Anti-hacking Law Questioned After Death of Internet Activist

Reuters

Lie about your identity on Facebook or delete files from your work laptop before you quit and you could run afoul of a 29-year-old U.S. computer security law that some experts say has been changed so often it no longer makes sense.

The U.S. Computer Fraud and Abuse Act has come under renewed criticism after last week's suicide of Internet activist Aaron Swartz, who could have faced prison time for alleged hacking to download millions of academic articles from a private database through a network at the Massachusetts Institute of Technology.

The 26-year-old's family blamed the suicide on "intimidation" from what they described as an overzealous U.S. prosecutor, who threatened Swartz with prison and up to $1 million in fines.

Swartz, who helped found popular website Reddit, had "problems with depression for many years," his friend, science fiction author Cory Doctorow, wrote in an online eulogy on Saturday.

The U.S. attorney's case was based on the 1984 CFAA law, which some legal experts contend has been amended so many times that some portions of it no longer make sense. Penalties for minor offenses can exceed those for more serious crimes and key terms of the law, written before the arrival of the Internet as a cultural phenomenon, remain undefined.

"So much has changed and gotten more complicated and the law has kept Frankenstein-ing," said Eric Goldman, a professor at the Santa Clara University School of Law. "You step back and see that it's become a horrible, hideous monster."

Other legal experts said the prosecution, led by U.S. Attorney Carmen Ortiz in Boston, followed the law closely in bringing charges against Swartz, who argued that research created with public funds should be freely shared on the Internet.

Authorities charge that, when MIT tried to shut off the downloads, Swartz hid and altered his computer's network identity and eventually sneaked into a closet at the university's Cambridge, Massachusetts, campus to gain access to the 4 million articles.

"The prosecutors weren't stretching the law to fit the facts," said Orin Kerr, a professor at George Washington University law School and a former federal prosecutor. "The law is broad and seems to cover this kind of act."

PROSECUTORS PUSH ON

The act penalizes a person who accesses computers "without authorization, or exceeds authorized access" to obtain something of value worth at least $5,000. But courts across the United States have split about just what constitutes unauthorized access.

In one case, a court upheld a lawsuit against an employee who deleted files from his work laptop before quitting to form a competing business. Once the defendant decided to quit, he no longer was authorized to access his laptop, the court said.

In a better known case, a judge overturned hacking charges against a woman from Missouri after she created a false profile on social networking site MySpace to fool a teenage girl who later committed suicide. Prosecutors alleged the woman did not have authorization to access MySpace servers because she violated the site's terms of service.

The confusion has not slowed prosecutors, who have brought 297 federal criminal cases under the CFAA and related computer fraud laws from 2010 through 2012, about the same as in the prior three years, according to court filings reviewed in Westlaw, a legal data division of Thomson Reuters.

Over the same period, nearly 300 civil lawsuits were brought in private disputes citing the CFAA and related laws, up from 243 in the prior three years, the filings show.

Prosecutors have taken advantage of the vague terms to add huge penalties to lesser cases, said Marcia Hofmann, a senior staff attorney at the Electronic Frontier Foundation, a non-profit civil liberties organization.

"They make an aggressive reading of what unauthorized access means to try to throw the book at somebody," she said. "Usually, their real beef isn't with the hacking, but with something else the person did that the prosecutor didn't like."

Hofmann and many of Swartz's supporters believe that might be what happened to the popular online activist, one of the inventors of a key Internet standard called RSS, which is used by media companies and bloggers to distribute articles. More than 30,000 people have signed an online petition calling on the administration of President Barack Obama to remove U.S. Attorney Ortiz from Swartz's case, a move that would have little practical effect after his death.

Ortiz's office declined to comment.

Swartz had been investigated before after downloading almost 20 million pages of text from a government-run database of court records called PACER in 2008. No charges were filed.

But he got into more serious trouble in 2011 after the MIT incident, which led to his prosecution in a trial that had been due to start in a few months.

Following Swartz's death, MIT President Rafael Reif launched a review of the elite school's handling of the case.

Swartz's possible desire to make the articles public did not exempt him from prosecution, said Kerr, who represented the woman accused of hacking for using a fake MySpace profile.

"There's no 'good guy' exception to the criminal laws."

The outcry in the wake of Swartz's suicide may provide a rare opportunity for lawmakers to revisit the hacking statute, which has been repeatedly expanded over the past two decades.

"Usually, Congress wants to expand these laws," Kerr said. "This may be an unusual time when the public reaction is that the law gives government too much power."

Source URL (retrieved on *03/11/2014 - 10:55pm*):
http://www.wirelessdesignmag.com/news/2013/01/anti-hacking-law-questioned-after-death-internet-activist?qt-digital_editions=0