



In Memory of Aaron Swartz: Reboot Draconian Computer Crime Law

In the wake of social justice activist Aaron Swartz's tragic death, EFF has been working with a coalition of legislators and experts to reform the Computer Fraud and Abuse Act (CFAA), the infamously problematic U.S. anti-hacking law. Enacted in 1986, the CFAA is dangerously broad and wildly outdated.

In June, Reps. Zoe Lofgren and Jim Sensenbrenner introduced **Aaron's Law**, a terrific start to bringing the CFAA into the modern era.

What's wrong with the CFAA?

You can be criminally liable for violating a website's terms of service

Lying about your age on Facebook? Letting a friend log in to your Pandora account? Saying you're "tall, dark and handsome" on Craigslist when you're actually short and homely? These are all violations of terms of service—those long walls of text that you "agree" to before using a website or service.

According to the government's interpretation of the CFAA, violating this fine print—something any Internet user can easily do—could mean criminal penalties. It's dangerous for a private, one-sided contract to be enforceable with punishment of severe criminal penalties at a prosecutor's whim.

Solution: No criminal exposure for violating private agreements or duties

Accessing information in an innovative way can be a crime

As the CFAA is written today, users can expose themselves to criminal liability if they are authorized to access data, but do so while engaging in commonplace "circumvention" techniques like changing IP addresses, MAC addresses, or browser User Agent headers. But these "circumvention" activities can have great benefits: they can help protect privacy, ensure anonymity, and aid in testing security.

Solution: If access to data is already authorized, gaining that access in a novel or automated way is not a crime.



Current penalties are extremely harsh

As a general principle, minor violations of the CFAA should be punishable with minor penalties. As the law is currently written, first-time offenses can be too easily charged with felonies instead of misdemeanors.

Furthermore, several sections of the CFAA are redundant with other parts of the law, which lets prosecutors "double dip" to pursue multiple offenses based on the same behavior. And the stiff penalties for "repeat" offenses can be used to dole out harsher punishment for multiple convictions based on the same conduct. Prosecutors shouldn't count the same actions more than once to ratchet up the pressure for a plea bargain by threatening a defendant with decades of jail time.

Solution: Make penalties proportionate to offenses

Common sense reform: Aaron's Law

In June, Reps. Zoe Lofgren and Jim Sensenbrenner as well as Sen. Ron Wyden introduced a bipartisan fix to the Computer Fraud and Abuse Act, called **Aaron's Law**. The bill draws from EFF's own proposal written in the wake of Aaron Swartz's tragic death and fixes some of the main problems with the CFAA.

In order to bring sanity to the CFAA, we need your help.

Here's what you can do

Email Your Representative

Tell Congress that we need to fix computer crime law at eff.org/Aarons-Law or scan the QR code to go directly to EFF's Action Center tool.



Learn more about EFF's CFAA reform proposals at eff.org/CFAA

Call Your Representative in Congress

Use our toll free number to call your Representative and demand change:

STEP 1: Call **1-866-338-1015** to reach the Congressional switchboard.

STEP 2: Ask to be connected to your Representative.

STEP 3: Tell the staffer or leave a voicemail *politely* urging your Representative to support Aaron's Law. Say something like:

*Hi, I'm a constituent of the Representative and want to urge him/her to support **Aaron's Law, HR 2454**, to reform the Computer Fraud and Abuse Act. The CFAA overcriminalizes everyday online Internet activity and is sorely out of date. The representative must support the common sense changes to the CFAA that are found in Aaron's Law HR 2454.*