Statement of

Gregory T. Nojeim
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology

On

"Restoring the Rule of Law"

Hearings Before the Senate Judiciary Committee, Subcommittee on the Constitution

September 16, 2008[*]

Chairman Feingold, Ranking member Brownback, Members of Subcommittee:

Thank you for the opportunity to submit this written statement for the record on behalf of the Center for Democracy & Technology in these important hearings on Restoring the Rule of Law. CDT is a non-partisan, non-profit organization devoted to keeping the Internet open, innovative and free. We advocate for democratic values in the digital age. Since the horrible attacks of September 11, those values have been severely tested, and in some cases, compromised in the search for security. We compliment Chairman Feingold and the entire Subcommittee for conducting this hearing now so that recommendations to the new President and Congress about measures to restore the rule of law can be assembled and analyzed this year and be acted on early next year.

Privacy, one of our most fundamental rights, recently has been dramatically eroded as a result not only of policy failures stemming from the response to September 11, but also because our privacy laws and policies have not kept pace with advances in technology. Increasingly, Americans use the Internet and other digital services to access, transfer and store vast amounts of private data. Financial statements, medical records, travel itineraries, and photos of our families – once kept on paper and secure in a home or office – are now stored on networks. Electronic mail, online reading habits, business transactions, Web surfing and cell phone location data can reveal our activities, preferences and associations. Information generated by digital services is accessible to the government under weak standards based on outdated Supreme Court decisions and laws. Indeed, the major federal law on electronic communications was written in 1986, before the World Wide Web even existed.

In the wake of the 9/11 attacks, laws and policies have been adopted that unnecessarily weaken privacy rights and other constitutional liberties. The government has adopted data mining techniques, expanded electronic surveillance, and launched new identification programs without adequate safeguards for the rights of Americans. These

[*] This statement for the record was submitted on October 1, 2008.

and other programs have often been adopted before careful assessment of whether they are even likely to be effective. But bad policy choices are only half of the story.

Any effort to restore the rule of law must account both for poor policy choices and for advances in technology that require new policies. In other words, reversing course on policies chosen in order to restore the rule of law insufficient because the old course is outdated. Return to prior status quo is not an option. Instead, more must be done to impose checks and balances. Such checks and balances not only preserve liberty, but also help enhance security by ensuring that the government is focusing its limited resources on real threats and effective measures.

In short, the next President and Congress should --

- **Update electronic communications laws to account for the way that Americans communicate today;**
- **Restore checks and balances on government surveillance, including vigorous judicial and congressional oversight of surveillance programs;**
- **Review information sharing policies and practices to ensure that the government can "connect the dots" while preserving privacy; and**
- **Revisit the REAL ID Act and ensure that governmental identification programs include proper privacy and security protections.**

Updating Electronic Communications Privacy Laws

The Electronic Communications Privacy Act (ECPA) sets the standards for government surveillance of email and other communications in criminal cases. Adopted in 1986, ECPA has been outpaced by technology developments. For example, though cell phones can be used to track a person's location, ECPA does not specify a standard for law enforcement access to location information. In this instance, the rule of law cannot merely be "restored" because the law specifies no rule. It should.

E-mail, personal calendars, photos, and address books, which used to reside on personal computers under strong legal protections, now are stored on communications networks where privacy rules are weak or unclear. Instead of the law being technology neutral to put technologies that operate "in the cloud" on the same privacy footing as technologies that operate on a desktop computer, the law discriminates against Web-based technologies in terms of the privacy afforded to users.[1] A patchwork of confusing standards and conflicting judicial decisions has arisen, and it has confounded service providers and created uncertainty for law enforcement officials.

ECPA should be updated to tighten and clarify the standards for government access to data that is that is communicated and stored. Updating ECPA will require the next President to work with Congress, industry, and NGOs to strengthen protections against

[1] See http://blog.cdt.org/2008/09/29/liberty-technology-and-the-next-president/.

unwarranted government access to personal information.[2] CDT has been working for over six months with industry and NGO stakeholders to develop policy recommendations that could become a blueprint for updating ECPA. We look forward to providing those policy recommendations to the new President and Congress in the coming months.

Ensuring that Intelligence Collection Complies with FISA and Is Subject To Judicial Oversight

While ECPA governs electronic surveillance for criminal purposes, surveillance to gather sound and timely intelligence is also needed to head off terrorist attacks and otherwise to protect the national security. Recent history shows that intelligence gathering powers can be abused. For example, the Administration for over five years after September 11, 2001 conducted an unlawful, unconstitutional warrantless surveillance program aimed at the international communications of individuals who were themselves al Qaeda members, or who were suspected of being in communication with such persons. Strong statutory standards, judicial checks and balances, and congressional oversight are critical to protect the rights of Americans and ensure that the intelligence agencies are acting effectively and within the law. Both Congress and the President can play crucial, complimentary roles in restoring checks and balanced on intelligence surveillance.

The President should announce that it is the policy of his administration to refrain from engaging in warrantless surveillance in the United States, to comply with the Foreign Intelligence Surveillance Act, and to cooperate fully with any investigation of post 9-11 warrantless surveillance. But compliance with FISA is not enough because the law itself has been changed in ways that erode the checks and balances originally built into it.[3] An Inspector General's report on implementation of the 2008 FISA Amendments Act, due out next summer, should be reviewed carefully with an eye toward making the changes in the law that are to address any abuses or misuses of FISA authorities that it identifies.

Congressional leaders should also commence a joint congressional investigation of domestic intelligence activities that is designed to uncover illegal or inappropriate surveillance and prevent it from recurring. Necessary legislation resulting from this review should be attached to the legislation Congress considers in connection with the expiration of key provisions of the USA PATRIOT Act on December 31, 2009.[4] Such legislation should, at a minimum, include the checks and balances on issuance of national security letters and orders under Section 215 of the USA PATRIOT Act.

---

[2] More information about what needs to be done can be found in this CDT Report on "Digital Search and Seizure" http://www.cdt.org/publications/digital-search-and-seizure.pdf and in this CDT Policy Post on how digital technology requires stronger privacy laws: http://www.cdt.org/publications/policyposts/2006/4.

[3] See CDT's testimony on changes to FISA proposed earlier this year, many of which were enacted in the FISA Amendments Act: http://www.cdt.org/security/20070925dempsey-testimony.pdf and http://www.cdt.org/security/20070918dempsey-testimony.pdf.

[4] On December 31, 2009, both Section 215 of the PATRIOT Act (the "library records provision") and the PATRIOT Act provision authorizing roving intelligence wiretaps, will expire unless renewed by Congress. In addition, a related provision of FISA permitting electronic surveillance for intelligence purposes of non-U.S. Persons who are not associated with foreign powers (the "lone wolf" provision) will also expire.

A National Security Letter is a demand by the FBI or by other elements of the intelligence community, issued without prior judicial approval, for sensitive bank, credit and communications records from financial institutions, credit reporting agencies, telephone companies, Internet Service Providers, and others. These records are important to national security investigations, but the PATRIOT Act dramatically expanded the scope of these demands while reducing the standards for their issuance. The Inspector General of the Department of Justice found widespread errors and violations in the FBI's use of NSLs.[5] A Section 215 order is an order issued by a judge requiring any person to turn over records or objects when the judge finds that the material sought is relevant to an authorized intelligence investigation. To protect Americans' privacy and focus investigative resources more effectively, the next President should curtail the use of NSLs and should propose, and the next Congress should enact, legislation such as S. 2088, the NSL Reform Act, introduced in the 110th Congress. It would require a court order for access to sensitive personal records.[6] The President should also cooperate with congressional and Inspectors General oversight of intelligence surveillance and the next Congress should conduct vigorous, non-partisan oversight of the full range of intelligence surveillance programs affecting the rights of Americans.

Connecting the Dots Without Short Circuiting Privacy Protections

Reforming the way intelligence is collected is only one part of the equation. In addition, the sharing of intelligence information is in need of an overhaul as well. Government watch lists, fusion centers, databases, and data mining programs[7] are growing at an alarming pace without adequate safeguards. Connecting the dots is crucial to preventing the next attack, but inaccurate information and flawed analytic techniques can result in a person being wrongfully treated as a terrorist, with devastating consequences such as arrest, deportation, job loss, discrimination, damage to reputation, and more intrusive investigation.

The next President and Congress should adopt a balanced framework for information sharing and analysis for counterterrorism purposes. The next President should review all information sharing and analysis programs for effectiveness. The next President and Congress should bring all information sharing and analysis programs under a framework of privacy protection, due process and accountability. A Markle Foundation Task Force has issued a report[8] on implementing a trusted information sharing environment that should be a valuable resource for the next President as he seeks to implement information sharing while protecting civil liberties.

---

[5] DOJ Inspector General Report on NSL abuses: http://www.usdoj.gov/oig/special/s0703b/final.pdf.

[6] See CDT's testimony on national security letters, http://judiciary.senate.gov/hearings/testimony.cfm?id=3255&wit_id=7127 and our policy post on NSLs: http://cdt.org/publications/policyposts/2007/5

[7] See CDT's testimony on government data mining programs http://www.cdt.org/testimony/20070109harris.pdf and CDT's memorandum on government mining of commercial data: http://www.cdt.org/security/usapatriot/030528cdt.pdf.

[8] http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php#report1

Information sharing for counter terrorism purposes often results in the government using information collected for one purpose for an entirely different purpose – thus implicating the Privacy Act, which was adopted to control such practices. Designed for the mainframe world of 1974, the Privacy Act needs to be updated to reflect the distributed nature of government information systems and the ease with which data maintained by the government or obtained from the commercial sector can be shared and mined. The next Congress should adopt legislation to update and strengthen the Privacy Act, including by adopting standards for government use of commercial data.[9]

The E-Government Act of 2002 provides additional protections. It requires agencies of the federal government to issue privacy impact assessments (PIAs) before they launch a new system or program that collects or processes personal information in identifiable form. These PIAs can act as an effective check on the abuse of personal information maintained by the government, and can spur agencies to consider means of carrying out necessary programs while limiting the privacy risks associated with them. However, the quality of PIAs issued varies widely from agency to agency,[10] and sometimes within the same agency. The President should appoint a senior White House official as Chief Privacy Officer to issue a guide to best practices for the PIAs required by the E-Government Act of 2002 and to ensure that agencies increase the quality of their PIAs. The Chief Privacy Officer would also advocate for privacy within the Executive Branch and chair a Chief Privacy Officer Council consisting of the Chief Privacy Officers of each agency united in a structure similar to that of the Chief Information Officer Council.

Making Identification Programs Effective and Safe

In recent years, the federal government has launched a variety of ID card programs, including, most notably, REAL ID. Some of these programs would incorporate biometric and Radio Frequency Identification (RFID) technology without safeguarding the privacy and security of information on the cards or limiting how they can be used by government or commercial entities to track the movements of ordinary Americans. Poorly designed programs could actually contribute to ID theft. The REAL ID program is already showing signs of "mission creep."

The next President and Congress should revisit the REAL ID Act and ensure that all governmental identification programs are necessary and effective and subject to adequate privacy and security protections. In particular, the REAL ID program should be given a top to bottom review to determine whether it will be effective and whether the costs of the program to the federal government and to state governments – in terms of dollars and risks to security and privacy – outweigh the benefits. If such review justifies continuation of the program, the next President should direct the Secretary of Homeland Security to recommend improvements in the REAL ID Act and to withdraw the

---

[9] For information about the new policies and laws that should be adopted to protect personally identifiable information in government data bases, see CDT's June 2008 testimony: http://cdt.org/testimony/20080618schwartz.pdf.

[10] For example, the State Department's PIAs have been woefully inadequate and the PIAs issued by the Department of Homeland Security have generally been of high quality. See CDT's testimony on the privacy of passport files, p. 4. http://www.cdt.org/testimony/20080710schwartz.pdf.

regulations that have been issued under it or make substantial improvements in the existing regulations to enhance privacy protections.[11]

Congress should conduct its own review of the REAL ID Act and make improvements where necessary. It should also amend the Driver's Privacy Protection Act to further protect privacy against both governmental and commercial abuse.

Conclusion

Thank you for the opportunity to outline some of the policies and legislation that should be adopted by the next President and the new Congress to restore the rule of law. We look forward to working in the coming years with the Subcommittee, and with the new Administration, to implement as many of these proposals as possible.

[11] CDT's analysis of REAL ID and of the REAL ID regulations can be found here: http://www.cdt.org/testimony/20070321dhstestimony.pdf, and its testimony on implementation of REAL ID and the Western Hemisphere Travel Initiative can be found here: http://www.cdt.org/testimony/20080429scope-written.pdf.