures. GAO, “Computers and Privacy: How the Government Obtains, Verifies, Uses and Protects Personal Data,” August 1990, GAO/IMTEC-90-70BR. Agency personnel have regularly told CDT that there are thousands of systems of records that do not have systems of records notices, suggesting that a substantial proportion of covered systems have still not been properly noticed.

<sup>6</sup> GAO “OMB Leadership Needed to Improve Agency Compliance,” June 30, 2003, GAO-03-304 <http://www.gao.gov/new.items/d03304.pdf>

<sup>7</sup> GAO, “Privacy Act: Federal Agencies’ Implementation Can Be Improved,” August 22, 1986, GGD-86-107 <http://archive.gao.gov/d4t4/130974.pdf>

<sup>8</sup> GAO “Agency and Reseller Adherence to Key Privacy Principles,” April 4, 2006, GAO-06-421 <http://www.gao.gov/new.items/d06421.pdf>.

<sup>9</sup> Comments of Ed Meagher, Deputy Chief Information Officer, Department of Interior, before the National Institute of Standards and Technology Information Security and Privacy Advisory Board, June 5, 2008.

<sup>10</sup> This issue is explored in detail in other recent testimony: Statement of Ari Schwartz before the Committee on Homeland Security and Governmental Affairs “Protecting Personal Information: Is the Federal Government Doing Enough?” June 18, 2008 <http://www.cdt.org/testimony/20080618schwartz.pdf>

Privacy Act. In order to address the larger privacy issues, Congress must address these concerns. In particular:

- **Scope of the Act**

A major concern with the Privacy Act centers on its most important term, "system of records." The definition of "system of records" excludes from the coverage of the Privacy Act information that is not regularly "retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."<sup>11</sup> Information that falls outside of the definition is not covered, no matter how it is used or misused.

The definition has been outpaced by major advancements in database technology. Today, it is rare that a system is created with a specific identifier that will be used for searching as was commonplace in the 1970s. Instead, agency personnel and contractors can search on a range of different types of criteria. For example, because it did not specifically search on an identifier, the DHS "ADVISE" datamining program was not covered by a system of records notice. (Because of scrutiny, DHS eventually suspended the system.<sup>12</sup>)

Another major flaw in the scope of the Act relates to the increased government use of private sector data. In passing the Privacy Act, Congress made it very clear that an agency could not get around the Act by having a contractor hold the data,<sup>13</sup> yet Congress clearly did not envision that data services companies in the private sector would amass enormous databases that federal government agencies could subscribe to and search without either bringing the information into a government database or falling under the provision of the Act that covers contractors. Nevertheless, data brokers that sell information to the federal government today are not held accountable to the privacy, security or data quality standards of the Privacy Act.

- **Breadth of Routine Use Exemptions**

Another major concern has been the frequent, seemingly standardless invocation of the "routine use" exemption to override the Act's limits on reuse and sharing of information between agencies. The "routine use" exemption was designed to allow agencies to share information in limited circumstances. Successive Administrations have become ever more accepting of this exemption. Routine uses are now so

---

<sup>11</sup> 5 U.S.C. § 552a(a)(5).

<sup>12</sup> Ryan Singel, "DHS Data Mining Program Suspended After Evading Privacy Review, Audit Finds," Wired Threat Level Blog, August 20, 2007 <http://blog.wired.com/27bstroke6/2007/08/dhs-data-mining.html>.

<sup>13</sup> 5 U.S.C. § 552a(m).

widely used and utterly unchecked that almost every Privacy Act Notice required by the law lists numerous routine uses, including vague boilerplate language confusing both citizens who want to understand what is happening to their data and the agency personnel responsible for it care. For example, the Department of Defense regularly lists over 20 routine uses and then includes a Web link to a set of 16 "Blanket Routine Uses" that are included with every Privacy Act Notice it publishes.<sup>14</sup> Clearly, this is not what Congress intended.

### **Shortcomings of the Privacy Impact Assessment Process**

The Privacy Act is not the only federal law affecting the privacy of personal information. Important steps toward updating government privacy policy were taken with the passage of the E-Government Act and efforts toward its effective implementation. In particular, Section 208 of the Act was designed to "ensure sufficient protections for the privacy of personal information."<sup>15</sup> To improve how the government collects, manages and uses personal information about individuals, Section 208 requires that agencies post privacy notices on their Web sites and that they conduct PIAs.

Section 208(b) of the E-Government Act requires that agencies perform PIAs before (i) developing or procuring new technology that collects, maintains, or disseminates personal information or (ii) initiating new collections of personally identifiable information. PIAs are supposed to be public documents and are supposed to contain a description of the project, a risk assessment, a discussion of potential threats to privacy, and ways to mitigate those risks. PIAs are intended to ensure that privacy concerns are considered as part of the design of information systems and that the public has access to this element of the decision making process.

Over the past five years, PIAs have become an essential tool to help protect privacy. They are sometimes called "one of the three pillars" of the US government privacy policy.<sup>16</sup> Unfortunately, as with the other privacy laws, federal agencies unevenly implement even the basic requirement of PIAs. The State Department is especially egregious in this regard, preparing PIAs that are not only cursory but also inaccurate. For example, the State Department Inspector General determined that information in the PIERS PIA "appears to contradict what OIG observed during the course of this review," specifically sharing information with DHS. In this case, it is especially worrisome because it is unclear from any public information which components of DHS are getting

<sup>14</sup> The "Blanket Routine Uses" are available at [http://www.defenselink.mil/privacy/dod\\_blanket\\_uses.html](http://www.defenselink.mil/privacy/dod_blanket_uses.html)

<sup>15</sup> PL 107-347, Section 208.

<sup>16</sup> DHS Chief Privacy Officer Hugo Teufel, *Presentation before the European Commission's Conference on Public Security, Privacy and Technology*, November 20, 2007 Brussels, Belgium. Mr. Teuffel suggested that the three current pillars are the Privacy Act of 1974, Section 208 of the E-Government Act and the Freedom of Information Act.

the passport data and what they are doing with it. Overall, the woefully inadequate nature of State Department PIAs highlights the need for better enforcement of the PIA requirement.

### **Specific Concerns with PIAs and Steps to Address Them**

The recent OMB Federal Information Security Management Act (FISMA) report to Congress highlighted the fact that agencies, as rated by their own Inspectors General, range from “excellent” to “failing” in their implementations of the PIA requirement.<sup>17</sup> This wide range of compliance is due to two major factors: (1) guidance issued by OMB with respect to PIAs is vague and has simply not provided agencies with the tools they need to successfully implement the PIA requirement, and (2) the reporting standards themselves are not uniform, as each Inspector General is basically developing its own standards for issuing these ratings.

While some agencies, like the DHS,<sup>18</sup> have set a high standard for the quality of their PIAs and have continued to improve them over time, the lack of clear guidance has led other agencies to conduct cursory PIAs or none at all. Yet DHS received only a “good” mark and the State Department received a “satisfactory” mark in the FISMA report because the ratings are based solely on the number of PIAs completed and not on their quality or accuracy.

Even more troubling is the finding that some agencies simply do not perform PIAs on as many as half of their qualifying technologies.<sup>19</sup> An official at the Department of Defense, which received a failing mark in the FISMA report, suggested to CDT that PIAs are still just not considered a priority there and are not taken seriously as an important tool for identifying and addressing privacy and security issues.

Finally, and perhaps most importantly, even those agencies that prepare in depth PIAs too often complete them after a project has been developed and approved. PIAs are supposed to inform the decision making process, not ratify it. They are supposed to be prepared early in the system design process, so they can be used to identify privacy problems before the system design is finalized. They cannot serve this crucial role if they are done after design is completed.

While OMB has begun to take steps to address the inconsistent implementation of PIAs,

---

<sup>17</sup> MB FY 2007 Report to Congress on Implementation of the Federal Information Security Management Act of 2002. [http://www.whitehouse.gov/omb/inforeg/reports/2007\\_fisma\\_report.pdf](http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf).

<sup>18</sup> The DHS Website on Privacy Impact Assessment offers a range of resources to DHS components and to other agencies. [http://www.dhs.gov/xinfo/share/publications/cditorial\\_0511.shtm](http://www.dhs.gov/xinfo/share/publications/cditorial_0511.shtm).

<sup>19</sup> OMB FY2006 Report to Congress on Implementation of the Federal Information Security Management Act of 2002, at [www.whitehouse.gov/omb/inforeg/reports/2006\\_fisma\\_report.pdf](http://www.whitehouse.gov/omb/inforeg/reports/2006_fisma_report.pdf).

it should be of great concern to this Committee that some agencies are still not conducting PIAs in a timely and comprehensive manner. The work of those agencies that have taken seriously the mandate to develop PIAs and used them as a tool for analysis and change should be a starting point for developing best practices for all federal agencies. The E-Government Act Reauthorization Act (S.2321) currently in front of the Senate includes a provision that would help address these concerns by specifically requiring OMB to create best practices for PIAs across the government. CDT supports this provision.

### **Private Sector Data**

Another concern with Section 208, similar to concern about the coverage of the Privacy Act, is the failure to specifically require PIAs for government access to private sector data. OMB guidelines allow agencies to exempt the government's use of private sector databases from the requirement to conduct PIAs when the commercial data is not "systematically incorporated" into existing databases. CDT believes that this permissive approach is wrong. Companies that provide private sector data to the government have a range of security and privacy practices. Government agencies should use the PIA process to take those issues into account when making decisions about the use of commercial data. Notably, some agencies are already requiring PIAs for uses of commercial data even when the data is not integrated into existing databases despite OMB's guidance.

GAO's report published today points out that, in 2006, it recommended that OMB revise its guidance to clarify the applicability of requirements for PIAs with respect to agency use of data obtained from commercial re-sellers. The GAO further notes that OMB did not address that recommendation<sup>20</sup> and openly disagreed with it in House Oversight and Government Affairs Committee testimony.<sup>21</sup> Simply put, OMB has ignored the serious concerns raised by the ease with which an agency can avoid the PIA requirement simply by subscribing to an information service rather than creating a database of the same information within the agency.

The Chairman and Ranking Member's bill, S.495, would require PIAs for government access to private sector data, a highly necessary step in protecting the information of citizens as government agencies contract with private data brokers.

### **Lack of Privacy Leadership**

---

<sup>20</sup> GAO-03-304.

<sup>21</sup> Karen Evans before the House Committee on Oversight and Government Affairs Subcommittee on Information Policy, Census, and National Archives on "Privacy: The Use of Commercial Information Resellers by Federal Agencies," March 11, 2008.  
<http://informationpolicy.oversight.house.gov/documents/20080318172705.pdf>.

Much of the blame for privacy failures at the State Department and other agencies clearly falls on the leadership of those agencies for not giving adequate attention to information privacy and security; their failure stands out because others have done better. But blame also falls on OMB because it is responsible for interpreting and overseeing the implementation of the Privacy Act and Section 208 of the E-Government Act. In June 2003, GAO issued a report entitled "Privacy Act: OMB Leadership Needed to Improve Agency Compliance." In that report, the GAO identified deficiencies in compliance and concluded: "If these implementation issues and the overall uneven compliance are not addressed, the government will not be able to provide the public with sufficient assurance that all legislated individual privacy rights are adequately protected."<sup>22</sup> Such criticism of OMB for failing to provide adequate oversight and guidance to agencies is not new. Going back as far as 1983, the House Committee on Government Operations raised concerns that OMB had not updated its guidance in the first nine years of the Act's passage.<sup>23</sup> Other agencies have also failed to fulfill their government-wide responsibilities. The Department of Justice, which had published an official case law guide to the Act every two years since the late 1980s, has not done so for the past four years.<sup>24</sup>

OMB is now just beginning to provide the kind of leadership that is needed to help agencies build programs to protect privacy, as evidenced by the changes in its FISMA report to Congress to require some kind of yearly reporting by agencies and the creation of a privacy working group within the CIO Council, led by E-Government Administrator Karen Evans. While these are important steps in the right direction, they are not long-term leadership solutions. The next Administration should be encouraged, on a bipartisan basis, to make major improvements in Privacy Act implementation and oversight.

### Recommendations

Recent revelations about problems in the State Department's handling of passport files highlight longstanding and government-wide weaknesses in protecting the privacy and security of personal information in the hands of the government. We urge the Congress and the Executive Branch to begin this year to implement a series of long overdue reforms:

**1) Update Privacy Protections for Passport Records** — As mentioned earlier, using the Taxpayer Browser Protection Act as a model, Congress should strengthen protections

---

<sup>22</sup> GAO-03-304.

<sup>23</sup> House Report No. 98-455.

<sup>24</sup> Ken Mortenson, Acting Chief Privacy and Civil Liberties Officer at DOJ suggested that the delay in publishing the Privacy Act Overview was due to internal changes at the Department and a new version would be released this summer.

for passport records and penalties for misuse. This includes increased oversight and specific penalties for the agency for failure to set and meet specific privacy goals.

**2) Increase Oversight of Privacy at the State Department** — Passport browsing is not the only privacy problem at the State Department. The Department should be held accountable through its information technology budget for failing to protect the privacy of all individuals.

**3) Review Privacy Act Coverage and Close Loopholes** — CDT agrees with GAO's basic assertion that Privacy Act definitions are out of date. We believe that these issues must be addressed in legislation.

**4) Improve Privacy Impact Assessments Across the Government** — CDT supports the creation of best practices for PIAs. CDT also urges the Committee to require PIAs for any program that uses commercial data, whether the personal information used will be stored at the agency or kept by the commercial entity. CDT supports requiring PIAs government-wide for rulemakings as well as information collections. This is currently the law only for DHS. CDT also supports requiring PIAs for systems of government employee information. Finally, we stress the importance of ensuring that PIAs are begun early in the development of a system or program and that they are completed before the project or procurement begins, so that the findings of the PIA can shape rather than merely ratify the activity's impact on privacy.

**5) Creating a Chief Privacy Officer Position at OMB Who Will Run a Separate CPO Council** — To ensure that agencies have greater consistency on privacy and leadership is taken, CDT would like to see a permanent Chief Privacy Officer (CPO) position at OMB written into law. At the agency level, the new legislative requirements for appointment of CPOs have clearly been a success. Yet many large agencies that have a lot of personal information still do not have statutory CPO, including cabinet agencies such as the Department of Veterans Affairs, the Department of the Interior and the Department of Housing and Urban Development. Based on this experience, we believe that all large agencies (the so called "CFO agencies" based on the threshold from the CFO Act) should be required to have a CPO. These privacy officials should be placed outside of the structure of the CIO office where resources and attention are almost always rightly focused on systems procurement and maintenance instead of information policy. In addition, department heads should ensure that CPOs are engaged in the early stages of developing policies and planning systems or programs that will have a privacy impact. CDT also urges the creation of a CPO Council with a similar structure to the CIO and CFO Councils.

**6) Increase and Improve Privacy Reporting and Audits** — OMB requirements for privacy reporting in FISMA are a major leap forward in focusing attention on privacy issues, but getting the right implementation and accountability processes in place is an essential goal. Most importantly, OMB should be required to create standardized measurements for privacy protecting processes (such as, quality of both the PIA process and the PIAs themselves) and make them public. CDT also believes that agencies should

be required to ensure that the systems of greatest privacy risk (both in size and in program activity) undergo regular audits by IGs and/or, when IGs are overwhelmed or not experts in privacy, by outside third party audit firms.

### **Conclusion**

The violations of the employees who have been browsing passport records are certainly egregious and Congress must address this specific practice. Yet, the State Department and Congress would be treating the symptom of a larger problem if it only took this opportunity to address the problems around this one sensitive database. The failure to protect information in the federal government is far more widespread. The State Department has clearly been a failing agency across the board in this regard and there are several other failing agencies as well. To prevent another serious breach of public trust in this way, Congress will need to address the roots of the problem by updating privacy laws, oversight and leadership.

