

## **LIBERTY AND SECURITY: RECOMMENDATIONS FOR THE NEXT ADMINISTRATION AND CONGRESS**

A coalition of more than twenty organizations and over seventy-five individuals collaborated to create “Liberty and Security: Recommendations for the Next Administration and Congress.” The Constitution Project coordinated the production of the report, which was released in November 2008.

“Liberty and Security” indexes policy proposals across 20 different issue areas, including privacy, secrecy and surveillance; detention, interrogation, and trials of so-called “enemy combatants”; and discrimination in immigration and charities policy. It includes recommendations for congressional and executive action, and provides in-depth background information to support action by policy makers. It also includes lists of issue-based resources and experts in the community. The report includes the following chapters:

### ***Charities, Foundations, and National Security***

**CHAPTER 1:** Eliminate Unnecessary Barriers to Legitimate Charitable Work

### ***Detention, Interrogation, and Trials of Suspected Terrorists***

**CHAPTER 2:** Closing Guantánamo

**CHAPTER 3:** End Illegal Detention, Torture, and Rendition

**CHAPTER 4:** Prosecute Terrorist Suspects in Accordance with the Law

### ***Immigration and National Security***

**CHAPTER 5:** Failing to Protect Refugees and Asylum Seekers: Overly Broad Definition of Material support for Terrorism.

**CHAPTER 6:** Ending Immigration Enforcement Based on National Origin, Ethnicity, and Religion

**CHAPTER 7:** Misuse of Immigration Detention Laws in Counterterrorism Efforts

### ***Secrecy, Surveillance, and Privacy***

**CHAPTER 8:** Revising Attorney General Guidelines on FBI Investigations

**CHAPTER 9:** Updating the Law Governing the Privacy of Electronic Communications

**CHAPTER 10:** Fusion Centers and the Expansion of Domestic Intelligence

**CHAPTER 11:** Promoting Government Transparency

**CHAPTER 12:** National Security Letters and Section 215 of the USA PATRIOT Act

**CHAPTER 13:** Reform of the National Security Surveillance Laws and Procedures

**CHAPTER 14:** Preventing Over-Classification and Retroactive Classification and Promoting Declassification of Government Documents

**CHAPTER 15:** Reforming the State Secrets Privilege

**CHAPTER 16:** Reforming Watch Lists

### ***Separation of Powers and Executive Authority***

**CHAPTER 17:** Assertion of Executive Authority in National Security Matters

**CHAPTER 18:** Executive Privilege and Congressional Oversight

**CHAPTER 19:** Signing Statements

**CHAPTER 20:** War Powers Authority

The full report is available online at <http://2009transition.org/liberty-security/>, at [www.constitutionproject.org](http://www.constitutionproject.org), and on the websites of many members of the coalition.

For policy questions, please contact the individuals or organizations identified in the catalogue as allies. Please direct general questions to Daniel Schuman, Director of Communications and Counsel, the Constitution Project, at 202-580-6922.

## APPENDIX

### Chapter 9: Updating the Law Governing the Privacy of Electronic Communications

#### I. Jurisdiction

- A. **Congress:** Congress has the authority to enact legislation necessary to update ECPA. The Judiciary committees in both the House and Senate have authority over any such legislation.
- B. **Executive Branch:** The Department of Justice, and within DOJ, the FBI, are the executive branch agencies that would be most effected by changes in ECPA.

#### II. Status of Actions in Legislative, Executive and Judicial Branches

##### A. Legislative:

1. The Electronic Communications Privacy Act was signed into law on Oct. 21, 1986 as Title III of the Omnibus Crime Control and Safe Streets Act (P.L. 99-508). ECPA has been amended several times. Most recently, ECPA was amended, and its privacy protections weakened, by the USA PATRIOT Act (P.L. 107-56), enacted on Oct. 26, 2001. It was again amended by the USA PATRIOT Act Improvement and Reauthorization Act of 2005 (P.L. 109-177), which was enacted on March 9, 2006. Finally, it was again amended by the FISA Amendments Act of 2008 (P.L. 110-261), which was enacted on July 10, 2008.
2. A number of bills have been introduced to update ECPA to set or to adjust standards for location information, stored email, and pen registers and trap and trace devices. The leading bills, both from the 106<sup>th</sup> Congress, were:
  - a. Electronic Communications Privacy Act of 2000 (H.R. 5018, 106th Congress) – Introduced by Rep. Charles Canady (R-FL); Referred to House Committee on the Judiciary where it passed 20-1 on Oct. 4, 2000; no action on House floor
  - b. Electronic Rights for the 21st Century Act (S. 854, 106th Congress) – Introduced by Sen. Patrick Leahy (D-VT); Referred to Senate Committee on the Judiciary; no action
3. In addition, the E-mail Privacy Act of 2005 (S. 936, 109th Congress) was introduced in response to the *U.S. v. Councilman* litigation to clarify the definition of "intercept" to mean the aural or other acquisition of the contents of any wire, electronic, or oral communication contemporaneous with transit, or on an ongoing basis during transit, through the use of any electronic, mechanical, or other device or process, notwithstanding that the communication may simultaneously be in electronic storage (thus covering e-

mail communications) – Introduced by Sens. Patrick Leahy (D-VT) and John Sununu (R-NH); Referred to Senate Committee on the Judiciary; no action.

## B. Executive

The Department of Justice published a 2002 manual on seizing computers and obtaining electronic evidence of crime:

<http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm>

DOJ is reportedly preparing an update of the manual.

## C. Judicial

### 1. Key location information cases:

- a. Magistrate Judge Smith's decision, *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747 (S.D. Tex., 2005) (supporting use of probable cause standard)
- b. Judge Lenihan's decision, *In re the Application of the United States of America for an Order Directing a Provider of Electronic Commc'n Serv. to Disclose Records to the Gov't*, 534 F. Supp. 2d 585 (W.D. Pa., 2008) (most recent published federal case supporting MJ Smith's decision and use of probable cause standard)

### 2. Key stored e-mail cases:

- a. *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004) (holding that e-mail messages are in storage for purposes of the Stored Communications Act even if they have already been delivered to the account holder)
- b. *Warshak v. U.S.*, 490 F.3d 455 (6th Cir. 2006) (upholding district court's decision that reasonable expectation of privacy triggered probable cause requirement; later vacated on ripeness grounds, 532 F.3d 521 (6th Cir. 2008))

*See also Electronic Frontier Foundation amicus brief in Warshak v. U.S.* (Nov. 22, 2006)