Deep Dive: ECPA and the Future of Electronic Privacy.

Saturday, December 1 2012, 9:56 AM

EFFector Deep Dive every few months.

View as a web page

EFFector
A Publication of the Electronic Frontier Foundation

In our 626th issue:

Deep Dive: ECPA and the Future of Electronic Privacy

In most issues of EFFector, we give an overview of all the work we're doing at EFF right now. Today, we're trying something new: doing a deep dive into a single issue. If our readers find this valuable, we'll try to give you an EFFector Deep Dive every few months.

Yesterday was a watershed moment in the fight for electronic privacy: the Senate Judiciary Committee overwhelmingly passed an amendment that mandates the government get a probable cause warrant before reading our emails. The battle isn't over -- the reform, championed by Senator Patrick Leahy (D-VT), still needs to pass the rest of the Senate and the House, and be signed by the President to become a law. But yesterday, thanks to thousands of people speaking out, we were able to begin the process of overhauling our archaic

privacy laws into alignment with modern technology.

It was a big win for us, even if it was only the first step in the process of reforming privacy law to keep the government out of our inboxes. So we're dedicating this EFFector to the battle to reform outdated privacy law: what the government can get,

Announcements

Let's Stop DDoS Attacks Together

EFF Director for International Freedom of Expression, Jillian C. York, will speak about best practices for mitigating against DDoS (distributed denial of service) attacks as part of a discussion on the future of cyber security.
December 5, 2012
New York City, NY

LISA '12 - Large Installation System Administration Conference

EFF is happy to support USENIX's 26th Large Installation System Administration Conference! The annual LISA conference is the meeting place of choice for system and network administrators and engineers; it is the crossroads of Web operations, DevOps, enterprise computing, educational

what the law ought to be, and what we're doing to fix the gaping loopholes that leave users vulnerable to government snooping.

The Fourth Amendment and Electronic Privacy

The Fourth Amendment protects us from unreasonable government searches and seizures. In practical terms, this means that law enforcement has to get a warrant -- demonstrating to a judge that it has probable cause to believe it will find evidence of a crime -- in order to search a place or seize an item. In deciding whether the Fourth Amendment applies, courts always look to see whether people have both a subjective expectation of privacy in the place to be searched, and whether society would recognize that expectation of privacy as reasonable. The Supreme Court made this point clear in a landmark 1967 case, Katz v. United States, when it ruled that a warrantless wiretap of a public payphone violated the Fourth Amendment.

The Third Party Doctrine, or How the Supreme Court Got Us Into This Mess

In 1979, the Supreme Court created a crack in our Fourth Amendment protections. In Smith v. Maryland, the Court ruled that the Fourth Amendment didn't protect the privacy of the numbers we dialed on our phones because we had voluntarily shared those numbers with the phone company when we dialed them. This principle -- known as the Third Party Doctrine -- basically suggests that when we share data with a communications service provider like a telephone company or an email provider, we know our data is being handed to someone else and so we can't reasonably expect it to be private anymore.

The government took this small opening created by Smith v. Maryland and blew it wide open. It argued that this narrow 1979 decision about phone dialing applied to the vast amount of data we now share with online service providers -- everything from email to cell phone location records to social media. This is bogus and dangerous. When we hand an email message to Gmail to deliver on our behalf, we do so with an intention that our private communications will be respected and kept in strict confidence, and that no human being or computer

computing, and research computing.
December 9-14, 2012
San Diego, CA

ICLN 11th Annual Conference

EFF Senior Staff Attorney Matt Zimmerman will speak at the ICLN 11th Annual Conference: COMBATING CYBERCRIME, Legal and Technical Standardization and Cooperation on a National, European, and Global Scale.
December 11-16, 2012
The Hague, Netherlands

Policing the Internet

Director for International Freedom of Expression Jillian C. York will represent EFF at Policing the Internet: Policy, Politics, and Consequences of Regulating Internet Content at the European University Institute.
December 14-15, 2012
San Domenico di Fiesole, Italy

Global Congress 2012

Carolina Rossini, EFF Director of International Intellectual Property, will organize a workshop on TPP negotiations and Global Chokepoints, a movie exhibition, and a discussion of OER and E&L for education issues.
December 15-17, 2012
Rio de Janeiro, Brazil

EFF on

will review the message other than the intended recipient. But the government argues that because we handed our communications to a service provider, the Fourth Amendment doesn't require them to get a warrant before snooping around our inbox.

Luckily, the courts are beginning to agree with us. In a leading case where EFF participated as amicus, United States v. Warshak, the Sixth Circuit Court of Appeals agreed with us that people had a reasonable expectation of privacy in their email, even if it is stored with a service provider, and therefore the government needed a search warrant to access it. And in the recent Supreme Court case, United States v. Jones, Justice Sotomayor said that she thought the Third Party Doctrine was outdated, while she and four other Justices -- including Justice Alito -- raised concerns about the information gathered by our cellphones.

The Eighties Were Good for a Lot of Things -- But Not Sustainable Email Privacy Law

It's not just the Constitution, however. Congress has made clear that certain forms of data are protected by federal statute as well. Following the Katz decision, Congress passed the Wiretap Act in 1968, supplementing the strong Fourth

Amendment privacy protections in phone conversations by enacting a comprehensive set of federal statutes. These statutes were designed to ensure that law enforcement has a compelling reason before intercepting phone calls.

And as electronic communication started to become more prevalent, Congress passed the Electronic Communications Privacy Act (ECPA) in 1986 that somewhat improved the privacy rights around certain electronic communications. But as it reflects the technology of 1986, ECPA has aged poorly. It doesn't address documents stored in the cloud, information revealing our personal associations, or the vast quantities of location data our mobile devices collect on us everyday. And, as a result of loopholes in the law, the Department of Justice, citing ECPA, has argued that it has a right to access emails without a warrant as soon as they are 180 days old, or have been opened and left on the server.

We think that 180-day limit and a distinction between opened and unopened email is arbitrary and wrong. As the Washington Post said in an editorial earlier this week, "If you left a letter on your desk for 180 days, you wouldn't imagine that the police could then swoop in and read it without your permission, or a judge's."

That's why this week's vote was so important: it was a critical first step in updating ECPA to evolve with the modern technologies we use today, and to close archaic loopholes that give government too much access with not enough judicial oversight.

What EFF and Activists Like You Are Doing

We're taking a two-prong approach.

First, we're fighting for the Fourth Amendment in the courts. We practice impact litigation, taking on clients pro-bono in cases

where we believe we can create positive legal precedent around digital privacy and government surveillance. We also submit amicus briefs in cases where we don't have a direct client, such as in the Warshak and Jones cases noted above. In Warshak we argued that the government could only access emails stored on an ISP with a search warrant, notwithstanding the third party doctrine. And in Jones, we argued the government's attachment of a GPS tracking device to a car for 28 days was a Fourth Amendment "search," meaning a warrant was required. The Court agreed with us in both cases, and as a result privacy protections are stronger now than in the past. And we've filed many more amicus briefs this past year, arguing for a search warrant requirement in cases involving cell phone location records [PDF], GPS devices, and home video surveillance.

Second, we're creating a movement of engaged Internet users and rallying them to demand the government stay out of our email. Yesterday's win was a result of the tens of thousands of concerned individuals who signed our petition to Congress calling for ECPA reform and who spoke out in other ways. We're also teaming up with advocacy groups, web companies, start-ups, and venture capitalists in demanding ECPA reform through the Digital Due Process coalition. And we recently

joined other advocacy groups in launching VanishingRights.com.

What aren't we doing? Compromising. Unfortunately often the pressure in DC inside politics is to trade off one important right against another. We don't think that's EFF's role. Instead, we're advocating for what's best for the Internet and Internet users, and while we are flexible, we aren't willing to horse trade with your privacy and due process.

Want to read more about ECPA and our work to reform it? Check out these links:

Attempt to Modernize Digital Privacy Law Passes the Senate Judiciary Committee

ECPA and the Mire of DC Politics: We Shouldn't Have to Trade Video Privacy to Get Common-Sense Protections of our Email

Don't be a Petraeus: A Tutorial on Anonymous Email Accounts

Reform to Require Warrant for Private Online Messages Up for Vote, but Down on Privacy

When Will Our Email Betray Us? An Email Privacy Primer in Light of the Petraeus Saga

Supported by Members

Our members make it possible for EFF to bring legal and technological expertise into crucial battles about online rights. Whether defending free speech online or challenging unconstitutional surveillance, your participation makes a difference. Every donation gives technology users who value freedom online a stronger voice and more formidable advocate.

If you aren't already, please consider becoming an EFF member today.

Donate Today

Administrivia

Editor: Adi Kamdar, Activist
editor@eff.org

EFFector is a publication of the Electronic Frontier Foundation.
eff.org

Membership & donation queries: **membership@eff.org**

General EFF, legal, policy, or online resources queries: **info@eff.org**

Back issues of EFFector

Change your email address

This newsletter is printed from 100% recycled electrons.

EFF appreciates your support and respects your privacy. **Privacy Policy**.

Unsubscribe or change your email preferences, or **opt out of all EFF email**

454 Shotwell Street
San Francisco, CA 94110-1914
United States