21st Century Cyber News: Law Enforcement v. Hackers

LIS461: Data and Algorithms: Ethics and Policy

Shia Aaron Lloyd Fisher

University of Wisconsin, Madison

2 August 2023

Shia Aaron Lloyd Fisher

Paul J. Kelly, Tallal Ahmad, Yinka Ajiobola

Data and Algorithms: Ethics and Policy – SADIE 2

2 August 2023

Law v. Hackers

Law enforcement and law makers have the challenge of continuously learning about new systems and protocols that may have the capability to circumvent the law. Considering the ethics of hacking we often think of Julian Assange or Edward Snowden, two incredibly famous men who both used their knowledge of computer technology to expose practices embarrassing to the United States government. This act is known as whistleblowing and is notably one moral rational for (and we will use the term loosely) "hackers" to execute their plans. Another rationale for hacking, as we will see later, may be more individualistic than this sense of ethical or moral requirement to share potentially troubling information, and that is hubris. Hubris is a sense of pride from defiance against an authority, it is the antithesis of paternalism.

Jullian Assange, publisher and founder of WikiLeaks developed a way for sensitive information to make its way to public view under the guise of freedom of speech. For many years, Assange continued his perpetual state of asylum in various Embassies in various countries, escaping several extradition attempts for other alleged crimes / misdemeanors both in Europe and the United States. He is currently confined in a London prison, (Rebaza & Fox). Edward

Snowden is also well-known for sharing secret information about the United States NSA program's massive surveillance of its citizens. In these cases, as well as other cases of hacking, we can say, hackers have the pattern of exposing information, or exposing vulnerabilities within a system either altruistically or for hubris.

In January of 2023, James Zhong pleaded guilty to wire fraud and was sentenced in April to spend one year in prison. Zhong carried out his crimes by utilizing a particular exploitation within the way transactions occurred on the 'dark web' site known as Silk Road. Zhong's hacking is different than both Assange and Snowden, in that Zhong does not seem to have an altruistic motivation. Before we discuss Zhong's intent or moral reasons let us first expand on a few concepts.

The Deep Web goes beyond the surface layer of the Internet. Typically, webpages contain information readable by a browser to display specific content for the user. Beyond the code that displays a page is a *deep web*, that is software and data accessible to website administrators that contains all the information a particular website may need to access. It is the raw files for a particular website. The Dark Web rests on the edges of the deep web and it operates using a special '.onion' top level domain (Finklea, p. 2-3). It requires the use of special software known as Tor browsers to navigate. Most users, especially those who have nefarious intentions, will use additional protocols such as VPN proxy services to hide their actions online. Use of a Tor browsers is not unlawful in the United States at the timing of this SADIE; however, the use of a Tor browser is likely to cause internet service providers to become suspicious.

Alleged Silk Road founder Ross Ulbricht was arrested by US Federal authorities in 2013 and was subsequently sentenced to life in prison. The US alleges Ulbricht designed the site to operate much like eBay with the exception that transactions were untraceable or anonymous.

This gives way for a tremendous number of illicit activities (US v. Ulbricht). The original Silk Road was taken down, but when Silk Road reemerged in 2014 (known as Silk Road 2) a vulnerability in the new "escrow service," was created, an algorithmic protocol that James Zhong found to be exploitable.

The escrow protocol works as Silk Road performs its online service on the dark web. Similar to an auction website in which users can contact sellers and buy goods with the hopes the seller will actually ship said goods. Sellers receive Bitcoin through a third-party service to Silk Road, making it that much harder to track or regulate. Plus, it requires special knowledge of computers and data systems to use the dark web or exchange Bitcoin. This obscurity makes the platform ripe for criminal activity.

Bitcoin does not by itself impute an illegal inference, it is simply a way of converting and transferring real financial property, very securely and discretely through a "blockchain" protocol. As a technology, Blockchain has the potential to become the future of online transactions. The "escrow service," was a way for buyers to regain their Bitcoin in the event of seller mishap. For instance, a buyer buys something, the Bitcoin is transferred to a third-party holding account, (the escrow), if the transaction is reconciled, meaning the buyer has no complaints, the funds are then released to the seller. If there are mishaps, the funds are returned to the buyer.

This provided a means for Zhong to illegally acquire over 50,000 Bitcoin for a total monetary value (at the time of attack) of 3.4 billion dollars. By the time Zhong was sentenced, in spite of the massive drop in value of Bitcoin, Zhong's take was worth well over 1.5-billion-dollars (Justice.gov). Along with Zhong's guilty plea, was a return of a sizable portion of the stolen funds, and statements about his "dysfunctional family" and other traumatic childhood experiences. These are all ways his defense argued for a lesser sentence.

In Zhong's confession authorities learned how Zhong was able to illegally acquire the massive funds. By creating multiple fraudulent accounts, each funded with 200-2,000 Bitcoin. Zhong was able to use latency (delay within the online system clock) to artificially transact against his own fraudulent accounts. Pretending to buy something, manipulating the system's time, he was able to withdraw his escrow multiple times and acquire over 50,000 in Bitcoin. In one instance he was able to, in quick succession, withdraw five-hundred Bitcoin five times having only deposited five-hundred Bitcoin to start for a net gain of 2,000 Bitcoin or 400% increase.

This crime and precedence have major implications for the future of cyber security and cybercrimes. The first intriguing aspect is this idea that law enforcement is also, by some interpretation, protecting criminals by charging and convicting a person who was stealing from a professedly criminal platform. This protects the Principle of Humanity by treating all humans equally, in this context, even potential suspects of crime. By prosecuting an individual accused of various wire fraud attacks on users of the Silk Road, the United States government is potentially protecting the real financial property of criminals. It has the appearance of applying the law to anyone who offends it regardless of who the victim is.

The second ethical consideration is related to the moral decision making of Zhong. Does his confession obfuscate or mitigate his moral intention? What was his intention to begin? He did purposefully commit the crime, while he may not have been aware of the exact consequences, he was aware he was doing wrong as stipulated in his confession. Is the repatriation of funds ethical if it belongs to a criminal enterprise? Afterall, not all funds were returned. In 2019, Zhong reported that a briefcase holding over $400,000 that he converted into cash had been stolen from his residence.

Law enforcement is wise to continue its mission of fighting crime wherever it exists within the pertaining jurisdiction. This year alone, numerous cyber incidents have been tracked and cataloged for public release. Where there are privacy concerns, financial considerations, misuse of a system, rules of conduct help to define concerns. Cases like James Zhong, Edward Snowden, Jullian Assange, or Mark Abene are all both popular and significant for the precedence setting reactions of both the law side as well as the defense. To promote a stable 21st century cyber society, a consistent approach to investigation and prosecution should be adhered to in the strictest sense.

Law enforcement has the duty of investigation and prosecution, but it is up to the legislative bodies to create the framework for their work. Law makers should modernize and clearly state US Codes in terms of their specific offensive by name and practice so as not to confuse or conflate other cybercrime cases' conduct with one another. There is a significant difference between stealing Bitcoin from potential criminals and stealing health records, or (to be more comparable) other financial assets from traditional securities. It is conceivable that Zhong's sentence would not be below-guidance if his crime were carried out in a traditional bank for instance. It is clear from Zhong's medical history that his intention was not altruism, and that instead he suffers from mental health issues. Having this view could inform future cases so that sentence guidance is more uniform therefore making a more consistent, ethical approach to enforcing cyber laws.

References

Arntz, P. (2022, November 9). *Silk road mega thief James Zhong pleads guilty*. Malwarebytes. https://www.malwarebytes.com/blog/news/2022/11/silk-road-mega-thief-james-zhong-pleads-guilty

Finklea, K. M. (2015). *Dark web*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R44101

Hon. Paul G. Gardephe United States District Judge. (2022, November 4). *United States v. Zhong*. Legal research tools from Casetext. https://casetext.com/case/united-states-v-zhong-7

Kujawa, A. (2014, February 14). *Bitcoin theft in the underground: Malwarebytes labs*. Malwarebytes. https://www.malwarebytes.com/blog/news/2014/02/bitcoin-theft-in-the-underground

Rebaza, Claudia; Fox, Kara (4 January 2021). "UK judge denies US request to extradite Julian Assange". CNN. https://www.cnn.com/2021/01/04/uk/julian-assange-extradition-wikileaks-us-gbr-intl/index.html

Significant cyber incidents: Strategic technologies program. CSIS. (n.d.). https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Silk road dark web fraud defendant sentenced following seizure and forfeiture of over $3.4 billion in cryptocurrency. Southern District of New York | Silk Road Dark Web Fraud Defendant Sentenced Following Seizure And Forfeiture Of Over $3.4 Billion In Cryptocurrency | United States Department of Justice. (2023, April 14). https://www.justice.gov/usao-sdny/pr/silk-road-dark-web-fraud-defendant-sentenced-following-seizure-and-forfeiture-over-34

US v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014).

Voreacos, D., & Bloomberg. (2023, April 14). *Theft of bitcoin that topped $3 billion in value leads to one-year prison sentence for James Zhong: "I always knew what I did was wrong."* Fortune. https://fortune.com/2023/04/14/bitcoin-thief-james-zhong-sentenced-to-prison/