Rebooting the Computer Fraud and Abuse Act

EFF has been working to rein 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 The CFAA is both outdated and vague. Recently, we've had some positive momentum, thanks to court rulings and changes in federal policy, but more work needs to be done to fix the law.

Congress enacted the CFAA 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" or to "exceed authorized access," but it fails to explain what these terms mean.

Courts have split about what conduct the CFAA covers. As a result, while the law was passed with the aim of outlawing computer break-ins, it has gradually become a tool to enforce violations of written computer use policies, like terms of service, which virtually no one reads. The CFAA is also known for chilling the work of security researchers and journalists, who may find unexpected ways of accessing other's computers without actually "breaking in."

In 2021, the Supreme Court issued its first decision interpreting the CFAA, *Van Buren v. United States*, holding that a police officer did not "exceed authorized access" by using a law enforcement database for an unofficial purpose that violated the police department's written rules and procedures. The Court wrote that the CFAA does not encompass "violations of circumstance-based access restrictions on employers' computers" and adopted what it called a "gates-up-or-down approach." Unfortunately, the Court stopped short of rejecting all "contract-based" restrictions on access, leaving open the question of whether breaking terms of service can ever lead to a CFAA violation.

In *hiQ v. LinkedIn*, issued in 2022, the Ninth Circuit Court of Appeals built on *Van Buren*, holding that the CFAA likely does not bar scraping data from a public website against the wishes of the website owner. However, the court reiterated an earlier misguided decision that allows owners of websites that are not fully public (such as Facebook) to invoke the CFAA against unwanted behavior, so long as they give personalized notice to the offending user.

Also in 2022, the Department of Justice announced a new policy under which it will not bring CFAA prosecutions against those engaged "solely" in "good faith" security research. It's an important step forward that the DOJ recognizes the invaluable contribution made by security researchers, and the CFAA's power to chill their work. But the new policy, which is only an agreement for the DOJ to exercise restraint, falls far short of protecting security researchers from overzealous threats, prosecutions, and the CFAA's disproportionately harsh prison sentences. We still need comprehensive legislative reform to address the harms of this law.

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 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?

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.

Generally, 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 to ratchet up the pressure for a plea bargain.

Common sense reform *starts* with Aaron's Law.

Rep. Zoe Lofgren's "Aaron's Law," introduced in 2013, would have been a great start. However, legislative fixes unfortunately haven't gained much traction, in part thanks to the unwillingness of the DOJ and tech giants to support needed reform. And 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 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.

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