Center for Democracy & Technology Transition Memo
Theme: Balancing Security and Liberty
Issue: Updating the Law Protecting the Privacy of Electronic Communications

✶**Issue/Problem.** The Electronic Communications Privacy Act (ECPA) of 1986 established standards for government access to email and stored communications in criminal investigations. However, ECPA has been outpaced by technological developments and does not set adequate privacy standards for many new electronic services. For example, cell phones can serve as tracking devices, but ECPA does not specify a standard for government access to location information. The emergence of "cloud computing," which enables storage on remote computers of business records and personal information such as calendars, photos, and medical records, represents a major trend in the way individuals use information technology, but ECPA provides weaker protection to information stored in the cloud than it does to the same information stored on a user's computer.

A patchwork of confusing standards and conflicting judicial decisions has arisen, confounding service providers and creating uncertainty for law enforcement officials. Strong, clear statutory standards would be better for business and better for privacy, while still giving government investigators access to all the information they need, subject to appropriate checks and balances.

✶**Policy History.** While the Department of Justice has secured multiple amendments to ECPA to enhance law enforcement access, there have been no improvements to ECPA's privacy standards since 1994, and key provisions in the Act have not been revisited since 1986, ages ago in Internet time.

For example, the PATRIOT Act (P.L. 107-56, Oct. 26, 2001) amended ECPA to apply to Internet surveillance the same relaxed standard that had applied to numbers dialed on a telephone. In the rush to enact the PATRIOT Act, Congress did not stop to consider that the standard for intercepting telephone dialing information was already too weak. Nor did it consider how much more revealing all of a person's usage of digital technologies is today compared to 1986 when the standard was enacted. It approved the DOJ proposal. As a result, government officials can now obtain a judicial order authorizing real time access to a very comprehensive picture of a person's online activity merely by certifying to a judge that the information is relevant to an investigation. The government does not have to offer any facts in support of its application, and ECPA says that the judge "shall" approve the request. The order can have effect nationwide, allowing the government to serve it on multiple service providers.

Over the years, some attempts have been made to strengthen ECPA. Congress in the 1994 Communications Assistance to Law Enforcement Act specified that pen registers and trap and trace devices cannot be used to access cell phone location information,[1] but it did not specify the standard that does apply. This has led to conflicting judicial decisions about the

[1] 47 U.S.C. § 1002(a)(2).

proper standard, with the majority of written decisions requiring probable cause for government access to location information.[2]

In 1998, Senators Ashcroft and Leahy introduced S. 2067 (105th Congress), a forward-looking bill that would have established probable cause protection for location information and information stored on networks. In 2000, the Clinton Administration supported some privacy enhancements to ECPA and bills were introduced in both the House and the Senate that went further than the Clinton proposals. The bills would have, among other things, established probable cause as the standard for government access to location information. The Senate bill, the Electronic Rights for the 21st Century Act (S. 854), did not go to Committee mark up, but the House bill, the Electronic Privacy Communications Act of 2000 (H.R. 5018) was reported by the Republican-controlled House Judiciary Committee on a vote of 20-1, but the full House did not vote on the bill. 9/11 derailed further efforts to properly balance privacy and law enforcement interests.

In the absence of Congressional action, the confusing and outdated rules governing law enforcement access to stored email have generated significant litigation. ECPA provides only weak protection to email more than 180 days old, and the Department of Justice has argued that ECPA does not afford strong protections to any "opened" email regardless of its age or sensitivity. No court has agreed with this position, and one has squarely rejected it,[3] but the uncertainty remains and service providers, not wanting to incur the expense of challenging the government, are likely complying with requests and orders issued under a variety of standards.

The uncertainty leaves email – a nearly indispensable communications tool for businesses and individuals -- in legal limbo. In *Warshak v. U.S.*[4] a 6th Circuit panel held that email, contrary to the government's position, is protected by the Fourth Amendment, and that law enforcement can gain access to it only with a warrant based on probable cause or a subpoena with notice to the target and an opportunity to object. The 6th Circuit later vacated the case *en banc* on ripeness grounds,[5] leaving only weakly protected a central form of private communication in the digital age.

✶**What the Obama Administration Should Do.** 1) President Obama should work with Congress to update privacy statutes to account for the ways Americans communicate today. A guiding principle for such reform should be "technology neutrality," so that information stored in a remote computer enjoys the same Fourth Amendment protection it would enjoy if stored on the user's desktop computer. The collaborative process among the Department of Justice, the White House, Congress, and privacy advocates that resulted in ECPA itself could serve as a model for this endeavor.

---

[2] *See, e.g.,* opinion by Magistrate Judge Stephen Smith, *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F. Supp. 2d 747 (S.D. Tex. 2005).
[3] *Thoefel v. Farley-Jones,* 359 F.3d 1066 (9th Cir. 2004), *cert. denied,* 2004 Lexis 5573 (U.S. Oct. 4, 2004).
[4] 490 F.3d 455 (6th Cir. 2007).
[5] 532 F.3d 521 (6th Cir. 2008).

2) Specifically, President Obama should work with Congress on legislation to update ECPA to strengthen and clarify the standards for government access to communications and stored data and to take account of new communications technologies:

- The touchstone for these reforms should be the Fourth Amendment standard of judicial review and probable cause. Probable cause should be required for government access to:
  - Location information, regardless of whether it is stored or is collected in real time;
  - Email content regardless of how old it is and regardless of whether it has been opened by the recipient;
  - Other non-public content, regardless of whether it is maintained on a desktop or on the Web; and
  - Information maintained on a social networking page that is not open to the public.
- The standard for issuing a pen register or trap and trace order, which can be used by law enforcement to intercept very revealing information about a person's activities, should be tightened to require specific and articulable facts that the information sought is relevant to a pending investigation.
- 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.

✶**Other Voices.** While DOJ lawyers recognize the absurdity of some of the current rules, the Justice Department and other agencies will be hesitant to support some measures to require more judicial oversight of their surveillance activities. They will benefit, however, from the increased clarity in surveillance standards that an update to the law would provide. Industry representatives such as large Internet Service Providers, network providers and leading companies in the Information Technology industry are expected to support an update of ECPA. CDT has been involved in a year-long effort with industry leaders to develop recommendations, which will be ready early in 2009. Strong support is likely to come from legal scholars who have already written of the need for an update to ECPA.

✶**For More Information.**

CDT issue experts: James X. Dempsey, jdempsey@cdt.org, 415-814-1712
Gregory T. Nojeim, gnojeim@cdt.org, 202-637-9800 x113

Resources:
- CDT Report on Digital Search and Seizure: http://www.cdt.org/publications/digital-search-and-seizure.pdf
- CDT Policy Post on how digital technology requires stronger privacy laws: http://www.cdt.org/publications/policyposts/2006/4

November 13, 2008