Spring 5-2020

A Comparative Analysis of Identity Theft within America and Australia

Vincent Alagna
University at Albany, State University of New York, valagna@albany.edu

A Comparative Analysis of Identity Theft within America and Australia

An honors thesis presented to the
Department of Criminal Justice,
University at Albany, State University of New York
in partial fulfillment of the requirements
for graduation with Honors in Criminal Justice
and
graduation from The Honors College

Vincent Alagna

Research Advisor: Alissa Worden, Ph.D.

May 2020

Abstract

Identity theft is a very prevalent crime within the United States that has substantial repercussions on society. This study analyzes factors that potentially contribute to America's elevated rate of identity theft in relation to Australia in order to reveal its cause. It was ultimately found that the United States experiences a greater amount of computer usage within its country, has the ability to implement a stricter prison sentence on those convicted of committing identity theft in accordance with its legal code, and has a greater conviction rate while Australia has a higher prosecution rate. These findings, when applied in the context of the Routine Activities Theory of crime and the notion of general deterrence, help to explain the reasons for the United States' greater identity theft rate.

Acknowledgments

I would like to begin by thanking Professor Alissa Worden for all of the help that you had provided while serving as my research advisor for this project. I would also like to thank my family for supporting me not only throughout this research process, but throughout my entire life. I would not be the person I am today without your love, support, and guidance. Lastly, I would like to extend a thank you to all of my friends that I have met at this university for making my time here memorable and something that I will cherish forever.

Table of Contents

Introduction

The introduction of computers has revolutionized modern society. While the benefits of such technological advancements are profound, they do not come without corresponding detriments. The growth of this electronic environment has provided criminals with a new interface to commit crime. Between the years 2015 and 2019, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center had averaged approximately 340,000 complaints regarding cybercrime each year. Since the inception of the complaint center in 2,000, there has been a total of over 4 million complaints, with that amount reaching its peak in 2019 with over 460,000 complaints and approximately $3.5 billion in victim losses ("2019 Internet Crime Report," 2020).

Cybercrime is a broad term used to describe (1) crimes designed to affect computers and/or other information systems, and (2) crimes committed in which computers or other technological systems are an integral part to the commission of the offense (Australian Federal Police, 2019). In other words, the term cybercrime is employed to categorize specific individual offenses, which may come in a variety of forms.

One of the most prominent types of cybercrime reported worldwide is identity theft, which is defined by the FBI as an act involving "a perpetrator stealing another person's personal identifying information, such as name or Social Security number, without permission to commit fraud" ("2019 Internet Crime Report," 2020). Despite its global presence, identity theft appears to have a varying impact between each country, as the rate of identity theft (a contributor to a country's overall rate of cybercrime) differs between nations. For example, in 2019, a total of 650,572 individuals became victims of identity theft within the United States (Federal Trade Commission, 2020). With a population size of 329,135,084 during this time, this equates to a rate

of 0.0020 (United States Census Bureau, n.d.). However, in Australia, only 11,373 complaints concerning identity theft were made to the country's Scamwatch, which is a website run by the Australian Competition and Consumer Commission (ACCC) that provides information and resources to consumers about scams and maintains statistics related to each type of scam (Jorna, Smith, & Norman, 2020). With a population size of 25.5 million, Australia's rate of identity theft is only 0.0004 (United States Census Bureau, n.d.). Thus, the purpose of this study is to identify and analyze potential factors for the discrepancies in the rate of identity theft between these two countries. Therefore, possible solutions may be proposed in order to address those factors and help to lower the United States' rate of identity theft and subsequently its rate of cybercrime as a whole.

Brief History of Identity Theft and its Schemes

Before the advent of the computer and Internet, identity thieves had to rely largely on printed information in order to steal their victim's identity. Various methods existed for these thieves to obtain said information necessary to facilitate identity theft. For example, dumpster diving involves a thief going through a potential victim's garbage with the goal of finding personal identifiable information (PII) off of items found within the garbage, such as bills and bank statements. Mail theft is similar in the fact that the objective is to obtain PII off of mailed documents, with the perpetrator stealing pertinent material from the victim's mailbox. Of course, identity theft also occurred through the ordinary theft of personal items. The theft of a wallet or purse would provide the thief with access to items such as a driver's license, credit and/or debit cards, and more, with all of these objects containing the PII required for the commission of identity theft (Center for Identity Management and Information Protection, 2015).

One method that didn't necessarily rely on printed information, however, is shoulder surfing. Shoulder surfing often occurred in a public setting and is similar to the concept of "eavesdropping". It involves an individual observing a potential victim from a nearby location as they provide their PII. Instances can include recording the victim's telephone calling card number, credit and debit card numbers, passwords, and PIN numbers as they present them over the telephone or another system (United States Department of Justice, 2017).

While the aforementioned methods have remained viable schemes, although they are by no means an exhaustive list of all of the techniques that were available pre-Internet, the arrival of the digital era has vastly expanded the ways in which an identity thief can acquire a victim's PII and perpetrate identity theft. This is because technology eliminates the requirement of a physical presence in order to obtain said PII. With the Internet, information can now be obtained remotely through various exploits and cyber-attacks. One of the most prevalent attack vectors is phishing. In a phishing scheme, the attacker impersonates an authentic or trusted entity, such as a bank or other financial institution, in an attempt to trick an unsuspecting victim into divulging their sensitive information. Although this scheme can come in an assortment of styles, it is often facilitated through spam emails that contain links directing users to a malicious website that appears as the genuine website for the entity being impersonated (Heller, 2008).

Another popular technological method of obtaining PII is skimming. Skimming targets credit and debit card information and involves an attacker placing a device called a skimmer over the mechanism that reads the card's information from its magnetic strip. The skimmer then records all of the card information for every card that gets passed through it. Because this method relies specifically on credit and debit cards, skimmers are frequently placed on ATM

machines or gas station pumps and retrieved by the attacker after a period of time (Center for Identity Management and Information Protection, 2015).

A third very significant method of obtaining PII for the purpose of committing identity theft through the Internet is hacking. The Internet has undoubtedly increased the convenience of daily life, offering a multitude of information and resources to users with just a few clicks of some buttons. However, it has also opened users and their personal information to possible exploitation by cyber criminals. Much of this can be attributed to the rise in e-commerce, with consumers entering their names, billing and shipping addresses, and payment information online in order to receive desired goods or services (Heller, 2008). Hacking enables technically-skilled criminals to obtain unauthorized access to this information provided over the Internet through the use of complex techniques designed to compromise a digital device, such as a computer, phone, or tablet. There are countless ways for an attacker to hack into a system, and with technology constantly evolving, so do the attack vectors (Malwarebytes, n.d.).

To illustrate how much of an impact technology has had on the growing instances of identity theft, at the turn of the 21st Century, 500,000 people had become victims of identity theft within America. Just four years later, the number of victims inflated to 10 million, an increase of 1900%. And by the year 2005, identity theft constituted 37% of all fraud complaints with the Federal Trade Commission's (FTC's) fraud database, the Consumer Sentinel, rendering it the largest category of fraud complaint on file (Heller, 2008). Today, identity theft still remains as the most reported category of fraud with the FTC, composing 20.3% of all complaints made (Federal Trade Commission, 2020).

Literature Review

Identity Theft Trends

United States

Many reports have been published tracking the trend of identity theft throughout the years within the United States. However, each report relies on a different data set. For example, the FBI's Internet Crime Complaint Center (IC3) refers to complaints submitted to its public website to determine the total number of identity theft occurrences within a given year. At the beginning of the decade, in 2010, nearly 30,000 of the 303,809 complaints (9.8%) submitted to the IC3 involved identity theft ("2010 Internet Crime Report," 2011). In 2015, that number decreased to approximately 22,000 complaints of identity theft, representing 7.6% of all complaints ("2015 Internet Crime Report," 2016). And in 2019, identity theft complaints were significantly reduced to comprise just 3.4% of all IC3 complaints, with 16,053 victims ("2019 Internet Crime Report," 2020). Based on this data, occurrences of identity theft have decreased by almost 14,000 (46.5%) within the past nine years.

On the other hand, the Federal Trade Commission's Consumer Sentinel Network (CSN) relies on data from several sources to comprehensively calculate instances of identity theft each year, including complaints received by the Federal Trade Commission, the IC3, Better Business Bureaus, the Canadian Anti-Fraud Centre, the U.S. Postal Inspection Service, the Identity Theft Assistance Center, and the National Fraud Information Center, among others. Compared to the number of complaints received by the IC3, in 2010, approximately 252,000 complaints concerning identity theft were identified by the CSN, comprising 19% of the overall number of complaints collected (Federal Trade Commission, 2011). In 2015, cases of identity theft increased to approximately 493,000, although its comprisal of the total number of CSN

complaints decreased to 16%. Identity theft continued to rise through 2019, where approximately 650,000 complaints (20.3% of the total amount) were received by the CSN (Federal Trade Commission, 2020). Based on this data, the total number of cases involving identity theft have increased by nearly 400,000 (158%) within the past nine years.

Australia

In 2010, 44,700 Australians were victims of identity theft (Australian Bureau of Statistics, 2012). This number increased significantly by 2015 when it was estimated that there were 126,000 instances of identity theft within the country (Australian Bureau of Statistics, 2016). However, by 2019, this number was reduced as Australia's Scamwatch received just 11, 373 reports of identity theft, which are received by web form and over the phone (Australian Competition and Consumer Commission, 2020).

Costs of Identity Theft

United States

In addition to recording the amount of cases of identity theft each year, reports have also publicized the financial damage that results from identity theft. According to the FBI's IC3, identity theft victims experienced a loss of over $160 million in 2019 ("2019 Internet Crime Report," 2020). This is a substantial increase from 2015, when victim losses were reported to be just over $57 million ("2015 Internet Crime Report," 2016).

Victim losses can be incurred due to lost time, lawyer fees, and in some cases, the required payment for fraudulent purchases. Further costs include credit card problems, particularly being turned down when applying for a credit card, having an account closed by the

issuer, and having a card rejected when attempting to make a purchase with it, being turned down for loans, bank accounts, or insurance, and experiencing harassment by debt collectors or creditors. Moreover, indirect costs could include the price of safety measures to protect against identity theft again and the foregoing of transactions that otherwise would have been undertaken if there was not a concern for the possibility of identity theft resulting from said transaction (Anderson, Durbin, & Salinger, 2008).

Australia

In Australia, identity theft resulted in $4,311,066 in out-of-pocket victim losses within the year 2019 (Australian Competition and Consumer Commission, 2020). In 2015, it was estimated that the total economic impact of identity theft in Australia was $2.65 billion. This figure contains the victims' costs of rectifying incidents, including legal fees, the cost of obtaining a credit report, and bank fees along with the costs of government actions to combat identity theft, which is worth an estimated $272 million, such as the implementation of biometrics (Jorna et al., 2020).

Identity Theft Victim Characterization

United States

Data has provided insight into the characteristics of individuals who are more likely to experience identity theft. In 2019, the CSN reported that identity theft was mostly reported by individuals between the ages of 30 and 39, with a little over 170,000 complaints coming from that age group. The next age group with the highest reported cases of identity theft was that between the ages of 40 and 49 with approximately 123,000 reports of identity theft. Individuals

between 20 and 29 years old followed with just under 111,000 complaints. After that came individuals between the ages of 50 and 59 (~77,000 complaints), individuals between ages 60 and 69 (~45,000 complaints), individuals within the ages of 70 and 79 (~17,000 complaints), individuals aged 19 and under (~14,000 complaints), and lastly individuals over the age of 80 (~6,000 complaints) (Federal Trade Commission, 2020).

Furthermore, in 2019, the CSN identified that Georgia experienced the most cases of identity theft, 427, per 100,000 population. Florida followed with 304 reports per 100,000 population and California succeeded that with 257 reports per 100,000 population. The state with the least amount of complaints per 100,000 population was South Dakota with 47. Vermont (54) and Wyoming (55) were also states that reported the least amount of cases of identity theft. Overall, though, California had the greatest number of complaints submitted to the CSN with over 101,000 while Wyoming had the least with only 319 (Federal Trade Commission, 2020).

Australia

A nationwide survey conducted by the Australian Institute of Criminology found that males between the ages of 25 and 34 was the group that was most likely to report identity theft victimization. Overall, males reported experiencing identity theft significantly more than females and people between 25 and 44 years of age were more likely to fall victim to identity theft than those in other age groups (Jorna et al., 2020).

Additionally, the study also found that Sydney experienced the greatest number of cases of identity theft, followed by Melbourne. On the other hand, Northern Territory experienced the least number of cases, with Hobart coming in with the second least (Jorna et al., 2020).

Statement of the Problem

Identity theft in America is a prominent issue that carries with it substantial financial repercussions. The continuous evolution of technology has increased the ease in which a perpetrator can commit this offense by providing them with an expanded attack surface for which to obtain a victim's PII necessary for the commission of identity theft. This is evident when observing the yearly progression of instances of identity theft within the United States along with the millions of dollars in losses that are reported as a result of becoming victim to this crime. Yet, despite technology having a worldwide presence and influence, some countries, such as America, are impacted by identity theft at a much greater rate than others. Thus, reasons for this discrepancy must be revealed so that countries, i.e., the United States, can become more secure against the threat of identity theft.

I hypothesize that the United States' higher rate of identity theft can be attributed to a greater amount of computer usage within the country, which would promote an increased attack surface, a less strict set of laws as determined by their sentencing guidelines, and a lower prosecution and conviction rate for the crime.

Methodology

To conduct this study, I utilized existing literature to perform a comparative analysis of the various factors that could possibly influence a country's rate of identity theft. The pertinent literature was acquired through Internet searches. The two countries compared are the United States of America and Australia[1]. The specific factors examined are the amount of computer

[1] Australia was selected for this study due to its relative comparability to the United States in terms of its size and social freedoms. Canada was also considered; however, Australia had a lower rate of identity theft, which made it more ideal for the analysis.

usage within each country, each country's respective federal laws that have been enacted pertaining to the crime of identity theft, and the prosecution of identity theft within each country, defined by their respective prosecution and conviction rates. Once each factor was identified, I compared their similarities and differences as they exist between the United States and Australia.

Results

Computer Usage

United States

In the year 2016, the United States Census Bureau reported that approximately 119 million households had access to at least one form of a computer and the Internet. This equated to 89% of the country's population at that time, symbolizing the computer as a common feature of everyday life (Ryan, 2018). During this year, there were nearly 400,000 complaints of identity theft submitted to the CSN (Federal Trade Commission, 2020). Assuming that these cases of identity theft were facilitated in some way through the use of a computer, this equates to a rate of 0.0034 instances of identity theft per household with Internet access.

Australia

In that same year (2016), in Australia, 86% of households had access to the Internet for a total of about 8.5 million households, according to the country's Bureau of Statistics (Australian Bureau of Statistics, 2018). This correlates to approximately 15,000 complaints of identity theft made to the country's Scamwatch around this time (Australian Competition and Consumer Commission, 2020). Assuming that these cases of identity theft were facilitated in some way

through the use of a computer, this equates to a rate of 0.0018 instances of identity theft per household with Internet access.

Computer Usage Analysis

The United States has 110.5 million more households with computer and Internet access than Australia (119 million compared to 8.5 million). The percentage of the total population of households that have computer and Internet access is also greater in the United States than Australia (89% compared to 86%). Furthermore, assuming that identity theft is committed with the use of computers, the United States experiences the offense at a greater rate, with 0.0034 instances of identity theft per household with Internet access compared to Australia's rate of 0.0018 instances per household with Internet access.

Identity Theft Laws

United States

In 1998, the United States Congress passed the Identity Theft and Assumption Deterrence Act, which amended Title 18, U.S. Code, Section 1028, marking the first time in which identity theft is considered a federal offense. This legislation prohibits the "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law" (Federal Bureau of Investigation, 2016). According to the United States Department of Justice, violations of this law can result, in most circumstances, in "a maximum term of 15 years' imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense" (United States Department of Justice, 2017).

Then, in 2004, Congress passed the Identity Theft Penalty Enhancement Act, which established penalties for aggravated identity theft. Aggravated identity theft is the use of another individual's identity to commit felony crimes. This act imposes a penalty of "(1) two years' imprisonment for knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person during and in relation to specified felony violations (including theft of public property, theft by a bank officer or employee, theft from employee benefit plans, various fraud and immigration offenses, and false statements regarding Social Security and Medicare benefits); and (2) five years' imprisonment for knowingly taking such action with respect to a means of identification or a false identification document during and in relation to specified felony violations pertaining to terrorist acts" (Identity Theft Penalty Enhancement Act of 2004). Essentially, this act increases the punishment of a felony crime by two years for a general offense and five years for a terrorism offense.

Most recently, the Identity Theft Enforcement and Restitution Act of 2008 was passed by Congress. This act did several things to promote the prosecution of identity theft by removing some of the barriers that existed prior to the act's ratification: (1) it authorized criminal restitution orders to compensate identity theft victims for the time spent to remediate the harm incurred, whether they be intended or actual; (2) it expanded the definitions of identity and aggravated identity theft to include that against organizations; (3) it identified the manufacturing, uttering, or possessing of counterfeit securities, mail, theft, and tax fraud as predicate offenses to aggravated identity theft; (4) it enabled the prosecution of cases that do not involve interstate or foreign communications; and (5) it eliminated the requirement to show that damage to a computer exceeded $5,000 in order to raise a prosecution (Identity Theft Enforcement and Restitution Act of 2008).

Australia

In Australia, identity crimes are primarily prosecuted under the Criminal Code Amendment (Theft, Fraud, Bribery & Related Offenses) Act of 2000, which amended Australia's Criminal Code Act of 1995. The amendment was designed to replace existing offenses with "a more modern and transparent scheme of theft, fraud, bribery, forgery, and related offenses" (Vanstone, 2000). Under this act, fraudulent conduct, including dishonestly obtaining property or a financial advantage by deception, false or misleading statements, forgery and related offenses, and impersonation, obstruction and causing harm offenses are all punishable by law as delineated in parts 7.3, 7.4, 7.7, and 7.8 of Chapter 7, respectively. These offenses all carry a maximum of 10 years' imprisonment except in the case of an individual impersonating a Commonwealth official who is a judicial or law enforcement officer and that impersonation results in harm, which carries a 13-year maximum prison sentence (Vanstone, 2000).

Identity Theft Laws Analysis

Both the United States' and Australia's legal codes contain provisions for which they can prosecute identity theft as a federal offense. However, key differences exist between the two country's statutes. Within America, the legislature explicitly defines the crime of identity theft, distinguishing it as the "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law", as mentioned above (Federal Bureau of Investigation, 2016). With this definition,

the United States labels the act of identity theft as a crime in itself. Australia, on the other hand, does not explicitly define the term of identity theft within its legal code. Rather, identity theft is grouped into the much broader category of fraud. As a result, the components that comprise identity theft are punishable according to Australia's statutes as opposed to the act of identity theft itself. In other words, the individual actions that lead up to the ultimate commission of identity theft, such as the use of deception, forgery, and the other acts identified previously, are what are punishable by Australian law. To provide an example, an identity thief wouldn't be prosecuted for identity theft. Instead, he would be prosecuted for the use of a false identity to deceive an entity into providing him with a financial advantage, such as a bank withdrawal.

The second key difference is the sentences that are distributed for a violation of the statutes regarding identity theft. In the United States, identity theft carries a maximum penalty of 15 years' imprisonment, with an additional two or five years in the case of aggravated identity theft, along with a fine and criminal forfeiture. In Australia, all of the offenses related to identity crimes carry a maximum of 10 years' imprisonment with the exception of impersonating and causing harm to a Commonwealth official who is a judicial or law enforcement officer, which carries a penalty of 13 years' imprisonment. Essentially, identity theft in America carries an extra five (or two) year prison sentence than that in Australia.

Prosecution of Identity Theft

United States

In 2015, America experienced approximately 493,000 instances of identity theft, with 160,520 being reported to law enforcement (Federal Trade Commission, 2016). With this, a total of 1,319 defendants were prosecuted in 854 cases of identity and aggravated theft raised in a

United States District Court (Offices of the United States Attorneys, 2016). Assuming that a defendant was only involved in one instance of identity theft that was perpetrated, this results in a prosecution rate of 0.27%. Furthermore, 1,223 of the 1,319 defendants were found guilty, equating to a conviction rate of 92.7% (Offices of the United States Attorneys, 2016).

Australia

In that same year (2015), there were an estimated 126,000 instances of identity theft within Australia. Of those 126,000 instances, Australia's police force recorded and prosecuted a total of 75,623 cases under the statutes discussed in the previous section (Jorna & Smith, 2018). This results in a prosecution rate of 59.5%. Furthermore, of those 75,652 cases, 60,951 resulted in a guilty verdict (Jorna & Smith, 2018). This equals a conviction rate of 80.6%.

Prosecution Analysis

Australia prosecuted identity theft at a 52.23% greater rate than the United States (59.5% compared to 0.27%). However, the United States had a 12.1% higher conviction rate for identity theft prosecutions (92.7% compared to 80.6%).

Discussion

This study sought to provide insight into the reasons for the United States' high rate of identity theft by analyzing potential factors with respect to Australia. I found that the United States has a larger total number of households that have computer and Internet access as well as a greater percentage of households with computer and Internet access in relation to the total population. This could potentially explain the United States' higher identity theft rate by

exemplifying the country's increased attack surface. Essentially, the United States' might suffer from more cases of identity theft at a greater rate simply because it contains more victims available to exploit through the use of the Internet. This idea is further supported when applied to the Routine Activities Theory of crime. The Routine Activities Theory proclaims that a crime will occur when three elements converge in time and space: (1) a motivated offender; (2) a suitable target; and (3) an absence of a capable guardian (Cohen & Felson, 1979). In the context of this study, these three elements converge when identity theft is committed through electronic means. First, there is the identity thief perpetrating the crime. Second, there is a suitable target due to the immense amount of Internet users within the United States who have opened themselves up to potential exploitation by providing their personal identifiable information online with the rise of e-commerce. And third, the relative anonymity of operating online along with the ability to do so remotely limits the possibility of a guardian being present who can stop the crime from being committed. As a result, a significant amount of identity theft occurs.

The second thing that I found is that while both the United States and Australia have the capability to prosecute identity theft under their respective legal codes, America's statutes are more tailored to the crime and carry a potentially greater punishment. These findings do not provide much insight into the reasons for the discrepancy between the United States' and Australia's identity theft rates; however, these laws become much more significant when coupled with the findings that Australia prosecutes identity theft at a much greater rate than the United States, although America has harsher punishments. These findings can explain the United States' elevated rate of identity theft based on the concept of general deterrence. General deterrence is the notion that the threat of punishment may discourage criminal acts from occurring. With this, evidence has more consistently supported the effect that the certainty of punishment has as a

deterrent as opposed to the severity of the punishment. Furthermore, recent literature suggests that the evidence pertains almost exclusively to the probability of getting apprehended (Nagin, 2013). When this information is applied to the results of this study, it is evident that the United States experiences a greater rate of identity theft because it fails to deter potential offenders unlike its Australian counterpart. Sure, America punishes identity theft more severely, but it doesn't prosecute nearly as many cases as needed to serve as a deterrent. And as just mentioned, the certainty of apprehension is much more effective in deterring crimes than the severity of punishment.

The implication of this study is twofold. Firstly, although computers improve the convenience of everyday life and are quite valuable, it is clear that they are also a source of misfortune. Despite this, computers and the Internet are and will remain to be an integral part of society. Therefore, users need to implement adequate safety measures necessary to protect their sensitive information online from various threats, such as identity theft. Various software and controls exist for this purpose and should be utilized to lower the probability and rate of victimization. Secondly, it is also evident that the United States needs to focus more on deterring identity thieves through criminal prosecutions. It is acknowledged that challenges exist that limit this capability that were not explored in this study. Future research could focus on identifying these challenges along with potential ways to eliminate them in order to better equip officials with the ability to effectively manage and prosecute instances of the crime within the country.

Limitations

The most glaring limitation of this study is that it relied on existing data and literature in order to perform the analysis. As a result, data and information was limited to that that had

already been presented in previous studies and that of which could be obtained. This significantly impacted the study's overall ability to utilize data from the most recent times as it was not always available. Consequently, the most recent data acquirable was utilized as it was discovered. Unfortunately, it is possible that not all of the statistical analysis contained within this study is relevant or representative of the data today.

Conclusion

This study focused on identifying potential reasons for the United States' high rate of identity theft by analyzing potential factors including the country's computer and Internet usage, its federal legislature pertaining to identity theft, and its prosecution and conviction rates and comparing them to those of Australia. It was hypothesized that the United States' elevated rate of identity theft would be attributed to a greater amount of computer usage within the country, less strict punishments for the crime of identity theft, and a low prosecution and conviction rate related to the offense. This study ultimately found that America does have a greater amount of computer usage, harsher punishments and a greater conviction rate than Australia, although Australia has a higher prosecution rate. These findings can explain the United States' increased rate of identity theft based on the Routine Activities Theory of crime and the concept of general deterrence.

References

2010 Internet Crime Report (Rep.). (2011). Federal Bureau of Investigation.

2015 Internet Crime Report (Rep.). (2016). Federal Bureau of Investigation.

2019 Internet Crime Report (Rep.). (2020). Federal Bureau of Investigation.

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives*, *2*, 171–192. Retrieved from https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.22.2.171

Australian Bureau of Statistics. (2012, April 19). Personal fraud costs Australians $1.4 billion. Retrieved from https://www.abs.gov.au/ausstats/abs@.nsf/lookup/4528.0Media Release12010-2011

Australian Bureau of Statistics. (2016, April 20). Personal fraud. Retrieved from https://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0/

Australian Bureau of Statistics. (2018, March 28). Household use of information technology. Retrieved from https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8146.0Main Features12016-17?OpenDocument

Australian Competition and Consumer Commission. (2020, April). Scam statistics. Retrieved from https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=30&date=2017

Australian Federal Police. (2019, November 15). Cyber crime. Retrieved from https://www.afp.gov.au/what-we-do/crime-types/cyber-crime

Center for Identity Management and Information Protection (2015). Identity crimes: Most common schemes. Retrieved from http://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588–608. Retrieved from http://faculty.washington.edu/matsueda/courses/587/readings/Cohen and Felson 1979 Routine Activities.pdf

Federal Bureau of Investigation. (2016, June 1). Identity theft. Retrieved from https://www.fbi.gov/investigate/white-collar-crime/identity-theft

Federal Trade Commission. (2011, March). *Consumer sentinel network data book*. Retrieved from https://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2010/sentinel-cy2010.pdf

Federal Trade Commission. (2016). *Consumer sentinel network data book*. Retrieved from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf

Federal Trade Commission. (2020, January). *Consumer sentinel network data book*. Retrieved from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf

Heller, I. (2008). How the internet has expanded the threat of financial identity theft, and what congress can do to fix the problem. *Kansas Journal of Law & Public Policy, 17*(1). Retrieved from https://law.ku.edu/sites/law.drupal.ku.edu/files/docs/law_journal/v17/heller.pdf

Identity Theft Enforcement and Restitution Act of 2008, Pub. L. 110-326 (2008)

Identity Theft Penalty Enhancement Act of 2004, Pub. L. 108–275 § 1028A (2004).

Jorna, P., & Smith, R.G. (2018). *Identity crime and misuse in Australia 2017*. Retrieved from https://aic.gov.au/publications/sr/sr10

Jorna, P. G., Smith, R. G., & Norman, K. G. (2020). *Identity crime and misuse in Australia: Results of the 2018 online survey*. Retrieved from https://www.aic.gov.au/publications/sr/sr19

Malwarebytes. (n.d.). *What is hacking - Everything you need to know*. Retrieved from https://www.malwarebytes.com/hacker/

Nagin, D. S. (2013). *Deterrence in the twenty-first century: A review of the evidence*. Retrieved from https://pdfs.semanticscholar.org/c788/48cc41cdc319033079c69c7cf1d3e80498b4.pdf?_ga=2.123544655.514546164.1587697633-209748425.1548723464

Offices of the United States Attorneys. (2016). *United States attorneys' annual statistical report*. Retrieved from https://www.justice.gov/usao/file/831856/download

Ryan, C. (2018, August 8). *Computer and internet use in the United States: 2016*. Retrieved from https://www.census.gov/content/dam/Census/library/publications/2018/acs/ACS-39.pdf

United States Census Bureau. (n.d.). *U.S. and world population clock*. Retrieved from https://www.census.gov/popclock/

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

Vanstone, A. (2000). *Criminal code amendment (theft, fraud, bribery & related offenses) act 2000 revised explanatory memorandum*. Retrieved from https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r957_ems_1590dbeb-d1b9-475f-8377-0d40d605d6fb/upload_pdf/35539rem.pdf;fileType=application/pdf