CHAPTER NINE
Updating the Law Governing the Privacy of Electronic Communications

I. The Problem

The Electronic Communications Privacy Act (ECPA) of 1986 established workable standards for government surveillance of email and stored communications in criminal cases. However, ECPA has been outpaced by technological developments and privacy safeguards have not yet been established for information related to new electronic services. For example, cell phone service providers now routinely store information about the location of their customers while their cell phones are turned on, but ECPA does not specify a standard for law enforcement access to location information. Moreover, the emergence of "cloud computing," which enables storage on remote computers of business records and information such as personal calendars, photos, and address books, raises new privacy issues that require clear standards for custodians of this information who receive government requests for access to it. Currently, this information is on a weaker privacy footing than the same information when it resides in the user's computer. A patchwork of confusing standards and conflicting judicial decisions has arisen, and it has confounded service providers and created uncertainty for law enforcement officials.

Strong statutory standards, coupled with increased clarity, would be good for business, good for privacy, and good for law enforcement.

II. Proposed Solutions

A. Guiding Principles

Fourth Amendment standards, including probable cause, should govern law enforcement access to communications contents and to location information, which many consumers regard as the most sensitive non-content information available to the government. Surveillance statutes should be updated to account for the ways Americans communicate today. The level of the privacy afforded to communications should be made technology neutral so that information stored in a remote computer enjoys the same level of Fourth Amendment protection it would enjoy if stored on the user's desktop computer.

B. Proposed Measures

ECPA should be updated to tighten and clarify the standards for government access to data that is that is communicated and stored and to take account of new communications technologies:

1. Comprehensive Fourth Amendment standards, including probable cause, should be required for law enforcement access to:

a. Location information, regardless of whether it is stored or is collected in real time;
b. Email stored with a communications service provider for more than 180 days – the same standard that is imposed for email stored for shorter periods of time – and all email regardless of whether it has been opened by the recipient;
c. User-generated content, regardless of whether it is maintained on a desktop or on the Web; and
d. Information maintained on a social networking page that is not open to the public.

2. The standard for issuing a pen register or trap and trace order, which can be used by law enforcement to access in real time, for example, a log of who a person telephones and who telephones the person, should be tightened to require at least specific and articulable facts that the information sought is relevant to a pending, full, investigation. The statute should also be clarified to ensure that under no circumstances is communications content to be collected based on such an order.
3. Consistent with current Department of Justice policy and the First Circuit's *en banc* decision in *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005), ECPA should be further clarified to ensure that any real-time or prospective collection of communications content is an "intercept" requiring an intercept order, regardless of whether that content is acquired while it is in temporary electronic storage incident to transmission.
4. The statutory exclusionary rule, which now applies to the contents of illegally intercepted telephone calls, should be extended to cover the contents of illegally intercepted email and other electronic communications.

III. Allies*

American Association of Law Libraries
Mary Alice Baish, Acting Washington Affairs Representative
baish@law.georgetown.edu
202-662-9200

American Library Association
Lynne E. Bradley, Director
lbradley@alawash.org
202-682-8410
The ALA Policy Manual: The Rights of Library Users and the USA Patriot Act (52.4.5) *available at*
http://www.ala.org/ala/aboutala/governance/policymanual/policymanual.31_3.pdf

Association of Research Libraries
Prudence Adler

prue@arl.org
202-296-2296 (ext. 104)

Bill of Rights Defense Committee (BORDC)
Chip Pitts, President
chip.pitts@att.net

Center for Democracy & Technology
Gregory T. Nojeim
gnojeim@cdt.org
202-637-9800 (ext 113)
The Internet in Transition, *available at* http://www.cdt.org/election2008/

Common Cause
Sarah Dufendach, Vice President for Legislative Affairs
www.commoncause.org
202-736-5709

Defending Dissent Foundation
Sue Udry, Director
Sue.udry@defendingdissent.org
202-549-4225
www.defendingdissent.org

Electronic Frontier Foundation (EFF)
Kevin S. Bankston
bankston@eff.org
415-436-9333 (ext.126)
A Privacy Agenda for the New Administration, *available at* http://www.eff.org/deeplinks/2008/11/privacy-agenda

Essential Information
John Richard or Robert Weissman
202-387-8034

Government Accountability Project
Jesselyn Radack, Homeland Security Director
JesselynR@whistleblower.org
202-408-0034 (ext. 107)

Liberty Coalition
Michael D. Ostrolenk, Co-Founder/National Director
www.libertycoalition.net
mostrolenk@libertycoalition.net
301-717-0599

Muslim Advocates
Farhana Khera
farhana@muslimadvocates.org
415-692-1485

OpenTheGovernment.org
Patrice McDermott
pmcdermott@openthegovernment.org
202-332-6736

Stanford Law School - Mills International Human Rights Clinic
Barbara J. Olshansky, Leah Kaplan Visiting Professor and Clinic Director
Kathleen Kelly, Clinical Teaching Fellow
bj.olshansky@gmail.com
650-736-2312

U.S. Bill of Rights Foundation
Dane vonBreichenruchardt, President
usbor@aol.com
202-546-7079

* These groups and individuals support the general principles expressed and the general policy thrust and judgments in the policy proposals described above. The allies listed do not necessarily endorse the specific language in every proposed solution, but they do agree that the proposals reflect the general principles that should govern policy in this area. Please contact the individuals and organizations listed in this section for more information.

IV. Counter-Arguments and Rebuttal

Agencies of the federal government engaged in electronic surveillance, such as the FBI/Department of Justice, and some state law enforcement agencies, will be hesitant to support measures to require more judicial oversight of their surveillance activities. However, DOJ representatives have often argued for the need to update surveillance laws to keep pace with technology. Law enforcement will benefit from the increased clarity in surveillance standards that an update to the law would provide. It would help agents better understand the facts that would need to be shown in order to secure a surveillance order, and it would facilitate cooperation with those orders from providers of communications services.

In addition, the Department of Justice has argued that the Fourth Amendment does not cover business records, and it even argues that communications content maintained by a service provider, has no Fourth Amendment protection. This is all the more reason for Congress to step in and clarify the level of protection that will be afforded these communications.

V. Recommended Documents for Further Reading:

a. Center for Democracy & Technology Report on Digital Search and Seizure: http://www.cdt.org/publications/digital-search-and-seizure.pdf

b. Electronic Frontier Foundation on cell phone tracking: http://www.eff.org/issues/cell-tracking

c. Electronic Frontier Foundation on pen registers and trap and trace devices: http://www.eff.org/issues/pen-trap

d. Electronic Privacy Information Center wiretapping page: http://epic.org/privacy/wiretap/

e. *Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act, Hearing before the House Committee on the Judiciary's Subcommittee on the Constitution*, Sept. 6, 2000. http://commdocs.house.gov/committees/judiciary/hju67343.000/hju67343_0.HTM

f. Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too* (2008)

g. Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail* (Notre Dame Law School, Legal Studies Research Paper No. 08-19; 5/9/08 Draft – do not cite or quote without permission)

h. Deirdre K. Mulligan, *Reasonable Expectations In Electronic Communications: A Critical Perspective On The Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004)

i. The Electronic Communications Privacy Act (ECPA)
   i. 18 U.S.C. §§ 2510-2522 – Wire and Electronic Communications Interceptions and Interception of Oral Communications
   ii. 18 U.S.C. §§ 2701-2712 – Stored Wire and Electronic Communications and Transactional Records Access
   iii. 18 U.S.C. §§ 3121-3127 – Pen Registers and Trap and Trace Devices

APPENDIX
LEGISLATIVE, EXECUTIVE, AND JUDICIAL ACTION
on
THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

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 106th 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)