Mother Jones

The 3 Most Absurdly Outdated Internet Laws

When federal tech law is inspired by a Cold War-era hacker flick starring Matthew Broderick, it's probably time for an update.

By: Dana Liebelson - July 19, 2013

The last time Congress passed a sweeping electronic privacy law, the Berlin Wall was standing, Reagan was cracking down on drugs, and cassette tapes—playing Men at Work and Duran Duran—were all the rage. More than 25 years later, there are more than a few '80s-era laws on the books governing the use of technology that didn't even exist when the legislation was written. As Americans place an increasing amount of personal data in social networks, cellphones, and email accounts, privacy advocates say that it's irresponsible not to update these laws to reflect changing technology. Here's a sampling of some of the nation's most outdated tech laws:

The Computer Fraud and Abuse Act
This anti-hacking law was birthed in 1984 by a bunch of lawmakers freaked out over the movie WarGames*—a clip was shown during congressional testimony—in which a teenaged hacker played by Matthew Broderick accidentally brings the United States and the Soviet Union to the brink of nuclear war.*

Today, the law's broad language can technically be used to prosecute internet users for offenses that seem downright silly. Under the CFAA, it's illegal to "knowingly [access] a computer without authorization" and obtain information from a "protected computer." Here's the problem: The way you get authorization to access most web sites is to agree to a company's terms of service (that check-box you click when you sign up for an account). The CFAA allows the feds to bring criminal charges against users who break companies' terms of service, meaning that a person could face jail time, not simply a fine, for what's essentially a civil disagreement. In other words, a user of the dating site eHarmony who lies about his or her marital status is technically breaking federal law, since its terms of service read:

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.

The law also allows the government to charge people who violate the CFAA twice for the same crime—under federal and state law—which leads to the kind of sentence faced by internet activist Aaron Swartz, who was threatened with 35 years in prison under the CFAA for allegedly stealing mass amounts of academic articles with the intention of releasing them for free to the 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 would reform CFAA by fixing the terms-of-service issue—simply violating the terms would no longer be a crime; instead, a hacker would have to actually break a technological barrier (like cracking a password)—and it would also prevent users from being charged twice for the same crime.

The Digital Millennium Copyright Act

The Digital Millennium Copyright Act is a cutting-edge piece of legislation intended to bring copyright law into the internet age—or at least it was in 1998. The law originally aimed to stop copyright infringement online and protect internet service providers. Big movie studios want to reform it (including through the highly unpopular Stop Online Piracy Act) because they don't think the law does enough to prevent piracy. But internet freedom advocates have a beef with the law because they say it chills freedom of expression. For example, under the DMCA, companies may deliver take-down notices when they're not happy with the way copyrighted content is being used—and because lawsuits are so expensive, tech companies will usually comply, even if they may be trampling on a user's First Amendment rights. Teachers have been targeted under the DMCA for using copyrighted material for educational purposes—and security researchers, like Dutch cryptographer Niels Ferguson, who found a security flaw in Intel's video encryption, have been reluctant to release their work because they may face criminal penalties. It's also been wielded by music studios to crack down on people who mash-up music—like DJs—or people who put copyrighted music on YouTube. In one case, Universal Music Corporation invoked the law against a mother who uploaded a YouTube video of her children dancing to Prince's "Let's Go Crazy." (She ultimately won the right to keep it up.)

The law also prohibits things like the unlocking of a cellphone, since service providers put proprietary software on phones so that they can't be used with a competing carrier's service. Tampering with the software is interpreted as violating a cellphone company's copyright. That also affects visually impaired people who install extra technology in order to read e-books, because the software conflicts with a publisher's copyright. "For me, using a screen reader is not exactly the same thing as paying to listen to Vincent Price read a novel," Mark Richert, director of public policy for the American Foundation for the Blind, told *Mother Jones* earlier this year. Rep. Zoe Lofgren (D-Calif.) introduced a bill this spring that would protect law-abiding Americans who modify their electronic devices—but it's been languishing in committee since May.

The Electronic Communications Privacy Act

The Stored Communications Act was enacted as part of the broader Electronic Communications Privacy Act (ECPA). Its aim was to stop service providers from releasing Americans' stored phone and internet communications without their consent. The law also prohibits phone and email providers from providing communications to law enforcement without a search warrant, if they have been stored for fewer than 180 days. Why the 180-day cutoff? Well, first of all, let's take a second to remember what computers looked like in 1986:

As the Center for Democracy and Technology explains, "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's email users often keep their messages indefinitely—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 merely getting a subpoena. "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."

The ECPA also authorized the use of National Security Letters, the controversial documents used by the FBI to secretly compel the disclosure of certain online records. When the law was drafted, lawmakers envisioned giving law enforcement agents the ability to compel phone carriers to turn over toll billing records—that is, the phone number you called, the

duration of the call, etc. But in the internet age, NSLs now apply to a whole new world of data, notes Julian Sanchez, a Cato Institute research fellow who specializes in privacy and tech issues. "It's totally unclear what that means in practice," he says. "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, NSLs could potentially compel information like the size of an email, the URLs of web pages users visit, or the time at which someone logs into a chat session—information that is far more expansive than what was envisioned under the law. While the FBI is forbidden from seeking email content using an NSL, Sanchez says that "sufficiently detailed metadata can often, at least in theory, be used to reconstruct or reverse engineer content." He adds, "You can bet the FBI pushes for the broadest interpretation a company's lawyers will accept."

When the ECPA was enacted, its backers also didn't envision an age of cellphone technology that made it easy to track the comings and goings of users. Christopher Calabrese, legislative counsel for privacy-related issues at the American Civil Liberties Union, notes that the Justice Department can use a section of the law to get location data from cellphones without a search warrant. Considering that 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, that's a pretty big loophole.

In March, a bill was introduced in the Senate and the House that would require law enforcement authorities to get a warrant before obtaining location data from service providers. Both bills have been idling in committee since March. Calabrese told *Wired* that he supports the bills because "innocent people shouldn't have to sacrifice their privacy in order to have a cell phone."