Sven Wiberg

Comp 401

3/17/15

**The overreach and abuse of the CFAA**

#### When dealing with computer security having laws passed to provide protections against unwanted tampering and use of computers is a no brainer. There need to be regulations in place to provide sufficient penalties to deter anyone from distributing malicious code or stealing information from computers. The Computer Fraud and Abuse Act was written as an attempt to curtail these sorts of offensives by making it a federal crime to access a computer without authorization or in a way that exceeds authorization. However exactly how computer authorization is defined is not brought up in the bill. By not defining exactly what authorized access is law makers have effectively left the definition of this term up to the courts discretion which has led to heavy handed prosecutorial bullying and sentencing which in no way reflects the severity of the crimes committed. A law which protects people against the abuse and misuse of computers is a necessity in today’s day and age, however such a law should be nuanced and bring into account the vagaries of how we treat access to our computers, the CFAA is not such a law, it has been demonstrated time and time again in multitudes of cases, including finding and notifying users of holes in a devices security of which the company was aware, such as in the case of Andrew Aurenheimer, and attempting to distribute files that were on an open network, such as in the case of Aaron Swartz, even in violating the terms of service of a product that was bought and paid for, as in the case of George Hotz. We must either update the CFAA to acknowledge that not all computer crimes are of equal severity and that the term authorized access is too black and white a term or write a new law to replace it.

The Computer Fraud and Abuse act was written into law in 1986 as an amendment to the existing computer fraud law. The law was supposed to limited to cases that. The act was intended to extend the protections of the original law and to add the criminalization of other computer related acts such as distribution of code for computer viruses and passwords as well as denial of service attacks. The main point of the law is the part protecting against the unauthorized access of a computer, either accessing a computer completely without authorization or accessing a computer in a way that exceeds authorization. The problem with the law arises in that the term authorization is completely undefined, which allows for any act that might meet those criteria to be prosecuted federally. One of the reasons that the CFAA is so ill defined is that it was written before computers were as wide spread as they are today, in fact computer use was so relatively new at the time that the report that lawmakers were given to inform them before voting on the law “specifically referred to testimony describing War Games as a ‘realistic representation of the automatic dialing and access capabilities of the personal computer,’ and thus, apparently, of the threat to computer security presented by those capabilities”(Kapitanyan p.6) This lack of familiarity with computers led to legislators passing a bill which left enormous holes which allow for the abuses of the law which we see today. The CFAA’s overreach has only become more obvious as computers have become much more widespread and complex, as it has been brought out more and more as a tool to inappropriately and inordinately punish those who violate this law by a system which hasn’t caught up to the current era of technology.

During June of 2010 a group of hackers, Goatse Security, which included Andrew ‘weev’ Auernheimer, breached AT&T’s security by finding a vulnerability when the AT&T servers connected to a user’s iPad which would allow them to gain access to the E-mail addresses of AT&T’s iPad users. After uncovering this flaw the group took advantage of it and proceeded to uncover the data of roughly 114,000 iPad users. After the group went public with its findings the FBI proceeded to investigate them and arrest Auernheimer on a multitude of charges, including violating the CFAA. This came as a surprise to Auernheimer who said that “We were just trying to be good guys” and that the method they used to release the information “was the only way to get public notification” (Computer Experts Face Backlash, wsj.com). On March 18, 2013 Auernheimer was found guilty of identity fraud and violating the CFAA and sentenced to 40 months in a federal penitentiary and ordered to pay $74,000 in restitution.

Through 2010 and the beginning of 2011 Aaron Swartz downloaded around 4.8 million articles from the academic database JSTOR. He accomplished this using MIT’s ‘open campus’ which allowed visitors to the college to access JSTOR through their network. During the period in which Swartz was downloading these articles from JSTOR there were several attempts to stop his use of the network, including banning his computer’s MAC address, he managed to circumvent these measures though. MIT even had the chance to permanently shut down Swartz’s downloading and yet they did nothing “MIT, for example, knew for 2½ months which campus building the downloader had operated out of before anyone searched it for him or his laptop — even as the university told JSTOR they had no way to identify the interloper” (Aaron Swartz and MIT: The Inside Story, bostonglobe.com). Even though MIT allowed anyone on their campus to freely access this network and put almost no effort into catching and stopping Swartz, in January 2011 Swartz was arrested. After the data had been in effect returned, JSTOR was willing to not press charges, however in September of 2012 Swartz was charged with nine felonies relating to breaking the CFAA and faced 50 years in prison and one million dollars in fines. Sadly, in the face of such severe and unwarranted jail time, on January 11, 2015 Aaron Swartz took his own life.

In January of 2011 George ‘geohot’ Hotz, publically released an exploit for the Sony PS3 which allowed owners of the system to access the read/write functions of the systems memory and hypervisor level access to the PS3’s CPU, this would effectively allow users to run a virtual machine on their PS3 allowing them to use another OS. This access could be gained through the use of the PS3’s root keys which Hotz also posted on his website. This led to Sony suing him, claiming that he had violated multiple laws including the CFAA as he had violated the terms of the PlayStation Network user agreement. Sony then requested access to all the IP addresses that had visited Hotz’s site while the information had been posted there, which the court granted them. On April 11, 2011 it was revealed that the case had been settled out of court with a gag order being placed on Hotz, meaning that he could never again work on hacking any of Sony’s products.

Within just these three cases The CFAA has been used to punish people that found a exploit in a popular piece of hardware, attempted to download data off of an open network, and hacked a product that they owned to add functionality. While all of these cases certainly fall into a gray area in terms of access the CFAA makes no distinction between purely malicious activities and attempts to improve software and technology or distribute data that is hidden behind a high paywall to those who couldn’t afford it. In most of these cases severe sentences were given to or threatened against the defendants in order to seem harsh on computer crime, however all this does is stifle creativity and ingenuity as if the law is so vague that people of prison time or exorbitant fines if they attempt to innovate using existing hardware or software then there will be a large slowdown in terms of new breakthroughs in hardware and software. There is hope though, an amendment has been proposed to the CFAA, called Aaron’s law in honor of Aaron Swartz, which would remove terms of service violations from being prosecutable through the CFAA. While is hasn’t passed yet, this would be an important first step in reforming the CFAA.

Bibliography

Worthen, Ben, and Spencer E. Ante. "Computer Experts Face Backlash." *Http://www.wsj.com*. The Wall Street Journal, 14 June 2010. Web. 17 Mar. 2015.

Bombardieri, Marcella. "The inside Story of MIT and Aaron Swartz." *BostonGlobe.com*. The Boston Globe, 30 Mar. 2014. Web. 10 Mar. 2015.

McSherry, Corynne. "Sony v. Hotz Ends With a Whimper, I Mean a Gag Order." *Eff.org*. Eff.org, 12 Apr. 2011. Web. 20 Mar. 2015.

Kapitanyan, Matthew. "Beyond WarGames : How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context." *I/S: A Journal of Law and Policy For the Information Society* 7.1 (2011): 1-50. *Http://moritzlaw.osu.edu*. Web. 3 Mar. 2015. <http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Kapitanyan.FE\_.Final\_.Weber\_.pdf>.