It's Time to Reboot Our Draconian, Outdated Computer Crime Law — Before it Destroys Open Access to Information Online

EFF has been working to reign in the Computer Fraud and Abuse Act (CFAA), the infamously problematic U.S. anti-"hacking" law, for years—both in Congress and in the courts. The CFAA is wildly outdated and notoriously vague. It was enacted in 1986, when there were only about 2,000 computers connected to the Internet. The law makes it a crime to access a computer connected to the Internet "without authorization" but fails to explain what this means.

Courts don’t even agree about what the CFAA covers. As a result, while the law was passed with the aim of outlawing computer break-ins, it has since metastasized in some jurisdictions into a tool to enforce computer use policies, like terms of service, which no one reads. The statute’s vague language has also enabled overzealous prosecutors, like the prosecutors behind Aaron Swartz’s tragic case, to use the law to go after behavior that doesn't have anything to do with computer break-ins.

The CFAA is notorious for chilling the work of security researchers. And now, thanks to efforts to use the CFAA as an anti-competitive tool, the CFAA is threatening open access to information on the web. Companies are trying to turn the law into a tool to block their competitors from using automated web browsing tools to access publicly available information. But giving websites the power to block anyone they don’t like from accessing public information would threaten open access for everyone.

Both Congress and the courts need to reign the statute in to what Congress originally intended—targeting malicious computer break-ins.

We’ve had some success in the courts, but the fight is far from over. Companies across the country continue to pursue dangerous interpretations of the CFAA, and we continue working to convince courts that the statute must be contained to the purpose Congress intended. Until—and after—we achieve these much-needed reforms, EFF will continue to advise and represent security researchers concerned about potential CFAA issues as part of our Coders’ Rights Project. Visit eff.org/issues/coders for more info, and email info@eff.org with requests for assistance.
Why do we need to change the CFAA?

Violating a website's terms of service—or any written private agreement or computer use restriction—should not be a crime.

Lying about your age on Facebook in violation of a terms of service shouldn't be the basis for CFAA liability. But some federal courts of appeal say that violating a website's fine print could mean criminal penalties. It's dangerous for a private, one-sided contract to be enforceable via severe criminal penalties. This turns millions of innocent people into potential criminals for ordinary behavior and ensures that people won't have notice of what conduct is illegal. It also gives prosecutors broad, unchecked discretion—which we've already seen abused.

Accessing information in an innovative way should not be a crime.

Using technological advances to make the collection of information easier should not be a crime. But according to some companies' interpretation of the law—which some federal courts have accepted—accessing information you are authorized to access in a manner the computer owner doesn't like can be a criminal offense. But accessing data that you are already authorized to access should never be a crime.

Current penalties are too harsh, and not proportional with offenses.

As a general principle, minor violations of the CFAA should be punishable with minor penalties. As the law is currently written, first-time offenders can be charged with felonies instead of misdemeanors, and 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. The stiff penalties for "repeat" offenses can be used to dole out harsher punishment for multiple convictions based on the same conduct in order to ratchet up the pressure for a plea bargain.

Common sense reform starts with Aaron's Law.

Proposed legislative fixes—like Rep. Zoe Lofgren's "Aaron's Law"—are a great start. They unfortunately haven't gained much traction, in part thanks to the unwillingness of tech giants to support needed reform. Not only that, but they don't go far enough. To fix the CFAA, we need to clarify the law's language to reflect Congress' original purpose of targeting those who break into computers in order to access or steal information—and not to give companies a tool for blocking the use of technological advances to access publicly available information online.

Brilliant, talented, visionary people should be spending their time building our future—not worrying about whether their research will land them in a federal prison. Until we update the CFAA, the law will continue to chill the work of security researchers and academics—putting us all at risk.

In order to bring sanity to the CFAA, we need your help: Join EFF and support our work to reign in the CFAA. EFF is a member-supported non-profit. Join today at eff.org/join

The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation. https://eff.org