ECPA

Parent: Security & Surveillance [1]
Current Issue: Current Issue
Intro:
[2]

The Electronic Communications Privacy Act (ECPA) of 1986 [3] is a federal statute that specifies standards for government monitoring of cell phone conversations and Internet communications. When first written, ECPA was a forward-looking statute that provided important privacy protections to subscribers of then-emerging wireless and Internet services. However, while technology has advanced dramatically in the decades since ECPA was enacted, the statute's privacy standards have not been updated, leaving important information without full protection. Meanwhile, the courts have been slow in extending the warrant requirement of the Constitution's Fourth Amendment to new technologies.

Consequently, the government claims the power to track our movements without a warrant, using our cell phones, which constantly report our location to our wireless service providers. And the government argues that it does not need a warrant to read much of our email or any of the documents that we store and share privately in the Internet "cloud."

The time has come for ECPA to be reformed to provide strong privacy protections while ensuring that law enforcement agencies can obtain the information they need to fight crime. The best way to do that is to ensure that government agents must get a warrant from a judge before tracking our movements or reading our private communications.

A BRIEF HISTORY OF SURVEILLANCE LAW

In 1967, the Supreme Court ruled that telephone conversations were protected by the Fourth Amendment of the Constitution, requiring the government to obtain a warrant from a judge in order to be able to listen in. The next year, in Title III [4] of the Omnibus Crime Control and Safe Streets Act of 1968 [5], Congress set out detailed standards for the government to follow when tapping a phone line. Title III, also known as the Wiretap Act, made it a crime to intercept telephone calls except with a judge's warrant or under some relatively narrow exceptions.

However, Title III only applied to voice communications over a wire or face to face. Technology continued to evolve. By the 1980's, companies were beginning to offer wireless telephone services, and businesses and individuals were beginning to communicate by transferring data, not voice. The Wiretap Act did not apply to email and other data transfers and it was unclear whether a cell phone conversation could be shoehorned into the Act's definition of a "wire communication." Meanwhile, the courts were uncertain whether communications using these new technologies were protected by the Fourth Amendment. The government argued that people surrendered their privacy when they used a mobile phone or sent their data through the computers of an Internet service provider.

A ruling by the courts that wireless or data communications were not private would have stopped development of these technologies dead in their tracks. So Congress adopted the Electronic Communications Privacy Act. ECPA added wireless communications and data communications to the Wiretap Act, making it clear that government agents needed a judge's warrant to intercept such

communications in transit.

However, in drafting ECPA, Congress was uncertain how to treat email when in storage with an email service provider. (ECPA gave email moving over the network essentially the same protection as a phone call or postal letter.) Congress said that while an email was in temporary storage, waiting to be accessed by the intended recipient, it should fall under the warrant standard. However, the Justice Department argued that, after a certain point, stored email became like abandoned property or the files of a business shipped off for "cold storage" and should no longer be considered private. At the time, electronic storage was expensive, and email service providers routinely deleted email after 30 or 90 days. Congress was swayed by the Justice Department's arguments. It assumed that, if someone wanted to keep a copy of an email, they would download it onto their own computer or print it out. Settling on what it thought was the outside limit of any conceivable network storage of email, Congress said that after 180 days email would no longer be protected by the warrant standard and instead would be available to the government with a subpoena, issued by a prosecutor or FBI agent without the approval of a judge.

At the same time, Congress concluded that, while the contents of communications must be highly protected in transit, the "transactional data" associated with communications, such as dialing information showing what numbers you are calling, was less sensitive. ECPA allowed the government to use something less than a warrant to obtain this routing and signaling information.

- Orin Kerr: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It [6]
- U.S. Department of Justice: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations [7]

TECHNOLOGICAL CHANGES SINCE ECPA WAS PASSED

In the 25 years since ECPA was enacted, new technologies have emerged, and the ways we use the Internet and communicate with one another have changed dramatically. Two developments stand out in particular: the movement of storage to "the cloud," that is to network servers, and the development of location-based services and the growing precision of location tracking capabilities of smart phones, cell phones and other mobile devices.

As a result of radically lower costs of storage and the availability of nearly ubiquitous Internet access, most people now save their emails indefinitely and they store them not on their hard drives but in the cloud, on the servers of their email providers. And people store not only email in the cloud, but also their calendars, their photos, draft documents and a wealth of other sensitive, private data. Any of this data stored on your laptop is fully protected by the Constitution, requiring a warrant for the government to seize it. And as you access the data in real-time over the Internet, your communications are fully protected by ECPA (and also by the Constitution). Yet the same data, sitting in your private, password protected account with a service provider, is available to the government without a warrant under ECPA.

The growing significance of location data is driven by two developments: the incorporation of GPS technology into cell phones and other mobile devices and the build-out of wireless networks with smaller and smaller cells and more and more WiFi hotspots, all of which are mapped to precise latitude and longitude. Maps, navigation aids, and other location-based services have become very popular. As a result, the constant generation of location data from a cell phone can reveal a person's activities and associations, far more precisely than Congress ever contemplated in 1986. ECPA does not set a clear standard for government access to this data. The government argues that it does not need a warrant to force a service provider to disclose your whereabouts in real-time or going back for weeks or months, precisely time-stamped and easily plotted on a map.

- CDT Policy Post: Digital Technology Makes Surveillance Easier, Requiring Stronger Privacy Laws [8]

ECPA REFORM

ECPA today is a confusing patchwork of standards that have been criticized by the courts and that bear little resemblance to the expectations that the average person has about the privacy of her personal communications. The courts have begun to respond -- one federal appeals court has held that ECPA is unconstitutional because it allows the government to read a person's email without a warrant -- but it could take years, even a decade or more, for the courts to work through all the issues posed by the new technology.

This situation is not in the best interest of citizens, corporations, or the government. Therefore, a diverse coalition of companies, think tanks, and public interest groups from across the political spectrum have founded Digital Due Process [9] and have called for change. The coalition has said that the following principles [10] should guide ECPA reform:

- Information should receive the same protection regardless of technology or platform.
- Reform should preserve the building blocks of criminal investigations--subpoenas, court orders, etc.--as well as the sliding scale that allows law enforcement to escalate investigations.
- Generally, a type of information should have the same level of protection whether it is in transit or being stored.
- How old a communication is--or whether or not it has been opened--should be irrelevant to the privacy protections it receives.
- All stakeholders--service providers, users and government investigators--deserve clear and simple rules.
- The exceptions that have been written into ECPA over the years should be left in place.

Based on these principles, Digital Due Process recommends that ECPA be amended to make it clear that the government, except in emergency situations, must obtain a warrant from a judge before reading a person's email or tracking his movements with his mobile phone.

KEY RESOURCES

- CDT Senate Testimony: The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age [11] (2010)
- CDT Blog Post: The Courts Boldly Go Fourth: Rulings Validate Digital Due Process [12]

Major Court Cases

- Katz [13] (Supreme Court, 1967) - holding that telephone conversations are protected by the Fourth Amendment and establishing the principle of "reasonable expectation of privacy.
- Smith v. Maryland [14] (Supreme Court, 1979) - deciding that the use of pen registers or trap and trace devices does not constitute a search requiring a warrant. Pen registers and trap and trace devices record dialed numbers, information the Court said that individuals voluntarily give to telephone companies
- Warshak [15] (6th Circuit, 2010) - held that law enforcement must have a warrant to obtain emails stored by email providers
- Application of the US [16] (3rd Circuit, 2010) – held that judges may require the government to obtain a warrant to access stored location information.

Weight: 1

Source URL: https://cdt.org/issue/wiretap-ecpa

Links:
[1] https://cdt.org/issue/security-surveillance
[2] https://www.cdt.org/feeds/child_issue/82/rss.xml
[3] http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.html
[4] http://www.it.ojp.gov/default.aspx?area=privacy&page=1284#contentTop
[5] http://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1615.pdf
[6] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860&
[7] http://www.cybercrime.gov/ssmanual/index.html
[8] http://cdt.org/policy/digital-technology-makes-surveillance-easier-requiring-stronger-privacy-laws
[9] http://www.digitaldueprocess.org/
[10] http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163
[11] http://cdt.org/files/pdfs/20100922_jxd_testimony_ecpa.pdf
[12] http://cdt.org/blogs/joshua-gruenspecht/courts-boldly-go-fourth-rulings-validate-digital-due-process
[13] http://www.law.cornell.edu/supct/html/historics/USSC_CR_0389_0347_ZS.html
[14] http://supreme.justia.com/us/442/735/
[15] http://scholar.google.com/scholar_case?case=11707608375476732 55&q=united+states+v+warshak&hl=en&as_sdt=2,9&as_ylo=2010&as_vis=1
[16] http://www.ca3.uscourts.gov/opinarch/084227p.pdf