12-2018

Identity Theft: Is the U.S. Really Safe in the Police's Hands?

Hoang Vo

Identity Theft: Is the US Really Safe in the Police's Hands?

Hoang Vo

FYS 100-24: From Facebook to FaceTime: Living and Learning in the Digital Age

Professor Elizabeth Lewis

Dickinson College

Hoang Vo

FYS 100-24 (Professor Elizabeth Lewis)

Date: 12/07/2018

Final Research Paper

Identity Theft: Is the US Really Safe in the Police's Hands?

Introduction

The ever-growing popularity of the Internet in recent years has been conducive to the development of cybercrimes. Not only have new types of cybercrimes emerged, but traditional crimes, including identity theft, have also become more complex with the assistance of new technologies. The US, as a financial and technical powerhouse, has been a primary target of this new form of identity theft. According to Javelin Strategy and Research (2018), in 2017 alone, 16.7 million people in the US were victims of identity theft, with an aggravated loss of more than $16.8 billion.

To counter the growing threat of identity theft, the US law enforcers have a key role in investigating and prosecuting identity theft cases. However, the efficiency of their efforts has been questionable. This research argues that the ineffective prosecution and investigation from US law agencies fail to prevent identity theft. Specifically, the following paper identifies the persistent weaknesses in legal enforcement and technical difficulties in the investigation process as central factors undermining these prevention efforts.

Definition

According to the United States Department of Justice (2017), identity theft is "all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain" (n.p.). Identity thieves can then falsely apply for loans and credit cards, make unauthorized bank withdrawals or obtain other goods or privileges under victims' names (United States Department of Justice, n.d.). In more serious cases, identity theft may entail organized crimes such as money laundering, drug trafficking, tax evasion or terrorism (Clough, 2015).

Traditional identity theft involves physical means to obtain personal information. The thieves may "dumpster dive," which is to dive trash bins for throwaway documents containing sensitive information, or surreptitiously listening to victims' phone conversations with banks and authorities. Technology, however, has eliminated the need for physical theft. Using spam emails and texts, phishing websites, and malwares, thieves can target a wide range of users and take away from each of them a small amount of money (Button, Nicholls, Kerr & Owen, 2012). These gains when combined, however, can reflect a substantial loss for the economy as described above. This fact, therefore, reflects the importance of identity theft as an all-encompassing, ultimate goal of all cyber misconducts.

Ineffective Legal Enforcements Against The Prevalence of Identity Theft

The United States has one of the most developed cybersecurity laws in the world. Effective laws are enforced across local, state, and federal administrations to protect citizens and organizations from online criminal activities. Despite such a seemingly established legal system, there are several shortcomings that limit the power of these regulations against identity theft, which will be discussed below.

Differences in state law enforcement

The strictness of legal requirements following data breaches, a highly dangerous source of identity theft, varies state by state. In California, entities (e.g. organizations affected by data breaches) must provide free identify theft prevention and mitigation services for at least 12 months "if a breach includes Social Security numbers, driver's license numbers, or state identification card numbers" ("California Civil Code," 2017). Additionally, if medical information is exposed, entities are liable to a penalty of $25,000 per patient whose data was leaked ("California Civil Code," 2017). Mississippi, in contrast, does not specify how firms must recover the damage to customers ("2017 Mississippi Code," 2017). Such discrepancies in legal enforcement may cause legal pitfalls for interstate firms (Aguilar, 2014; Ready, 2018) as they are susceptible to non-compliant lawsuits. They also put residents in states with less strict cybersecurity laws at a disadvantage, as they are less likely to receive due compensations from organizations and law enforcement when their data is compromised.

Difficulties in establishing federal regulations

The federal government has made efforts to resolve differences among states' cybersecurity laws. However, proposed regulations have existed as frameworks for voluntary actions from organizations to improve cybersecurity, rather than affirmative legal requirements. Therefore, it is argued that the flexibility of these regulations fails to offer enough incentive for organizations to implement them, due to their lack of binding power and specificness. The failure to adopt appropriate protection measures ultimately leaves firms and organizations in perpetual vulnerability against cyberattacks.

An example of such frameworks is the Cybersecurity Enhancement Act of 2014. The Act directed the National Institute of Standards and Technology to develop a voluntary cybersecurity framework for organizations to manage their data breach risks (Fleming, Richmond, Farber, Singh, & Nuzum, 2018). However, several challenges remain. First, Fleming et al. have argued that organizations prioritize physical security, natural disaster response and insider threats over cybersecurity. This finding infers that voluntary participation will only allow firms to further deprioritize or deliberately neglect cybersecurity investment. In addition, the framework lacks a clear measure of success and guidelines for its implementation (Fleming et al., 2018; Dourado & O'Sullivan, 2015). This statement signifies the framework's failure to consider the nuances of cybersecurity issues across millions of organizations. As organizations' sizes and resources vary greatly, there cannot be a one-size-fits-all approach to cybersecurity for all of them. Finally, local laws and industry or other requirements inhibit framework adoption, as they may present conflicting obligations with the proposed framework (Fleming et al, 2018). Such a patchwork level of law enforcement further hinders organizations to adopt new regulations over the concern of violating existing ones.

The Effects of Technical Shortcomings to Identity Theft Protection and Investigation

The General Lack of Technical Expertise Among Police Officers

Jurisdictions' lack of capability against identity theft represents limited technical training for investigators. While only a small minority of police officers have knowledge about basic cyber prosecution, investment in cybersecurity training for law enforcing personnel has not been a priority of local administrations (Shelby, 2017). This is evident in a Ponemon Institute report (2015), which found that most state cyber budgets constitute less than two percent of their overall IT budget, compared with 10% on average in large companies. The indifference towards technical training reflects law agencies' assumption that Internet crime incidences will not proceed beyond reporting, as investigation costs may far outweigh the losses (Shelby, 2017; Loker, 2018). This argument is flawed, as it neglects the increasing manipulation of the Internet as a tool for identity theft and other criminal conducts. There exists a possibility that the majority of crimes in the future will be Internet-based. Consequently, a failure to develop the required capabilities to handle cyber investigation will render law enforcers powerless against most criminal activities.

The Anonymous and Transnational Nature of Identity Theft Attacks

Investigators' ability to examine identity theft is also limited by the anonymous and transnational nature of identity theft attacks. According to Greenemeier (2011), hackers use malwares to take over control of other computers to launch their attacks. This technique allows hackers to maintain their anonymity, which can be particularly difficult for investigators to detect the correct origins of the attacks. In addition, these computers may be located in several countries (Greenemeier, 2011; Grimes, 2016). This implies that in order to launch an investigation, the United States may be required to collaborate with other countries for the exchange of evidence, which is considered too complicated due to budget limitations and differences in legislations.

Technical Infrastructure Limitations

Limitations in technical infrastructure also aggravate the difficulties in investigating identity theft. According to Chouhan (2014), evidence of attacks might contain documents, pictures, videos and audio files that take up a significant amount of storage space. Obtaining the required space calls for substantial investment from law enforcement agencies, which further discourages them from conducting proper investigations.

In addition to the requirement of large storage space, investigators may face obstacles in gathering log files. Log files are records generated by the digital devices that document system activities (Zhang, 2018). According to Vatis (2002), log analysis is the key to detect anomalies in network traffic of devices and signal signs of a system intrusion aimed at identity theft. Such an analysis requires the ability to perform log analysis across multiple platforms and sources (Vatis, 2002; Grimes, 2016). This requirement can be challenging for police departments with limited cybersecurity infrastructure, as they may lack the qualified personnel and infrastructure to analyze the data*.* These difficulties again highlight the issue of cybersecurity investment, which has not been addressed by legal authorities, especially at lower levels.

Discussion and Conclusions

Are the US law enforcement agencies effectively thwarting identity theft? Arguably, they do not. This paper has highlighted that the reasons for their losing battle against this crime are legal enforcement shortcomings and technical difficulties in the investigation process. It is clear that, with more valuable personal data available online and growing complexity of attacks, if measures are not taken, the US will be left more and more devastated while criminals remain free from any effective deterrence.

The findings of this paper suggest several possible improvements in identity theft prevention. Legally, it is suggested that governments and local authorities work together to resolve differences in cybersecurity laws with the aim of protecting customers' rights. The common set of legal instruments reached by these authorities may need to include certain obligations and detailed guidelines for organizations and citizens to implement. Technically, while it remains difficult to trace identity theft criminals, emerging technologies, including text mining and deep learning, allow enhanced detection of malicious websites (Yang, Manoharan & Barber, 2015; Vinayakurmar, Soman & Poornachandran, 2018). The government, therefore, may implement these technologies to blacklist deceptive sites. Most importantly, it is imperative that the government invests in the development of new preventive technologies, along with enhancing law enforcers' capacity to handle cybersecurity investigation effectively. The detailed implementation of these solutions is for other papers to address.

References

2017 Mississippi Code § 75-24-29. (2017). Retrieved from https://law.justia.com/codes /mississippi/2017/

Aguilar, L. (2014, June 10). Boards of directors, corporate governance and cyber-risks: Sharpening the focus. Retrieved from https://www.sec.gov/news/speech/2014-spch061014laa

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology*, 47(3), 391–408.

California Civil Code §§ 1798.29. (2017). Retrieved from http://leginfo.legislature.ca.gov/ faces/codes_displaySection.xhtml? lawCode=CIV§ionNum=1798.29.

California Civil Code §§ 1798.82. (2017). Retrieved from http://leginfo.legislature.ca.gov/ faces/codes_displaySection.xhtml? lawCode=CIV§ionNum=1798.82.

Chouhan, R. (2014). Cyber crimes: Evolution, detection and future challenges. *IUP Journal of Information Technology, 10*(1), 48–55. Retrieved from http://search.ebscohost.com/ login.aspx?direct=true&db=aci&AN=96588552&site=eds-live&scope=site

Clough, J. (2015). Towards a common identity? The harmonisation of identity theft laws. *Journal of Financial Crime, 22*(4), 492-512.

Dourado, E., & O'Sullivan, A. (2015, June 22). Poor federal cybersecurity reveals weakness of technocratic approach. Retrieved from https://www.mercatus.org/publication/ poor-federal-cybersecurity-reveals-weakness-technocratic-approach

Fleming, G. K., Richmond, T., Farber, M. D., Singh, D., & Nuzum, R. (2018, March 5). GAO reports challenges and successes in cybersecurity framework adoption. Retrieved from https://www.natlawreview.com/article/gao-reports-challenges-and-successes-cybersecurity-framework-adoption

Greenemeier, L. (2011, June 11). Seeking address: Why cyber attacks are so difficult to trace back to hackers. Retrieved from https://www.scientificamerican.com/article/ tracking-cyber-hackers/

Grimes, R. A. (2016, December 6). Why it's so hard to prosecute cyber criminals. Retrieved from https://www.csoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html

Javelin Strategy & Research. (2018, February 6). Identity fraud hits all time high with 16.7 million U.S. victims in 2017, according to new Javelin Strategy & Research study. Retrieved from https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin

Loker, M. (2018). Conveniently Exposed: How the Convenience of the Internet Is Exposing You to Identity Theft. *Journal of Internet Law*, *22*(2), 3–7.

Ponemon Institute. (2015). 2015 Cost of data breach study: Global analysis. Retrieved from https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of- Data-Breach-Study.PDF

Ready, F. (2018, October 19). The Case For, and Against, Federal Cybersecurity Standards. Retrieved from https://www.law.com/legaltechnews/2018/10/19/the-case-for-and-against-federal-cybersecurity-standards/

Selby N. (2017, April 21). Local police don't go after most cybercriminals. We need better training. Retrieved from https://www.washingtonpost.com/posteverything/wp/2017/04/21/local-police-dont-go-after-most-cybercriminals-we-need-better-training/

United States Department of Justice. (2017, February 7). Identity Theft. Retrieved from https:// www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Vatis, M. (2002). Can the U.S. investigate a cyber attack? Retrieved from http://www.crime-research.org/library/Vatis2.htm

Vinayakumar, R., Soman, K., & Poornachandran, P. (2018). Evaluating deep learning approaches to characterize and classify malicious URL's*. Journal of Intelligent & Fuzzy Systems, 34*(3), 1333-1343.

Yang, Y., Manoharan, M., & Barber, K. (2015). Modelling and analysis of identity threat behaviors through text mining of identity theft stories. Retrieved from https://identity.utexas.edu/assets/uploads/publications/Yang-2015-Modelling-and-Analysis-of-Identity-Threat-Behaviors-Through-Text-Mining.pdf

Zhang, E. (2018, September 12). What is log analysis? Use cases, best practices, and more. Retrieved from https://digitalguardian.com/blog/what-log-analysis-use-cases-best-practices-and-more