The Boston Globe Metro

Swartz case prompts debate over cyber law

By Peter Schworm and Shelley Murphy | GLOBE STAFF JANUARY 25, 2013


The family of free-information activist Aaron Swartz (right) and lawyers have blamed the office of US Attorney Carmen Ortiz for contributing to Swartz's death and said his offenses did not warrant jail time. Ortiz said the case was "reasonably and appropriately handled."

The suicide of Aaron Swartz, the Internet pioneer and free-information activist, touched off accusations that federal prosecutors abused their power by seeking a long sentence and stiff fine against him for hacking into the MIT network. But the case may say as much about problems with federal cybercrime law as it does prosecutorial judgment, say those familiar with the law.

The cybercrime statutes are broad — critics would say disproportionately so — subjecting even minor offenders to heavy criminal penalties, say specialists. That fact, coupled with sentencing guidelines that encourage prosecutors to take advantage of the tough sanctions, can give rise to overreaching prosecutions, they say.

“If there’s a statute that allows for 13 felonies and decades in prison to flow from what he was accused of doing, there’s a problem with the statute,” said Zoe Lofgren, a California congresswoman who is seeking to amend the law. “Aaron’s activity was not for personal gain, which is a very different situation from other crimes.”

Boston lawyer Martin Weinberg, who was one of Swartz’s lawyers, said the sentencing guidelines federal courts rely on are “Draconian and dehumanizing” because in white-collar cases, including computer fraud, sentences hinge largely on the amount of financial loss.

CONTINUE READING BELOW ▼

Related

Timeline: Swartz’s life, legacy

“The starting place for a federal sentence for a corrupt hedge fund manager, a Ponzi schemer, a corrupt banker who betrays his oath, and somebody that entered a computer without authorization is all the same,” Weinberg said. “And it’s all driven by the potential loss to the person who owns the data or the person who owns the money.”

Weinberg said the government alleged that JSTOR, which provides access to its online archive system to the Massachusetts Institute of Technology and other users for a subscription fee, estimated its potential loss would have been millions of dollars if Swartz had posted the articles on the Internet.

While critics say prosecutors have used the expansive law to cast a wide net, subjecting minor offenders to disproportionate punishment, other legal specialists note that prosecutors in the Swartz case have stayed well within the legal sanctions provided by the law. While prosecutors have the discretion to recommend lesser sanctions, they typically rely on strict sentencing guidelines, many specialists say.

In the Swartz case, that financial calculation led to a sentencing guideline range of about five to seven years, even though he had no criminal record and did not profit from the downloaded documents.

“That’s the institutional problem,” said Marc Zwillinger, a former federal cybercrime prosecutor who founded a law firm that works with companies on computer crime issues. “Everything in the sentencing process is guideline-driven, which warps the perspective of all the participants. The focus is on how the sentence compares to the

guidelines, instead of what is the right outcome for this individual."

As a result, many defendants are pressured to strike a deal with prosecutors and plead guilty to avoid the prospect of lengthy prison sentences, legal specialists say.

Such specialists, including former federal prosecutors, say the Swartz case is highly unusual and has no obvious precedents. Most people who steal data, they say, do so in hope of financial profit, which prosecutors acknowledge was not Swartz's motive.

Prosecutors alleged that Swartz, while a fellow at Harvard University's Safra Center for Ethics, downloaded millions of documents from JSTOR between September 2010 and January 2011, using different computers and IP addresses as MIT Police, Cambridge police, and Secret Service agents were trying to block his access and identify him.

They alleged he broke into a basement closet at MIT, using a bicycle helmet to obscure his face, and hard-wired his laptop to the network to download more articles.

Swartz was initially arrested on state charges in January 2011, then US Attorney - Carmen Ortiz's office indicted him six months later on charges of wire fraud, computer fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a protected computer. In September 2012, federal prosecutors increased the number of counts against Swartz from four to 13. Ortiz's office would not comment on why.

The charges against Swartz carried a maximum sentence of 35 years in prison, but in plea negotiations, prosecutors said they would recommend a six-month jail sentence if Swartz pleaded guilty to all 13 felony charges, according to Elliot Peters, the lawyer who took over Swartz's case in the fall. The judge would ultimately decide whether to accept it. But Swartz, who had battled depression, rejected the deal and was awaiting trial when he hung himself in his Brooklyn apartment Jan. 11.

His family and lawyers have blamed the prosecution for contributing to Swartz's death and said his offenses did not warrant jail time.

Last week, Ortiz defended her office's handling of the case, saying her review had determined it was "reasonably and appropriately handled."

Some lawyers agreed that Swartz's alleged actions were clearly criminal violations and that prosecutors were justified in pursuing the case.

“This one fell squarely in the statute,” said Michael Sussmann, a Washington, D.C., lawyer who specializes in Internet-related crimes and former cybercrime prosecutor at the Department of Justice. “This is what the statute was written for. People who have data in computers want them to be confidential.”

But Ted Claypoole, an intellectual property lawyer in North Carolina, said that while the charges were legitimate, the prosecution’s insistence on a prison sentence for downloading scholarly articles was highly unusual.

“I don’t know anyone who has served time for releasing academic journals into the wild,” he said.

Claypoole and other lawyers said that Swartz’s reputation as an activist, particularly his previous downloading of millions of pages of court documents during a brief period in 2008 when they were available free of charge at public libraries, may have spurred prosecutors to take a hard-line stance.

“This is a guy who said, ‘I’m going to do this on a massive scale,’ ” he said. “His approach was a direct challenge to law enforcement, and they went after him in a big way.”

Others saw the prosecution as a clear lapse of discretion.

“The premise for a prosecution shouldn’t be, ‘If you can indict, you should,’ ” said Nancy Gertner, a former federal judge in Boston who retired in 2011. “You should look at whether the penalties are proportional to the charge.”

In announcing Swartz’s indictment in 2011, Ortiz said that “stealing is stealing, whether you use a computer command or a crowbar.”

Gertner pointed to the remarks as evidence of Ortiz’s failure to weigh the individual circumstances of cases.

“There’s no sense of proportion,” she said. “There’s no sense of when you use the extra-ordinary powers of the office and when you don’t.”

There have been at least a couple of cases before Ortiz took over the office in which plea deals were negotiated that allowed defendants accused of illegally using computers to plead guilty to a misdemeanor and receive probation. In one of those cases, the defendant agreed to cooperate with the government.

“While we will not comment on individual cases, it is important to understand that there are a variety of factors that go into both charging decisions and sentencing recommendations in every case,” said Christina DiIorio Sterling, a spokeswoman for Ortiz. “Every case is different, and we try to take into account the variety of circumstances of each case in making decisions.”

The US attorney’s office in Boston created its cybercrimes unit in 2005, and it remains one of a handful of such units in the country.

Three of the four lawyers have at least a decade of specialized training and experience in the investigation and prosecution of cybercrime, the office said.

Over the past four years, the unit has prosecuted 47 cases, including 16 last year.

Peter Schworm can be reached at schworm@globe.com. Follow him on Twitter @globepete.