Project - 3

FACT PATTERN ANALYSIS

Sravani Ravulaparthi
CYBR 641 - Cybercrime Investigations
University of Maryland Baltimore County
M.P.S. Data Science
Prof. Adam Lippe
12/11/2022

Fact Pattern One

Criminal Liability

1. **What evidence would you seek to obtain from or about each individual and from what entities?**

Individual A:

Evidence:

Student, (A) personal computer and all communication happened between (A) and (B) over the chat in G.com & Email address related to Azul@MSU.edu

Entities:

G.com + Email Server Provider of MSU.EDU

Individual B:

Evidence:

B Computer and all communication happened between (B) and (A) over the chat in G.com& Email address related to Azul@MSU.edu

Entities:

G.com + Email Server Provider of MSU.EDU

Individual C:

Evidence:

Information related to their Spyware, log files information on the school's computer and Suspyware.com

Entities:

Suspyware.com ISP host

Individual D:

Evidence:

Log information of the school's computer and students' credentials collected.

Individual E:

Evidence:

Information related to the website CampusHackers.com, and stolen Kryptonite (K) program

Entities:

CampusHackers.com, ISP host

Individual F:

Evidence:

Just the Computer

Individual G:

Evidence:

Computer, Phony templates, phony documents, laminating machine, lock picking tools, and files stored in his account.

Entities:

Student

Individual H:

Evidence:

Computer and Email conversation between H and I

Entities:

Email Server Provider MSU.EDU

Individual I:

Evidence:

Computer and Email conversation between I and H

Entities:

Email Server Provider MSU.EDU

2. **Who may be charged with criminal offenses and what offenses can be charged?**

(B) may be prosecuted with cyberbullying, because (B) is attempting to pose as a girl by proxy and sexting(Maras, p.264, 2015) with victim (A) over email. (B) can be charged under 18 U.S.C. § 2252, which is a section of **Child Pornography Prevention Act of 1996**, which relates to actions involving child pornography that sexually exploits kids, and 18 U.S.C. § 2252 (A) forbids such acts.(Holt, p.324, 2018). **(B)** also violated **Sexual Exploitation of Children Act of 1978** which is a "Law

that made it illegal for someone to manufacture and commercially distribute obscene materials that involve minors younger than 16 years old." (Maras, p.614, 2015)

Owing to the use of their spyware, **(C) (D)** will be charged under 18 U.S.C. § 1030, which is **Computer Fraud and Abuse Act (CFAA)** (Holt, p.119-121, 2018) for breaking into a university computer's security system and gathering data on the users who have been using such machines on purpose. Due to the fact that their Suspyware caused the university's systems to crash, (C) (D) will also be held accountable under 18 U.S.C. § 1030(a)(5)(C). They will also be charged in accordance with 18 U.S.C. § 1030(a)(5)(B) since (C) (D) actions were unintended and not done with the intent to harm the university system.

A charge of violating 18 U.S.C. § 1030(c)(2)(B) (Holt, p.119-121, 2018), will be brought against **(C) (E)** for pushing the spyware (K) on his website CampusHackers.com and for promoting his friend's (C) Suspyware via CampusHackers.com

Due to accessing the student's [(A) (G) (H)] log-in credentials, **(F)** will be charged with identity theft under 18 U.S.C. § 1028(a)(5)(6), which is **Identity Theft and Assumption Deterrence Act** of 1998 (Holt, p.253, 2018). Given that she had access to the student's [(A) (G) (H)] emails, she might also be prosecuted with mail theft under 18 U.S.C. § 1708.

(G) will be charged under 18 U.S.C. § 1028(a)(7) for attempting to construct fraudulent identities for individuals, including SSNs and driver's licenses

Due to an alleged threat to kill (I) and his/her family via email and his/her promise to go across the nation to carry it out, **(H)** will be charged under 18 U.S.C. § 875(C).(D.O.J Archives, 2020)

3. What are each defendant's substantive defenses?

(A) can provide a substantive defense for himself because he never asked (B) for the nudes, always put them in the trash, and didn't intend to do commit a crime.

By pleading guilty, **(D)** can argue that he did not intend to sell or promote the spyware as (C) because he shared the information with (F) and got in touch with (E) to advertise it on his website. He also asserts that he checked the software's functionality on a computer at a university before getting the data the next day.

The acquisition of the evidence from **(G)** and **(H)** respective dorms should be questioned, they can claim, violation of the Fourth Amendment and the US Privacy Act, making the evidence inadmissible in court.

Due to her prompt notification to the authorities on her usage of mailboxes of (A), (G), and (H), **(F)** may enter a plea agreement with the law enforcement authorities.

4. What is the government's counterargument to each defense?

Prosecutors can argue that even though **(A)** consciously did not to ask for or distribute the allegedly (B)-owned pornographic images, but even after receiving the images, he didn't end the conversation or notify the authorities.

An argument can be made that **(D)** should have gotten permission from the university dean (J) and students who have access to that system, to test the Spyware, instead of testing it on his own, which makes him liable for what he did on the University's systems.

Even though she promptly notified the authorities on her usage of mailboxes of (A), (G) and subsequently getting an acknowledgment from the authorities, **(F)** accessed another student's(H) account, proving that she is operating maliciously by having access to the data that she requested from (C).

Given that the email transfer includes a third party and there is no reasonable expectation of privacy, the Fourth Amendment and the US Privacy Act claim presented by **(G)(H)** is void.

5. **What evidence should arguably be suppressed, and why?**

The evidence that (F) acquired may be suppressed due to a couple of facts. First it can be argued that it is hearsay evidence(Maras, p. 81, 2015). And second, the absence of a proper search and seizure warrant and the fact that the police have already started their investigation will be argued to get it suppressed.

6. **What other relevant issues do you feel are worthy of discussion based on this fact pattern?**

I believe the institution is a little lenient regarding network security and email regulations. If they had restricted email access within the campus or established a surveillance mechanism for emails sent outside of their organizational network, the scenario would've been different. Furthermore, by allowing students to install third-party apps in the university system, the university exhibits its flaws in granting administrators access to the system instead of guest access, who might ostensibly reduce risk by preventing installations.

Civil Liability

1. **Who may be civilly liable to whom, and under what theories?**

I believe this is a classic case that comes under Routine activities theory, "which states that a crime occurs when the following three elements come together in any given space and time:

1. an accessible target
2. the absence of capable guardians that could intervene
3. the presence of a motivated offender" (N.S.W Government, 2014)

In our case the accessible targets are (A) and (I), and the motivated offenders are (B), (C), (D), (E), (F), (G), (H), (K). The capable guardian who can prevent the crime from happening but is absent is (J). Everyone other than the victims are liable in this case.

C and D could be charged with destroying university computers and sentenced to up to $5,000 in fines or five years in prison under 18 U.S.C. § 1030(a)(5)(B).

Since the court has already set the precedent in addressing threats to privacy posed by spyware, as we can see here: “It is already illegal to sell or advertise surreptitious interception devices of this type. Indeed, the department recently successfully prosecuted the maker of the “StealthGenie” spyware, and the court fined the offender half a million dollars”(Caldwell, 2015). **(C)** and **(E)** can be charged under 18 U.S.C. § 2512 (1)(a)(b)(c)(i)(ii) (US Code Notes, 2022), for making and selling Spyware inside the U.S territory.

Due to the fact that (F) violated 18 U.S.C. § 1028(a)(5) and used (A), (G), and (H), she may be subject to fines of up to $1,000 per occurrence, a total of $3,000, or both.

2. What are each defendant’s defenses?

I believe arguing that the evidence is **hearsay** and suppressing that is the only way each defendant can do. Additionally, as the investigation's following stages will probably reveal how the evidence was seized and obtained, each defendant's secondary line of defense would likely be that (F) accessed their credentials and breached university network by using that information.

3. What are the plaintiff's counterarguments to each defense?

All of the material acquired during the search in compliance with the aforementioned laws would be the plaintiff's counterarguments in this case. To prove this the plaintiff could employ numerous digital forensic investigators and have them perform similar tests on the material acquired. The plaintiffs can also argue that it was a **Consent search**—"A type of search that can occur without a warrant and without probable cause if an individual who has authority over the place or items to be searched has consented to the search”(Maras, p.157, 2015), (**J**) in this case. Its legitimacy may be challenged but it’s worth to make an argument about.

Fact Pattern Two

1. **What crimes did Xavier commit?**
   - Xavier has sent bomb threats via email in February 2019 to the school and its property.
   - Using a portable wireless Internet access device and one or more accomplices in April 2019, making multiple simultaneous bomb threats against the school.
   - Malware infection of a representative of a significant Internet service provider ("ISP").
   - Accessing part of the ISP's operational data, gaining access to its internal network, and remotely approving its internet computer systems in March 2019 violating the aforementioned **Computer Fraud and Abuse Act (CFAA)** (18 U.S.C. § 1030 (5) (a) (b) (c)).
   - Including unauthorized access to various private cell phones violating (18 U.S.C. § 1030 (a) (2) (c)) Xavier also made an illegal access to a protected computer belonging to a major phone service provider violating (18 U.S.C. § 1030 (a) (1))
   - In an effort to pay for their calls fraudulently (18 U.S.C. § 1030 (4)) Xavier has fabricated phone accounts for himself and his associates
   - He was able to search for specific clients whose data has been posted online as a result of unlawful access ((18 U.S.C. § 1030(7)(a)(b)(c)), by creating an account with associate access and the skill to save customer identifying data (18 U.S.C. § 1030 (a) (2) (c))
   - In April 2019 threatened a separate phone company over a recorded line(Observe AI), that he will start a denial of service attack that was successful in blocking a significant portion of the phone company's web activities.

2. **What issues do you believe authorities may have had in the investigation? Specifically examine the issues related to any search and seizure, collection of evidence, chain of custody, prosecution and sentencing of the case. Be specific on the items that should be seized and how they should be analyzed. You should spend over two pages detailing all of the relevant issues.**

A major law that is violated in this case is **Computer Fraud and Abuse Act (CFAA) 18 U.S.C § 1030.** It is critical to recognize which law enforcement authorities are in charge of investigating computer hacking. Several scenarios, including the use of email, electronic devices, and hacks into important ISPs and telecommunications service providers, are present in this instance. The first concern for the authorities would be data preservation because the case ranges from January 2019 to April 2019. Each entity is required to store data for up to 90 days in accordance with 18 U.S.C. 2703(f), and an extra 90 days if a lawful extension is obtained.

Even though, obtaining a search and seizure warrant in accordance with the procedure will be the investigator's is a challenge when collecting digital evidence from the crime scene, the investigation's location is an even bigger issue. Both on-site and off-site searches are the methods. If the investigator believes a site search should be conducted, there is no need to seize the digital evidence. “Consider the following variables while deciding whether to conduct onsite research:

1. Density of device deployment
2. Device type and
3. Device location
4. Recording history
5. Device interface”(Cameron, 2019)

Now that the preservation letters request was granted, it is obvious that the authorities would want a search and seizure warrant in order to proceed with the investigation for additional evidence to prosecute Xavier. The authorities must submit a request to the court specifying the

precise location of the search and seizure, the sort of evidence used to support it, the justification for the search and seizure, the background of the case, and the current status of the case.

Investigators from the law enforcement must gather information from Xavier's email, personal computers, portable wireless internet access device, ISPs, and telecom service providers to better comprehend his case. The act of looking for digital evidence on a computer can quickly turn into a detailed analysis of a wide range of information.

Citizens in the United States are protected from unreasonable government searches and seizures by the Fourth Amendment of the Constitution. Privacy of people is protected. It should come as no surprise that many of the strategies used by law enforcement to combat cybercrime overlap with this defense. The access and monitoring of communications on email, cell phones, and personal computers by law enforcement is not always authorized. People's rights to privacy and the worth of their private property may be violated by these methods. Regardless of this disparity, when investigating cybercrimes, law enforcement must adhere to the procedures for searches that are permitted by the constitution.

Authorities must always follow a search methodology that specifies what is being looked for, since there are numerous ways to store damning data on a computer. Law enforcement agents must perform thorough computer searches due to the fact that criminals may use IP spoofing, encryption, labeling, or concealing to conceal incriminating information. The biggest challenge facing law enforcement when gathering digital evidence is that it is somewhat less palpable than most physical evidence. It qualifies as brittle evidence because of how easily it may be changed or destroyed. In fact, simply acquiring it or studying it could change it.

Since the prosecutors presenting the evidence must show that it hasn't been changed or tampered with since it was gathered at the crime scene in order for it to be admitted in court, this creates a problem. The admissibility of evidence is subject to strict rules. For the court to accept

evidence for presentation, admission into the case file, and consideration in the decision, it must be pertinent, material, and competent.

In order to ensure that the chain of custody is as authentic as possible, a series of steps must be followed. It is important to note that, the more information a forensic expert obtains concerning the evidence at hand, the more authentic is the created chain of custody. Due to this, it is important to obtain administrator information about the evidence: for instance, the administrative log, date and file info, and who accessed the files. “You should ensure the following procedure is followed according to the chain of custody for electronic evidence:

1. Save the original materials
2. Take photos of physical evidence
3. Take screenshots of digital evidence content
4. Document date, time, and any other information of receipt
5. Inject a bit-for-bit clone of digital evidence content into our forensic computers
6. Perform a hash test analysis to further authenticate the working clone”(Obbayi, 2019)

It is necessary to take the device and send it safely to the lab when a forensic expert wants information from a portable wireless device or computer device since these devices lose their evidence if the power is gone which is termed as non-volatile data in computer terms.

Assume that you are an investigator who received a piece of metadata for proofing. Yet you can’t find any meaningful information in it. The fact that there is no meaningful information within the metadata does not mean that the evidence is insufficient. We can find out where information may lie can be found by analyzing the chain of custody. If it maintained as mentioned above, and explained further below, you can dig out meaningful information from it.

When dealing with digital evidence and Chain of Custody, a few considerations are involved and accepted by global law enforcement authorities:

1. “Never ever work with the Original Evidence
2. Ensuring storage media is sterilized
3. Document any extra scope
4. Consider the safety of the personnel at the scene” (Garg, 2020)

During an examination, the steps of the aforementioned process may be repeated several times. Once the evidence obtained is sufficient for prosecution, and the original evidence is preserved till the court hearing then there is no second thought in believing that the accused, Xavier in this case, gets sentenced.

References

1. Maras M.-H. (2015). Computer forensics: cybercriminals laws and evidence second edition (2nd ed.). Jones & Bartlett Learning.
2. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and Digital Forensics: An Introduction (2nd ed.). Routledge.
3. N.S.W Government, 2014, Web: https://www.crimeprevention.nsw.gov.au/Documents/routine_activity_factsheet_nov2014.pdf
4. D.O.J Archives, 2020, Web: https://www.justice.gov/archives/jm/criminal-resource-manual-1069-overview-pertinent-provisions-interstate-and-foreign-extortion
5. Caldwell. L. R., 2015, Web: https://www.justice.gov/archives/opa/blog/addressing-threats-privacy-posed-spyware
6. US Code Notes, 2022, Web: https://www.customsmobile.com/uscode/title18_partI_chapter119_section2512
7. Cameron. L, 2019, Web: https://www.computer.org/publications/tech-news/research/digital-forensics-security-challenges-cybercrime
8. Obbayi. L, 2019, Web: https://resources.infosecinstitute.com/topic/computer-forensics-chain-custody/#:~:text=What%20is%20the%20chain%20of,control%2C%20transfer%2C%20and%20analysis.
9. Garg R., 2020, Web: https://www.geeksforgeeks.org/chain-of-custody-digital-forensics/