The Computer Fraud and Abuse Act: Current Coverage and Needed Reform

LAUREN HARRIMAN*

In 1984, Congress was facing a rapidly changing technological landscape. The world wide web was not yet available at the consumer level, but Internet use was growing quickly among universities. Law enforcement officers felt unprepared to handle what they believed would be “brand new” crimes of the Internet. Officers were not only concerned with domestic computer security threats, but international threats as well. Thus, in 1986, Congress enacted the Computer Fraud and Abuse Act (CFAA) to clarify the law surrounding computer-related crimes. However, the “brand new” Internet crimes that law enforcement feared and the CFAA meant to address were not entirely novel. In fact, the CFAA duplicated charges for several crimes already included in the Penal Code, simply providing prosecutors with one more tool to use in plea bargaining.

In plea negotiations, prosecutors are able to threaten law violators with extensive jail time if a settlement cannot be reached. This is especially true when prosecutors can charge violators under multiple statutes for the same crime. This plea bargaining tactic discourages the exercise of the right to a jury because violators are not willing to risk being found guilty of all charges. Aaron Swartz, prosecuted under multiple sections of the CFAA for excessively downloading documents from JSTOR over MIT’s network, fell prey to this tactic in 2012. Rather than face a sentence of thirty years in prison, Swartz committed suicide in 2013. His fate has united the Internet community in demanding for reformation of the CFAA.

Although the CFAA is necessary to protect against the hacking of critical infrastructure, amendments to the Act have since expanded it to cover any “computer involved in interstate communication.” Due to the infrastructure of the Internet, it is almost impossible to use a computer to access the Internet without sending a communication outside of the state where the computer is located, thereby potentially implicating the CFAA.

* J.D. Candidate 2015, University of San Francisco School of Law.


5 Id.

anytime a user accesses the Internet. Even something as simple as running a Google search will send a communication to a computer outside of the user’s state.

Further, because the CFAA does not define “unauthorized access,” the Act has been interpreted to cover Terms of Service (TOS) violations. Thus, law enforcement can charge users under the CFAA if a user violates a TOS, his use of a given website is “unauthorized,” and any information he retrieves from the site is information obtained from “a computer . . . which is used in . . . interstate . . . communication” in violation of the CFAA.7 Though prosecutors argue that they will only target serious violators, several of the charges brought against Swartz were simply violations of JSTOR’s TOS. Swartz exceeded his authorized access of JSTOR’s website and was accused of downloading educational documents in order to make them available to the public.8 His actions can hardly be considered a threat to critical infrastructure.

Unfortunately, the laws of cyberspace often develop during cases which tug at the public’s heart strings. For instance, in United States v. Drew, the defendant created a MySpace account and used it to bully a thirteen-year-old girl, who eventually committed suicide.9 Fortunately, the court in Drew kept emotion out of its decision and recognized that prosecutions for TOS violations under the CFAA may be unconstitutional. The court granted the defendant’s void-for-vagueness motion despite any personal need it may have felt to hold the defendant accountable.10 The Electronic Frontier Foundation (EFF), an organization devoted to electronic civil rights, even noted that the girl who committed suicide was herself violating MySpace’s TOS, which require that users be over the age of fourteen.11

The Internet community remains intent on amending the “unauthorized access” portion of the CFAA to prohibit actual hacking rather than simply computer research or mere URL manipulation.12 The EFF supports Congresswoman Zoe Lofgren’s proposed approach to the CFAA, which would redefine “access without authorization”13 as “to circumvent technological access barriers to a computer, file, or data without the express or implied permission of the owner or operator of the computer to

---

7 Id.
10 Id.
access the computer, but does not include circumventing a technological measure that does not effectively control access to a computer, file, or data.”

Lofgren’s proposed language would place the burden on the server owners to protect their data and their users’ data, rather than on Internet users to not poke around where they were not “invited.” Server owners, however, want their content secure. The Googles and Facebooks of the world likely believe that they need TOS to protect their servers and are thus not likely to support a bill which would shift the burden of protection to server owners.

The potential misuse of the CFAA by law enforcement must be weighed against the burden placed on service providers to protect data. In balancing these sides, we must keep in mind the Aaron Swartz’s of the world. Rather than prosecuting violators like Swartz, prosecutors should be focusing on the threats which the CFAA was originally created to protect against: threats against critical infrastructure, which, due to the nature of the Internet, can come from anywhere on the globe. This goal of the CFAA can be achieved by amending the language of the CFAA to criminalize only true hacking activities.

14 Id. at 1 (emphasis added).