Mother Jones

The Most Dangerously Outdated Laws Governing the Internet, Explained

By: Dana Liebelson – July 16, 2013

The last time Congress passed a sweeping electronic privacy law, the Berlin Wall was standing, Reagan was cracking down on drugs, and compact discs—playing Slayer and Judas Priest—were all the rage. More than twenty five years later, Congress is still using more than one 1980s law to govern technology that didn't even exist when the legislation was written. As Americans place an increasing amount of personal data in social networks, cell phones, and email accounts—Internet freedom advocates say that it's downright dangerous not to update privacy laws to reflect changing technology—particularly in the wake of the recent NSA disclosures made by Edward Snowden. Here are some of the most outdated technology laws:

The Computer Fraud and Abuse Act (CFAA): Your eHarmony Date is a Criminal

This anti-hacking law was birthed in 1984 by a bunch of lawmakers freaked out over the movie WarGames—a clip of which was shown during congressional testimony. The intention of the law was to give the government and US companies the tools to crack down on cyber attacks like this:

VIDEO

Today, thanks to the law's vague language, it can be used to turn an average Internet user into a federal criminal. Under CFAA, it's illegal to "knowingly [access] a computer without authorization" and obtain information from a "protected computer." The way you get authorization to access most sites is to agree to a company's terms of service (that agreement check-box you click when you sign up for an account.) CFAA empowers companies to bring criminal lawsuits against users who break their terms of service, meaning that a person could face jail time, not simply a fine. This is highly unusual, as contract terms can be completely arbitrary. For example, there are definitely a ton of federal criminals on the dating site, eHarmony, whose terms read:

> Marital Status. By requesting to use, registering to use, or using the Singles Service, you represent and warrant that you are not married. If you are separated, but not yet legally divorced, you may not request to use, register to use, or use the Singles Service....You will not provide inaccurate, misleading or false information to eHarmony or to any other user."

Hanni Fakhoury, a staff attorney for the Electronic Frontier Foundation, says this gives companies an "absurd" amount of power to bring lawsuits against users they don't like. It also allows the government to charge people who violate the act twice for the same crime—under federal and state law—which leads to the kinds of sentences faced by internet activist Aaron Swartz, who was threatened with 35 years in prison under CFAA

for allegedly stealing mass amounts of academic articles with the intention of making them public. Swartz committed suicide before his case went to trial. In June, a bill called Aaron's Law was introduced in the House and Senate. It reforms CFAA by fixing the terms of service issue and preventing users from being charged twice for the same crime.

The Stored Communications Act (ECPA): It's Easy for the Government to Read Your Old Emails

The Stored Communications Act was enacted in 1986 as part of the broader Electronic Communications Privacy Act (ECPA). Its aim was to stop service providers from giving Americans' stored phone and Internet communications away without a user's consent. The law also prohibits phone and email providers from giving away communications that had been stored for under 180 days to law enforcement without a search warrant. Why the 180 day cut-off? Well first of all, in 1986, high-tech cell phones looked like this:

VIDEO

And as the Center for Democracy and Technology notes, "At the time, electronic storage was expensive, and email service providers routinely deleted email after 30 or 90 days. Congress...assumed that, if someone wanted to keep a copy of an email, they would download it onto their own computer or print it out." Needless to say, today with Gmail, users can keep their email for far longer than 180 days—but the law hasn't changed. That means that law enforcement must meet a much lower standard in order to seize archived email, such as getting a subpoena. Under some interpretations of the law, protections are greater for email that has been opened, so you might want to get cracking on your inbox. "I don't use Gmail or Hotmail or any of those things," says Lee Tien, a Senior Staff Attorney with the Electronic Frontier Foundation. "I don't see any reason why I should let a provider sit there with a pile of my old emails that they could easily give away to the government. Apparently many people don't care, or they don't know."

National Security Letters (ECPA): Which Parts of Your Email Are Off Limits? Ask The Phone Companies

National Security Letters, which are controversial documents used by the FBI to secretly compel the disclosure of certain online records, are also technically part of ECPA. Under the law, the FBI can compel companies to turn over online information that is equivalent to toll billing records—aka, the phone number you called, how long you spoke, ect. But as Julian Sanchez, research fellow for the CATO Institute notes, "it's totally unclear what that means in practice. Taken literally, as applied to many online services, there are NO "billing records" ("toll" or otherwise) because the sites are free and ad supported. For Internet providers, on the other hand, the literal "billing records" will probably, at most, just contain a flat monthly fee and maybe the total number of megabytes downloaded."

Left open to interpretation, national security letters could potentially compel information like the size of an email, the URL of each individual page, or even each time someone logs into a chat session. While the FBI is forbidden from getting content from a NSL, Sanchez notes that with broad interpretation, "sufficiently detailed metadata can often, at least in theory, be used to reconstruct or reverse engineer content." He adds that "you can bet the FBI pushes for the broadest interpretation a company's lawyers will accept."

ECPA: Dude, Where's My Car?

When ECPA was enacted, its backers likely had no idea that in less than three decades, cell phones would have the technology to map exactly where a user is, at all times. And as a result, ECPA does not set a clear protocol for how the feds can tap into GPS data. The Supreme Court ruled in January 2012 that law enforcement must get a warrant in order to physically place a GPS tracking device on a vehicle. But that same standard doesn't have to be met if the government simply wants to ask your cell phone company where you are. According to the Center for Democracy and Technology, "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."

In March of this year, a bill was introduced in the Senate and the House that would require police to get a warrant before obtaining location data from service providers, or finding someone in real-time by using information sent from from their cell phones. Both bills have been idling in committee since March. Chris Calabrese, the legislative counsel in the ACLU's Washington Legislative Office, told Wired, that he supports the bills because "Innocent people shouldn't have to sacrifice their privacy in order to have a cellphone."

The Fourth Amendment...Doesn't Really Apply to Facebook

"The biggest area where the law has failed to keep pace with technology is the collection and use of personal by information by large companies, such as Google, Facebook, data brokers, and others," says Marc Rotenberg, executive director of the Electronic Privacy Information Center. Right now, data brokers—companies that work with sites such as Facebook to better target online advertisements—know everything from "whether you're pregnant or divorced or trying to lose weight, about how rich you are and what kinds of cars you have," notes ProPublica. And Snowden's disclosures about PRISM, the NSA's massive surveillance program that requires cooperation from US tech companies, have raised big questions about how much personal information tech companies should be allowed to collect on users, and what they can do with that information once they have it.

"Current Fourth Amendment jurisprudence appears to leave data mining completely unregulated," notes Christopher Slobogin in the University of Chicago Law Review. Europe has strong privacy laws that routinely clash with the whims of tech giants—they're spending millions of dollars lobbying to weaken them—but no equivalent framework exists in the United States. Rotenberg says that President Obama's Privacy Bill of Rights, which he introduced in February 2012, is a good start in giving Americans the ability to opt out of online data collection. But he says, "it needs to be enacted into law. That is the top priority. By comparison, the other stuff is 'nip 'n tuck.'" Tien agrees that US law governing the Internet is defined more "by what we don't have, than what we do. We have laws that go out of date, and in-between, it's kind of a desert."