Some Legal and Practical Challenges in the Investigation of Cybercrime

Ritz Carr
Old Dominion University

A Few Legal and Practical Challenges in the Investigation of Cybercrime

By

Ritz Carr

April 13th, 2023

For the Coastal Virginia Commonwealth Cyber Initiative Undergraduate Research Program

Department of Criminal Justice and Sociology

Old Dominion University

ABSTRACT

According to the Internet Crime Complaint Center (IC3), in 2021, the United States lost around $6.9 billion to cybercrime. In 2022, that number grew to over $10.2 billion (IC3, 2022). In one of many efforts to combat cybercrimes, at least 40 states "introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity" with 24 states officially enacting a total of 41 bills (National Conference on State Legislatures, 2022).

The world of cybercrime evolves each day. Nevertheless, challenges arise when we investigate and prosecute cybercrime, which will be examined in the following collection of essays that highlight some legal challenges in the investigation and prosecution of cybercrime.

KEY WORDS: Cyber, Cybersecurity, Cybercrime, Data, Digital Forensics

REFERENCES

"Cybersecurity Legislation 2022." *National Conference of State Legislatures*, 22 July 2022, https://www.ncsl.org/technology-and-communication/cybersecurity-legislation-2022.

Internet Crime Complaint Center. 2022, *Internet Crime Report 2022*, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Accessed 28 Mar. 2023.

CHALLENGE 1:
DEFINING CYBERCRIME IN LEGISLATION – THE COMPUTER FRAUD AND ABUSE ACT

INTRODUCTION

The Latin quote *nullum crimen sine lege* encompasses one of the leading issues in investigating and prosecuting cybercrime: No matter how harmful the behavior, it cannot be prosecuted unless it is formally prohibited by law (LII; Nullum Crimen Sine Lege). In today's world, it is imperative that statutory crimes be worded clearly to be effective and survive a potential appeal.

The United Nations Office of Drugs and Crime (UNODC), states there is no official international standard definition for cybercrime (UNODC; Global Programme on Cybercrime). To effectively combat cybercrime, countries must produce, pass, and effectively prosecute cybercrime legislation. So, how many countries such have legislation?

As of 2023, 80% of the world has active cybercrime laws, as reported by the United Nations Conference on Trade and Development. In addition to those statistics, there are three other types of legislation regarding the regulation of the Internet: E-commerce laws (81%), Privacy laws (71%) and Consumer Protection laws (59%) (UNCTAD). For the most part, it appears the world has taken action on combating cybercrime *on paper*. While this is a great first step, it is not enough, as words do not equate to actions. How is the United States (U.S.) going about it?

In the U.S., the National Institute for Standards and Technology (NIST) is a department under the U.S. Department of Commerce whose mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life"; NIST defines cybercrime as "Criminal offenses committed on the internet or aided by the use of computer technology." The Department of Justice (DOJ), however, defines *computer* crime as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution." The DOJ states cybercrime and computer crime can be used interchangeably (DOJ). FBITraining.org defines cybercrime simply as "(a) crime that involves a computer and network." (FBI). Already, there is an issue: not only is there no official international standard definition of cybercrime, but there is also no standard *domestic* definition of cybercrime- and that is from government agencies and departments.

THE COMPUTER FRAUD AND ABUSE ACT

The first significant law that directly addressed computer fraud and some other computer crimes, the Computer Fraud and Abuse Act (CFAA), was passed by the U.S. in 1986. Essentially, it would prohibit "intentionally accessing a computer without authorization or in excess of authorization" (NACDL); however, many assert that the phrase "without authorization" is not properly defined, but the phrases "exceeds authorization" and "authorized access" *are* defined (LII; Fraud and Related Activity in Connection with Computers). But, even the definition of authorized access is not clear either, according to a 2020 Congressional Research Service report on the CFAA (Barris, 2020).

The problem? As mentioned before, the CFAA is too broad, in many areas including what information falls under authorized access or whether it is a federal crime to violate a

website's terms of service (Barris, 2020)(Crocker, 2021)- nearly 40 years later, even after amendments. Another problem: the wording. It is often regarded as vague, which poses an issue in due process when one considers the void for vagueness doctrine. Essentially, this occurs when "the law does not specify what is required or what conduct is punishable", as exemplified above regarding the "exceeds authorization" and "authorized access" clauses (LII; Void for Vagueness). In other words, it is not always clear what conduct is criminal. The following are real-life examples of the consequences the CFAA's vagueness causes.

VAN BUREN V. UNITED STATES: EXCEEDING AUTHORIZED ACCESS?

On June 3, 2021, the Supreme Court heard *Van Buren v. United States,* a landmark case regarding the broad scope of the CFAA. Former police sergeant Nathan Van Buren was offered $15,000 to provide the license plate number of a suspected undercover cop to someone who bribed him with money. So, using his own credentials, he logged into the database he *already* had access to and produced the number in exchange for the $15,000. His department wrote that "his conduct violated a department policy against obtaining database information for non-law-enforcement purposes". However, Justice Amy Comey Barret's majority opinion provided in part the following: "An individual "exceeds authorized access" when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases— that are *off-limits* to him" (*Van Buren v. United States* - 141 S. Ct. 1648 (2021)). Essentially, since Van Buren had access to the files he distributed, it was ruled that is conduct *did not* violate the CFAA.

Already, the CFAA has created issues for prosecuting cybercrimes: first, through not adequately defining "without authorization", and second, the conflicting meaning of information that is "off-limits" to someone who has access to it. Justice Barret wrote that "The relevant

question, however, is not whether Van Buren exceeded his authorized access but whether he exceeded his authorized access as the *CFAA defines that phrase*" (*Van Buren v. United States* - 141 S. Ct. 1648 (2021)). This further emphasizes the importance of how our cyber legislation should be worded clearly.

Even though what Van Buren did was unethical and a violation of his privilege as a policy violation, his appeal to the Supreme Court was far more beneficial to the cyber community in many ways more than one: a push to reform our cyber legislation, an emphasis on the importance of defining all technical terms within that legislation- no matter how scrutinizing –and the display of exercising one's civic duty of utilizing the appellate courts. *Van Buren v. United States* helped reform the CFAA in this opinion by going in depth to what "exceeding authorized access" *does not* look like regarding accessing information one had authorization to access but not using it for its intended purpose, further narrowing the scope (Millhiser, 2021).

AARON SWARTZ V. UNITED STATES: PENALTIES TOO SEVERE?

But there is another issue with the CFAA- the penalties. So much so, it is "putting people at risk for prison sentences for ordinary Internet behavior" (Jeschke, 2020).

To summarize, Aaron Swartz was a computer prodigy and formerly a Harvard research fellow who strongly supported an open-access internet for all, so much so he was able to rally strong opposition to the passing of the Stop Online Piracy Act in 2012 that would ultimately stop the bill from passing in 2012. His criminal conduct consisted of the following: as a research fellow, he sometimes studied at the Massachusetts Institute of Technology (MIT) and in 2010 he coded a script, grab.py, that would be run on MIT terminals through a laptop he hooked up in a ultility closet on campus that would roam the university's JSTOR (Journal Stoarge) database

downloading all the articles and journal publications it possibly could, eventually reaching a near 5 million files (Youtube, 2014). Although JSTOR and MIT would not press charges, the federal government saw an opportunity to exercise deterrence theory- to publicly punish a cybercriminal to deter others from online deviance.

According to Swartz's indictment, some the charges under the CFAA brought against him were the following: Knowingly accessing a computer to which he does not have authorization and further exceeding that authorization, accessing a protected computer with intent to defraud in addition to obtaining something of value, and the value of the forementioned goods totaling over $5,000, are a few (LLI; Fraud and Related Activity in Connection with Computers) (United States District Court of Massachusetts, 2011). A total of 13 felony charges, with 11 being under the CFAA, were brought against him that would expose him up to 35 years in prison and $1 million in fines. According to the United States Sentencing Commission (USSC), the maximum penalty for one count of *voluntary manslaughter* is 10 years in prison (USSC). In contrast, the penalties for the CFAA are the following:

> "*…first time offenders caught violating the CFAA may be punished with criminal fines of up to $5,000 per crime, imprisonment from 1 to 10 years, or a combination of both. For second time offenders, the CFAA provides that the offender will have to pay criminal fines of up to $5,000 for each violation, imprisonment for up to 20 years, or a combination of both."*

This means, for each of the 11 violations of the CFAA Aaron Swartz was charged with, his prison sentence could have reached 110 years maximum or 11 years minimum, if the maximum penalty for first-time offenders was applied to each charge, as he had never been charged with anything under the CFAA before then. The sentencing guidelines would likely

lower this number, but it would still be too high. Consider the weight of these crimes, as well as the type. Is accessing a computer without authorized access equate to sending someone flying after hitting them with a car, driving recklessly while drunk? Recall that both crimes, for first time offenders, carry a maximum sentence of 10 years.

Unfortunately, Aaron Swartz committed suicide likely due to the immense pressure he was under. Overnight, there was public outcry (Youtube, 2014)- many questioned whether the harsh penalties imposed by the CFAA were proper and many pushed for reform since, like the Electronic Frontier Foundation (EFF) who have "long fought to reform vague, dangerous computer crime laws like the CFAA" and "filed briefs both encouraging the Court to take today's case and urging it to make clear that violating terms of service is not a crime under the CFAA" (Crocker, 2021).

While a law like the CFAA had been a first, it was enacted when there was practically no Internet, one where its creators had no way of accounting for the exponential growth and evolution of the *idea* of the Internet into a whole new domain. Now that cybercrime is practically rampant and "ordinary" (Jeschke, 2020), should not the CFAA have penalties that better fit the nature and seriousness of the particular criminal conduct, like assigning someone to house-arrest with no access to computers/the internet for their sentence instead of wasting more tax dollars to aid overincarceration?

CONCLUSION

While 80% of the world may have cybercrime legislation, we know in at least one place, the U.S., that better legislation is needed. It takes real-life action to ensure the effective execution of said legislation. In both *Van Buren v. United States* and *Aaron Swartz v. United States District*

Court of Massachusetts we found that the U.S.'s CFAA posed major issues for prosecuting cybercrime due to unclear and ambiguous wording and the potential for such harsh penalties that make the prosecution of CFAA violations questionable.

REFERENCES

"§2A1.3 Voluntary Manslaughter." *United States Sentencing Commission*, 23 Apr. 2016, https://www.ussc.gov/policymaking/meetings-hearings/%C2%A72a13-voluntary-manslaughter.

"18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computers." *Legal Information Institute*, Legal Information Institute, https://www.law.cornell.edu/uscode/text/18/1030#e_6.

"Computer Crimes." *Computer Crimes | Office of Justice Programs*, Department of Justice, https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crimes-7.

"Computer Fraud and Abuse Act (CFAA)." *NACDL*, NACDL, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

"Cybercrime Legislation Worldwide." *UNCTAD*, https://unctad.org/page/cybercrime-legislation-worldwide.

"FBI Cyber Crimes Division, FBI Cyber Crimes Careers and Job Information." *FBITraining.Org*, FBI, 3 Nov. 2017, https://www.fbitraining.org/cyber-crimes/.

"Global Programme on Cybercrime." *United Nations: Office on Drugs and Crime*, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

"Glossary." *NIST*, 28 Feb. 2019, https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary.

"Jurisdiction." *Legal Information Institute,* Legal Information Institute, https://www.law.cornell.edu/wex/jurisdiction.

"National Institute of Standards and Technology." *NIST*, 28 Feb. 2023, https://www.nist.gov/.

"Nullum Crimen Sine Lege." *Legal Information Institute*, Legal Information Institute, https://www.law.cornell.edu/wex/nullum_crimen_sine_lege.

"Void for Vagueness." *Legal Information Institute,* Legal Information Institute, https://www.law.cornell.edu/wex/void_for_vagueness.

Barris, Peter. United States Congress, 2020, *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*, https://crsreports.congress.gov/product/pdf/R/R46536. Accessed 4 Mar. 2023.

Brown, Cameron. "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice." *International Journal of Cyber Criminology*, vol. 9, no. 1, Jan. 2015, pp. 55–119.

Crocker, Andrew. Opshal, Kurt. "Supreme Court Overturns Overbroad Interpretation of CFAA, Protecting Security Researchers and Everyday Users." *Eff.org*, Electronic Frontier Foundation, 3 Jun. 2021, https://www.eff.org/deeplinks/2021/06/supreme-court-overturns-overbroad-interpretation-cfaa-protecting-security. Accessed 5 Mar. 2023.

Jeschke, Rebecca. “EFF Asks the Supreme Court to Put a Stop to Dangerously Broad Interpretations of the Computer Fraud and Abuse Act.” *Eff.org*, Electronic Frontier Foundation, 17 Jan. 2020, https://www.eff.org/deeplinks/2020/01/eff-asks-supreme-court-put-stop-dangerously-broad-interpretations-computer-fraud. Accessed 5 Mar. 2023.

Knappenberger, Brian, director. *The Internet's Own Boy. Youtube - The Internet's Own Boy*, Luminant Media & Unjustus Films, 30 June 2014, https://www.youtube.com/watch?v=M85UvH0TRPc. Accessed 11 Apr. 2023.

Millhiser, Ian. “The Supreme Court Hands down Very Good News for Pretty Much Everyone Who Uses a Computer.” *Vox*, https://www.vox.com/2021/6/4/22507896/supreme-court-computer-crime-amy-coney-barrett-van-buren-hacking-fraud-abuse-clarence-thomas. Accessed 5 Mar. 2023.

Supreme Court. *Van Buren v United States - 593 U.S. ___ (2021). Justia*, https://supreme.justia.com/cases/federal/us/593/19-783/. Accessed 28 Mar. 2023.

United States District Court of Massachusetts . *Indictment of Aaron Swartz – Aaron Swartz v. United States District Court of Massachusetts*. 14 July 2011, https://www.documentcloud.org/documents/217117-united-states-of-america-v-aaron-swartz#document/p10. Accessed 6 Mar. 2023.

CHALLENGE 2:

JURISDICTION AND CLOUD COMPUTING IN THE CYBER DOMAIN

INTRODUCTION

Without a doubt, the cyberspace is not a place with physical boundaries. The lack of boundaries is what characterizes it and is what some say the primary factor that "connects the world". However, with such a connected world there are two main distinguishing factors that are a source for difficulties in investigating cybercrimes: jurisdiction and the Cloud.

JURISDICTION

First and foremost: what exactly is jurisdiction? The Legal Information Institute (LII) of Cornell Law School offers two main definitions: "Power of a court to adjudicate cases and issue orders" and "Territory within which a court or government agency may properly exercise its power". The LII also defines multiple types of jurisdictions, so the following are ones the most relevant to the cyberspace:

1. *Personal Jurisdiction/in personam: "*The Court's power over the defendant based on their contacts with the forum." (are they state citizens? Did the crime occur in state borders?)
2. *Subject Matter Jurisdiction:* "The power of a court to adjudicate (judge/decide) a particular type of matter and provide the remedy (solution) demanded."

3. *Territorial Jurisdiction:* "The Court's power to bind parties to an action to determine state/federal scope of power provided by the Due Process Clause in the Constitution." (LII)
    a. *Objective:* Action originated from outside state borders but completed within state borders.
    b. *Subjective:* Action originated from within state borders but completed outside of state borders. (The American Journal of International Law, 1935)
4. *Concurrent Jurisdiction:* "The notion that two courts might share the power to hear cases of the same type, arising in the same place."
5. *Diversity Jurisdiction:* "The power of Federal courts to hear cases in which the parties are from different states." (LII)

How can these types of jurisdictions be applied to the cyber space?

Before considering the following case example, it is important to understand and acknowledge the near worldwide condemnation and criminalization of child pornography, otherwise known as Child Sexual Abuse Images (CSAIs). Overall, one societal norm the world seems to share is opposition of CSAIs, whether the country criminalizes it or not. Unfortunately, the anonymous nature of cyberspace permits the ease of sharing and distributing CSAIs which make commonplace in the deepest reaches of the Internet.

Say we have nation state Alpha that has no criminal legislation regarding. This means CSAIs can be produced, distributed, etc. within state Alpha. Neighboring nation state Bravo, however, criminalizes CSAIs. Now, consider two friends: Jack in Alpha and Tim in Bravo.

Jack found CSAIs that his friend, also in Alpha, sent him. Jack decides to send them to Tim knowing he too likes CSAIs. Jack is not aware that Tim's state, Bravo, criminalizes the distribution and possession of CSAIs; however, Tim does not think they will be caught and refrains from mentioning it to Jack. So, they continue sharing CSAIs over the course of a few months.

One day, Tim's flat is raided by Bravo state authorities after lawfully securing a search warrant. This was due to authorities observing Tim's roommate, Charlie, distributing cocaine, which gave them enough probable cause [or, depending on that nation's law, authority to search] to be granted a search warrant. Upon finding Charlie's stash of cocaine, they seize Tim's laptop that Charlie had borrowed from time to time to search the files for any other contacts Charlie had in the drug trade. Upon inspection, authorities find the CSAIs Jack had sent Tim on the laptop and arrest Tim.

Consider the following jurisdictional issues in this scenario:

Personal Jurisdiction/in personam: Since Tim resides as a citizen in state Bravo, the courts in state Bravo have jurisdiction over him.

Subject Matter Jurisdiction: Since Tim possesses CSAIs in state Bravo, Tim is breaking nation state Bravo's CSAI law, thus giving courts in state Bravo jurisdiction over Tim's crimes.

Objective Territorial Jurisdiction: State Bravo claims to have some jurisdiction over Jack because Jack sent CSAIs to Tim- the contents of the crime originated from outside Bravo's borders but ended up inside Bravo's borders.

To put it simply, jurisdiction becomes a tricky subject when applied to the cyber domain. Local police departments and prosecutors investigating a cybercrime complaint may have

concerns in establishing jurisdiction to support further prosecution, making them hesitant to dig deeper. Victims become discouraged when they are informed of the difficulties in tracking cybercriminals, as it could be impossible to find them. And, if the offender is found, the odds of prosecuting them become uncertain due to the jurisdictional uncertainties.

JURISDICTION IN THE CLOUD

When there are cases to be investigated, though, jurisdiction is determined also by where the data in question lies- sometimes in multiple locations at once. One recent type of computing that has forever changed the way we store and transmit data is cloud computing. Referred to as the Cloud, it was first proposed by Dr. J. C. R. Licklider in a memo titled "Members and Affiliates of the Intergalactic Computer Network". The ultimate idea was to create a shared network for everyone (Nelson, 2018).

The National Institute for Standards and Technology (NIST) has defined cloud computing and outlined the three services it provides: Software as a service (SaaS), Platform as a service (Paas), and Infrastructure as a service (IaaS). All these services are offered over the internet, via the Cloud medium. The data is typically stored in servers owned by the vendor/business, or sometimes outsourced. There are also different types of cloud deployment methods: Public, which is accessible to anyone; Private, only accessible to a certain group with authorization; Community, a cloud meant to bring people together for a certain purpose; and a Hybrid, a mix of two or more methods (Nelson, 2018) The methods and services a Cloud Service Provider (CSP) offers will dictate the structure and organization of data.

Without a doubt, though, many know that the Cloud poses a variety of security issues, including jurisdiction. Many consumers and businesses use it as an online backup or repository

for a lot of data- including Personally Identifiable Information (PII), valuable economic data, and trade secrets- essentially utilizing the SaaS Cloud. But the big question is, where is our data physically located if it is 'up in the Cloud'? All Cloud providers are corporately structured and sometimes complex in where the headquarters and servers are located- the headquarters can be in the U.S. with servers in different states, or even servers overseas! This means your data can be stored in multiple servers in different places at once, which makes it difficult to determine jurisdiction. There is no concrete answer to this question except to refer to the headquarters of the provider for assistance (Willson, 2013). And that itself may be difficult.

Going back to the example outlined in the jurisdiction section, this can be reimagined in the sense that Jack and Tim are utilizing SaaS, but also downloading those CSAIs to their own computers, which poses another issue for data being in multiple locations at once- anyone who has access to a cloud service can essentially download content (they have access to, of course) from anywhere in the world at any time, simply by logging into their account. This could be at a guest computer at a resort in Mexico by an American citizen on vacation. In the U.S. and Mexico real CSAIs are illegal; in the U.S., however, fictional CSAIs (as in any media *depicting* minors engaging in sex) are allowed as long as it is not obscene, in addition to the possession of fictional CSAIs (United States Sentencing Commission, 1996), whereas in Mexico, both are completely illegal (United States Department of State, 2018). Already, the laws for one type of image (even though a very serious issue) in two different places are different and thus will be prosecuted and investigated on differing scales by both entities when their jurisdiction is involved.

UNITED STATES V. MICROSOFT CORP & THE CLARIFYING LAWFUL OVERSEAS USE OF DATA (CLOUD) ACT

To provide a realistic scenario concerning the Cloud and jurisdiction – and a possible solution – consider the following case of *United States v. Microsoft Corp,* in which Microsoft was required via warrant to produce all possible email content and information that was associated with a suspected illegal drug trafficker. Microsoft declined to fulfil this warrant due to the suspect's email contents residing in a database physically located in Ireland. Microsoft did not comply with the warrant at first and was then held in contempt. Their reason not to comply was due to data being stored outside U.S. borders and that applying 18 U.S. code 2703, the Required Disclosure of Customer Communications or Records, was an unauthorized extraterritorial application, which was held by the United States Second Circuit Court of Appeals (*United States v. Microsoft Corp. – 138S. Ct 1186 (2018)).* Also, this would violate the General Data Protection Regulation (GDPR) in Ireland under the EU, creating even more problems.

In March of 2018, the President signed into law the Clarifying Lawful Overseas Use of Data (CLOUD) Act. Essentially, this law requires companies and businesses to "preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information" to anyone with authorization (like a customer of the provider) regardless of where the data is located, like in Ireland. So, instead of retrieving the data from an overseas server, Microsoft is required to make backups of all its data domestically, even if the data originates from within the U.S (*United States v. Microsoft Corp. – 138S. Ct 1186 (2018)).*

How is this a solution to overcoming difficulties acquiring data from the Cloud? For one, it now requires the backing up of data, which is something that should have been occurring in the first place. So, this helps businesses and companies implement a data recovery system and to be responsible for their data. It also makes it less stressful to acquire data on servers outside of U.S. borders if it is backed up to a server within the U.S., which eliminates the need to cross

international borders and deal with that type of jurisdiction. It also "establishes a framework to allow the United States to enter into executive agreements with foreign governments to govern data access" (United States Congress, 2018).

CONCLUSION

Overall, jurisdiction in the cyberspace is a both a serious but confusing matter, and it is still unclear how it is applied, more so internationally than domestically, but there is room for better clarity and improvement. One main issue being widespread use of cloud computing; it may be convenient and affordable, yes, but seemingly lower prices come at a higher cost when things go wrong. While the CLOUD Act has provided us a small steppingstone to making it a little easier to conduct cloud forensics and take responsibility for potential jurisdictional issues, there continues be uncertainty in where boundaries lie in the cyber domain.

REFERENCES

"Article 3. Territorial Jurisdiction ". *The American Journal of International Law*, vol. 29, 1935, pp. 480–508. *JSTOR*, https://www.jstor.org/stable/2213639. Accessed 7 Mar. 2023.

"Jurisdiction." *Legal Information Institute*, Legal Information Institute, https://www.law.cornell.edu/wex/jurisdiction.

Nelson, Bill, et al. "Chapter 13: Cloud Forensics." *Guide to Computer Forensics and Investigations: Processing Digital Evidence*, 6th ed., CENGAGE LEARNING, New York, NY, 2018, pp. 524–548.

Supreme Court. *United States v Microsoft Corp. - 584 U.S. ___ (2018), Justia.* https://supreme.justia.com/cases/federal/us/584/17-2/.

United States, Congress, Cong. House, Judiciary and Rules. Introduced Feb 2, 2018. *Clarifying Lawful Overseas Use of Data Act or the CLOUD Act*, 115AD. 115th Congress, 2nd session, resolution Resolution 4943. *Congress.gov*, https://www.congress.gov/bill/115th-congress/house-bill/4943/text. Accessed 14 Mar. 2023.

United States Department of State, 2018, *2018 Country Reports on Human Rights Practices: Mexico*, https://www.state.gov/reports/2018-country-reports-on-human-rights-practices/mexico/. Accessed 14 Mar. 2023.

United States Sentencing Commission. 1996, *Report to the Congress: Sex Offenses Against Children Findings and Recommendations Regarding Federal Penalties*, https://web.archive.org/web/20090410163951/http://www.ussc.gov/r_congress/SCAC.PDF. Accessed 14 Mar. 2023.

Willson, David. "Legal Issues of Cloud Forensics." *Global Knowledge - Expert Reference Series of White Papers*, 2013, https://d12vzecr6ihe4p.cloudfront.net/media/965983/wp-legal-issues-of-cloud-forensics.pdf. Accessed 14 Mar. 2023.

CHALLENGE 3 –

DATA HIDING, CORROBORATION, AND THE FEDERAL RULES OF EVIDENCE

INTRODUCTION

When it comes to digital forensics, the handling of digital evidence is no easy task. Digital evidence must be isolated and examined with the utmost care to assure that corroborating and authenticating it will go as smoothly as possible- a taxing task at best. There are countless methods to hiding data, but not as nearly as many when it comes to recovering it. Moreover, introducing digital evidence is another tough hurdle to overcome, one directed by the Federal Rules of Evidence. As a result, investigators are presented with multiple challenges when collecting, evaluating, and presenting digital evidence in a trial.

CASE EXAMPLE

Say we have Jane Doe, a suspected narcotics trafficker part of a well-known drug enterprise. Jane has been arrested as a suspect and the authorities are trying to prove that Jane was at the neighborhood 7-11 at two in the morning meeting with a few other members of the ring to go over supply and sales. The authorities have not been keeping an eye on Jane as closely as higher-profile members, but upon hearing her name while surveilling another meet up, they thought catching and recruiting a lower-profile member may help them get more details about the enterprise.

Upon her arrest, Jane waives her Miranda Rights and is presented with a search warrant to search her phone, as per the Supreme Court case *Riley v. California*, which generally prohibits the search of an electronic device upon arrest unless a separate search warrant to search the device is acquired (*Riley v. California* - 573 U.S. 373 (2014)). While being interrogated, Jane provides the authorities with an alibi that sounds solid: she was home taking care of her grandmother, Janice. Little do they know, Janice has dementia and often mistakes Jane for someone else. But, on Jane's phone is a location tracking app that her grandmother can see where Jane is at all times and vice versa, so Janice can call Jane when she needs assistance. The location app provides a 24-hour location history of the host, solidifying Jane's alibi of being home earlier that morning when the meeting was taking place.

However, upon further examination of the files on her phone and those recently deleted, a digital forensics investigator discovers that Jane had downloaded a GPS spoofing app. And, upon later questioning her grandmother, she recalls hearing the front door open around three in the morning, but nothing before that. Janice also mistakes the officer questioning her for her son, Mason. With this information, the officers are able to build a case against Jane and believe that Jane was present at the drug meet and is a part of the drug ring.

The main point of this case example was to provide an instance of corroborating digital evidence. If there is a case where the only thing supporting an alibi is a GPS location, it can be difficult to trust whether that evidence is valid- there needs to be an adequate foundation to establish the authenticity of the evidence. If the offender in question is known to be tech-savvy, then the authenticity of the evidence would likely be questioned because of the possibility of the GPS location being spoofed. Considering that the cyber domain hosts a plethora of crimes and

that the internet is a player in nearly every crime, the corroboration of digital evidence becomes more and more vital as we struggle to sift through the seemingly endless troves of it.

DATA HIDING AND CORROBORATION

One way to corroborate digital evidence is by validating and authenticating it with cryptography; however, it helps to know how data is hidden via the art of steganography. Sometimes, some methods of steganography are difficult to detect and may pass as authentic evidence, making the sole task of corroborating digital evidence a daunting and lengthy one for digital forensics investigators. This is why we validate data through means of hashing.

Each file, be it an image, spreadsheet, word document, etc., has its own hash value that makes it unique; it is almost like how we as humans have unique DNA - that hash value identifies that piece of media and, like a gene mutation changes DNA, any changes in the file will change the hash *completely*. To check if a file has been changed, the hash can be obtained before the file is processed or analyzed. After you process it, you calculate the hash of the file once more and check it against the first hash to see if the file has been tampered with. The main two hashing methods used to corroborate digital evidence in digital forensics are MD5 and SHA-1. Most importantly, investigators first make a forensic copy of the evidence before making a hash (Nelson, 2018).

There does run the possibility, however, of a collision occurring. This means that even in theory while no two files are to have the same hash value, the possibility of two files having the same hash has occurred in practice. When this happens, the files must be examined side by side in a Hex editor that can display the bits to see if the files are both identical (Nelson, 2018).

But what makes the corroboration of digital evidence so difficult? Upon examining a file, you find that the hash has changed after processing, which means the file has changed; but how? Consider the methods of hiding data through various forms of steganography. The file with two different hashes may look identical *visually*, but through methods of steganography, there is data hidden in the second file somewhere - or maybe the files are not visually identical but do not give clues as to what has changed. It is up to the digital forensics investigator to figure out how the data was hidden in the file. Or there may be methods used such as the following to change a file and hide the true content of it (Jiang, 2022):

- *Renaming Files:* this method of hiding data is an easy one, especially if the host uses no naming convention for their files or does. Simply renaming a file "math_homework" that is really a spreadsheet of drug dealer contacts is one way to use this method.
- *Bit Shifting:* Bit shifting is taking the bits of a file and shifting them left or right a select number of times to make the file unreadable. A hex editor tool can accomplish this, like Hex Workshop, which can also be used to unscramble the file.
- *Changing File Extensions:* This method consists of taking a file and changing the extension of it, like changing a spreadsheet to a word document- "math_homework" looks like a word document but is actually a spreadsheet.

(Nelson, 2018; Chapter 9).

Since steganography has various methods of hiding data, the process of authenticating and validating it makes the process of introducing evidence into court a long one. Given that we now know the basics of digital evidence corroboration and hiding, how exactly is digital evidence handled in court, and why may it be difficult to use in a case?

THE FEDERAL RULES OF EVIDENCE

In the United States, the Federal Rules of Evidence (FRE) came into existence in 1972 in response to a Supreme Court order. Between then and 1975 when the FRE were officially enacted, several amendments were made by Congress. Since, then, the FRE have been amended multiple times, nearly every one to three years. Within the FRE, there are eleven articles (LII; "Federal Rules of Evidence."). Essentially, the FRE are "a set of rules that governs the introduction of evidence at civil and criminal trials in United States federal trial courts" (The National Court Rules Committee, 2022). Although all rules in the FRE are important, there are two notable rules that pertain to digital evidence: Articles VIII and IX titled Hearsay and Authentication and Identification respectively. Understand, too, that individual states are also able to establish their own rules of evidence.

ARTICLE VIII: HEARSAY

The Legal Information Institute defines hearsay as the following: "an out-of-court statement offered to prove the truth of whatever it asserts, which is then offered in evidence to prove the truth of the matter" (LII; "Hearsay."). Instead, for example, quoting someone else who is not present in the courtroom poses an issue for establishing a credibility; how do we know the person being quoted is reliable? There is also *no* opportunity for that witness to be cross examined. Digital evidence such as the content of email contents, text messages, and documents commonly contain hearsay, just like verbal testimony. Nonetheless, it is difficult to dispute when no eyewitness testimony can corroborate the content within those files, like email communications between a deceased victim and offender (Nelson, 2018; Chapter 4).

However, Rules 802, 803, and 804 list various exceptions to the Hearsay Rule. The following are common exceptions that apply to digital evidence:

- *Business records*
- *Certain public records and reports*
- *Evidence of the absence of a business record, public record, or entry.*

In the case of the business records exception, the court will allow those records that are of "regularly conducted activity" like memos, reports, etc., due to the fact that these records are authenticated by "verifying that they were created at or near the time by, or from information transmitted by, a person with knowledge..". However, there is also an amendment that for those documents or files older than 20 years, "ancient documents", that does not require their authentication through testimony (Nelson, 2018; Chapter 4). For the most part, digital business records are considered admissible.

Other records such as computer-generated records (CGRs) and computer-stored records (CSRs) are also subject to hearsay challenges. In order to be admissible evidence, CGRs and CSRs must be deemed authentic and trustworthy. This can be accomplished through several methods, but most commonly these records must be proved they were not altered or damaged after creation and that the program that created them is in correct working order, in addition to those records being proven to be created by a person- the data must also be reliable and trustworthy (Nelson, 2018; Chapter 4).

ARTICLE IX: AUTHENTICATION AND IDENTIFICATION

As discussed in previous sections, the authentication of digital evidence is vital to its admissibility. Authenticating digital evidence is essentially proving that it is accurate and

reliable. Rule 902, “Evidence that is Self-Authenticating”, is especially of interest when it comes to digital evidence. Until this past decade, establishing a foundation-testimony for digital evidence was difficult. However, times have changed.

As of 2017, the FRE were amended to include sections 13 and 14 in Rule 902 that include digital evidence specifications: “Certified records generated by an electronic process or system” and “Certified data copied from an electronic device, storage medium, or file” respectively. Essentially, the previously mentioned CGRs and CSRs will no longer need foundation-testimony to be deemed admissible, as long as appropriate certification can be provided to prove that the program that created these records produces accurate results and digital evidence copied is “authenticated by a process of digital identification” (Heinen, 2017).

Subsequentially, there must be a qualified body to authenticate both CGRs and CSRs used in a case, i.e. the digital investigator, who would likely need to be present at the trial to testify as an expert witness regarding the records’ authenticity *if* the opposing party objects to their certification. Furthermore, the opposing counsel must be given advanced notice of the acquisition of digital evidence that is to be used in trial, especially if the evidence is exculpatory to comply with the Brady Rule (Heinen, 2017). Undeniably, it is imperative to scrutinize the process of recovering, collecting, analyzing, and evaluating digital evidence.

CONCLUSION

Data corroboration is no easy task for digital evidence, especially if it is to be used in court. There are endless methods to hiding data, new methods being discovered every day. As a result, it is vital that digital forensics investigators be up to date on their tools at all times and possess the highest levels of innovation and initiative. Not only that, but they must also be

experts in understanding the foundational aspects of law when it comes to investigating, prosecuting, and examining evidence. But, knowing the ever-evolving world of cybercrimes, it is without a doubt a challenge to collect and corroborate digital evidence.

REFERENCES

"Federal Rules of Evidence." *Legal Information Institute*, Legal Information Institute, https://www.law.cornell.edu/rules/fre.

"Federal Rules of Evidence, 2023 Edition." *Federal Rules of Evidence*, The National Court Rules Committee, 13 Dec. 2022, https://www.rulesofevidence.org/.

"Hearsay." *Legal Information Institute*, Legal Information Institute, https://www.law.cornell.edu/wex/hearsay

Heinen, Gregory N. "New Federal Rules of Evidence 902(13) and 902(14)." *Foley*, Foley & Lardner LLP, 1 Dec. 2017, https://www.foley.com/en/insights/publications/2017/12/new-federal-rules-of-evidence-90213-and-90214. Accessed 24 Mar. 2023.

Jiang, Peng. "Digital Steganography." *CYSE 301 Cybersecurity Techniques and Operations.* Old Dominion University. August 2022.

Nelson, Bill, et al. "Chapter 4: Processing Crime and Incident Scenes." *Guide to Computer Forensics and Investigations: Processing Digital Evidence*, 6th ed., CENGAGE LEARNING, New York, NY, 2018, pp. 143 - 186.

Nelson, Bill, et al. “Chapter 9: Digital Forensics Analysis and Validation.” *Guide to Computer Forensics and Investigations: Processing Digital Evidence*, 6th ed., CENGAGE LEARNING, New York, NY, 2018, pp. 378 - 405.

Supreme Court. *Riley v. California - 573 U.S. 373 (2014). Justia*, https://supreme.justia.com/cases/federal/us/573/373/. Accessed 28 Mar. 2023.