Testimony of

Alan Raul

July 10, 2008

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. 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.