The Truth about Aaron Swartz's "Crime" « Unhandled Exception

Wednesday, April 10 2013, 4:03 PM

The Truth about Aaron Swartz's "Crime"

January 12, 2013
By Alex Stamos
in Cybercrime, Rights and Legality, Security
Tags: Aaron Swartz, Cybersecurity, Law
649 Comments

I did not know Aaron Swartz, unless you count having copies of a person's digital life on your forensics server as knowing him. I did once meet his fa intelligent and dedicated man who was clearly pouring his life into defend son. My deepest condolences go out to him and the rest of Aaron's family what must be the hardest time of their lives.

If the good that men do is oft interred with their bones, so be it, but in the meantime I feel a responsibility to correct some of the erroneous informat being posted as comments to otherwise informative discussions at Reddit, News and Boing Boing. Apparently some people feel the need to self-aggra opining on the guilt of the recently departed, and I wanted to take this cha speak on behalf of a man who can no longer defend himself. I had hoped Aaron to discuss these issues on the Defcon stage once he was acquitted, b that he has passed it is important that his memory not be besmirched by t ignorant and uninformed. I have confirmed with Aaron's attorneys that I to discuss these issues now that the criminal case is moot.

I was the expert witness on Aaron's side of US vs Swartz, engaged by his a last year to help prepare a defense for his April trial. Until Keker Van Nest iSEC Partners I had very little knowledge of Aaron's plight, and although spoken at or attended many of the same events we had never once met.

Should you doubt my neutrality, let me establish my bona fides. I have le investigation of dozens of computer crimes, from Latvian hackers blackm stock brokerage to Chinese government-backed attacks against dozens of American enterprises. I have investigated small insider violations of corpo policy to the theft of hundreds of thousands of dollars, and have responde break-ins at social networks, e-tailers and large banks. While we are no st pro bono work, having served as experts on EFF vs Sony BMG and Sony v our reports have also been used in the prosecution of at least a half dozen attackers. In short, I am no long-haired-hippy-anarchist who believes tha anything goes on the Internet. I am much closer to the stereotypical capit white-hat sellout that the antisec people like to rant about (and steal mail from) in the weeks before BlackHat.

I know a criminal hack when I see it, and Aaron's downloading of journa from an unlocked closet is not an offense worth 35 years in jail.

The facts:

- MIT operates an extraordinarily open network. Very few campus netwo you a routable public IP address via unauthenticated DHCP and then la basic controls to prevent abuse. Very few captured portals on wired net allow registration by any visitor, nor can they be easily bypassed by just assigning yourself an IP address. In fact, in my 12 years of professional work I have never seen a network this open.
- In the spirit of the MIT ethos, the Institute runs this open, unmonitore unrestricted network on purpose. Their head of network security admitt much in an interview Aaron's attorneys and I conducted in December. aware of the controls they could put in place to prevent what they consi abuse, such as downloading too many PDFs from one website or utilizi much bandwidth, but they choose not to.
- MIT also chooses not to prompt users of their wireless network with ter use or a definition of abusive practices.
- At the time of Aaron's actions, the JSTOR website allowed an unlimited of downloads by anybody on MIT's 18.x Class-A network. The JSTOR application lacked even the most basic controls to prevent what they mi consider abusive behavior, such as CAPTCHAs triggered on multiple do requiring accounts for bulk downloads, or even the ability to pop a box

warn a repeat downloader.

- Aaron did not "hack" the JSTOR website for all reasonable definitions o Aaron wrote a handful of basic python scripts that first discovered the U journal articles and then used curl to request them. Aaron did not use pa tampering, break a CAPTCHA, or do anything more complicated than c basic command line tool that downloads a file in the same manner as ri clicking and choosing "Save As" from your favorite browser.
- Aaron did nothing to cover his tracks or hide his activity, as evidenced b very verbose .bash_history, his uncleared browser history and lack of ar encryption of the laptop he used to download these files. Changing one's address (which the government inaccurately identified as equivalent to VIN number) or putting a mailinator email address into a captured por not crimes. If they were, you could arrest half of the people who have e airport wifi.
- The government provided no evidence that these downloads caused a ne effect on JSTOR or MIT, except due to silly overreactions such as turnir of MIT's JSTOR access due to downloads from a pretty easily identified agent.
- I cannot speak as to the criminal implications of accessing an unlocked an open campus, one which was also used to store personal effects by a homeless man. I would note that trespassing charges were dropped aga Aaron and were not part of the Federal case.

In short, Aaron Swartz was not the super hacker breathlessly described in Government's indictment and forensic reports, and his actions did not pos danger to JSTOR, MIT or the public. He was an intelligent young man wh a loophole that would allow him to download a lot of documents quickly. loophole was created intentionally by MIT and JSTOR, and was codified contractually in the piles of paperwork turned over during discovery.

If I had taken the stand as planned and had been asked by the prosecutor Aaron's actions were "wrong", I would probably have replied that what Aa would better be described as "inconsiderate". In the same way it is inconsi write a check at the supermarket while a dozen people queue up behind yo check out every book at the library needed for a History 101 paper. It is inconsiderate to download lots of files on shared wifi or to spider Wikipedia quickly, but none of these actions should lead to a young person being hou years and haunted by the possibility of a 35 year sentence.

Professor Lessig will always write more eloquently than I can on prosecutorial discretion and responsibility, but I certainly agree that Aaron demands a great deal of soul searching by the US Attorney who decided to

massively overcharge this young man and the MIT administrators who d involve Federal law enforcement.

I cannot speak as to all of the problems that contributed to Aaron's death, strongly believe that he did not deserve the treatment he received while he alive. It is incumbent on all of us to figure out how to create some positive out of this unnecessary tragedy. I'll write more on that later. First I need t some time hugging my kids.

Edit 1: Fixed typo. Thank you @ramenlabs.

Posted from San Carlos, CA.

« *Answering Questions about .Secure*

649 Responses

Delores Quade says:

January 12, 2013 at 12:58 pm

; (

Quixote (@Quixote34) says:

January 13, 2013 at 12:06 pm

The arrogant government prosecutors who, in effect, murdered Aaron, as well as the irresponsible academics who shrugged their shoulders in indifference and the various media outlets that casu