Activity 7: Authentication

Ryan Coon

CST-407

Professor Ty Howard

February 4, 2024

Part 1:

Loom Video URL:

<https://www.loom.com/share/a2a4212874b94e068ce0e6b5381c6235?sid=bc971fad-901f-4b5a-823e-6bfb258e3052>

Heroku Deployment URL:

<https://jokesapp-5e6f51d6c310.herokuapp.com/>

Code Repository:

<https://github.com/rcoon1/herokuphp>

I had the files zipped and got notification that the file was too large to upload into the assignment submission.

Part 2:

Background: On December 2, 2015, 14 people were killed, and 22 others were seriously injured when Syed Farook and Tashfeen Malik conducted a mass shooting and attempted bombing at the Inland Regional Center, a community college, in San Bernardino, California. The two were killed in a shootout with the police. An iPhone used by Farook for work purposes was recovered during the investigation. The phone was encrypted and designed by Apple to delete all data on the phone if too many unlock attempts were attempted.

1.Issue 1 - Legal Precedent: The FBI requested and then sued Apple to create a method that would unlock the phone. Apple refused. James Comey, the FBI Director at the time, stated “…any decision made by any judge in any form is going to be possibly precedential,” (Al Jazeera English, 2016).

a.Explain what “precedential” consequences James Comey is referring to.

I believe he is referring to the case of whether it goes either way, it will allow or block some pretty huge parts of an individual’s personal life. If it passes, they can now unlock any phone at their will and go through it with a fine-tooth comb, and if it’s blocked, it protects the personal private information of individuals.

b.How does the All-Writs Acts of 1789 relate to the Apple vs. FBI case?

The All-Writs Act of 1789 is a federal statute that authorizes United States federal courts to issue all necessary writs in aid of their respective jurisdictions. In the context of the Apple vs. FBI case, the All-Writs Act was invoked by the government to compel Apple to assist in unlocking an iPhone that belonged to one of the San Bernardino shooters.

c.According to Cindy Cohn, what information did Apple and Verizon give to the FBI after the attacks at San Bernardino?

Apple ended up access to all of the information they had, including the metadata, they now knew everyone they called from said phone. She also stated that it was a Verizon phone, and that they could have accessed the call data from them.

d.Cindy Cohn is from the Electronic Frontier Foundation, an organization that fiercely opposes all manner of government or corporate control over internet resources. How does Cindy view the level of cooperation that Apple was willing to provide?

She believes that it is completely appropriate for Apple to have created technology that takes it out of the equation. She goes on to state, “Technology doesn’t know the consequences of how it will be used”, that once it is created, it could be used by anyone for illegal or even evil purposes.

2.Issue 2 - Ubiquitous as Possible: Max Marlinspike, creator of the Signal App, states, “…that's the idea, to make this stuff as ubiquitous as possible.” Marlinspike also stated, “but the thing about a world where the FBI never misses anything is that's also a world where the FBI has access to everything,” (Al Jazeera English, 2016).

a.According to Marlinspike, what other popular products are using the encryption tools developed for the Signal App?

According to the video, Marlinspike stated that WhatsApp and Facebook Messenger are using the end-to-end encryption developed for the Signal App.

b.What is your opinion on the use of strong encryption for personal communications? Support, oppose, regulate, have a central control or other option?

To be fair I’m rather neutral about this situation. On one hand we are talking about everyday chatting between 2 people and should have nothing to worry about but shouldn’t invade their privacy, so encryption is warranted. On the other hand, many of the applications are used by extremist groups due to chat encryption. So the way I see it, is you take from one to protect another.

c.Which amendments to the constitution relate to the idea of “the FBI has access to everything?”

I could not find any amendment that states that the FBI has access to everything. I did find that we as American citizens are protected under the fourth amendment.  The Fourth Amendment protects people from unreasonable searches and seizures by the government.

This brings us to an interesting act that has been passed called the USA/Patriot Act. One of the most significant provisions of the Patriot Act makes it easier for the authorities, including the FBI, to gain access to records of citizens' activities being held by third parties, such as phone companies, internet service providers, and financial institutions.

3.Issue 3 - Going Dark:

“The challenge we face is that the advent of default, ubiquitous, strong encryption is making more and more of the room that we are charged to investigate, dark,” – James Comey (Comey, 2016)

“We don’t know what we don’t know and what we're missing because of this issue… We have lawful authority to get access to the content” – Sasha O’Connell.

“The vast amounts of data that are collected, don’t suggest a ‘going dark’ problem at all” – Morgan Marquis (Al Jazeera English, 2016)

a.Who do you think has the stronger argument on the “going dark” problem, the FBI agents quoted here who say that law enforcement will be impossible, or Morgan, from First Look Media, who says we have more data than ever?

I think Morgan has a stronger argument in this case that the government has more data than ever. With that being said, we as the public do not know what lengths the government can and will go to collect this data. With all the surveillance in the United States today, going dark is not the problem. The problem will arise when the government can crack encryption of some of the most popular applications/websites. This would cause a lot of panic.

4.Issue 4 - Back Doors = Security Flaws: Two experts are quoted, Bill Marczak and Ted Lieu.

a.Summarize their viewpoint, which is in support of strong, no-backdoor encryption.

Their viewpoint supports a strong, no-backdoor encryption emphasizes how important it is to preserve individual privacy while at the same time enhancing cybersecurity. This would also include maintaining a delicate balance between security imperatives and fundamental rights.

b.What is the opposing viewpoint presented on this issue of backdoor vulnerability?

The opposing viewpoint of those who are in favor of backdoor encryption is that backdoors would compromise the main goal of encrypted services, which is security. Backdoors can lead to potential breaches and make encrypted services less secure. Some even believe that backdoors are counter productive and lead to invasion of privacy.

c.Write a one paragraph summary that contrasts the two points of view presented in the Apple vs. FBI debate. Finish the paragraph by stating which state you support and why.

On Apples side they advocate for strong encryption without backdoors. This further emphasizes the importance of protecting user privacy and data security. The FBI on the other hand argues that law enforcement agencies require access to encrypted devices and communications in order to combat crime and national security threats. Both perspectives highlight the clash between privacy and security. I feel that the more I read about this topic, I am leaning more towards the side of the FBI. There would have to be multiple steps when getting access to such information, but I feel that if someone had done something so horrific and their device is the key that holds the evidence, they should have a way to access it.

References:

6 reasons to be on Apple’s side in its fight against the FBI. (2016, March 2). Ideas.ted.com. https://ideas.ted.com/6-reasons-to-be-on-apples-side-in-its-fight-against-the-fbi/

Al Jazeera English. (2016, October 25). Crypto Wars: Behind the Encryption Debate | Fault Lines [Video File]. YouTube. https://www.youtube.com/watch?app=desktop&v=j7VA4H8m4uk&feature=youtu.be

Comey, J. B. (2016, August 30). The FBI's Approach to the Cyber Threat. Symantec Government Symposium. https://www.fbi.gov/news/speeches/the-fbis-approach-to-the-cyber-threat

Crypto Wars, an upcoming Faultlines documentary on Al Jazeera explores this year’s Apple vs FBI encryption war | Al Jazeera Media Network. (2016). Al Jazeera Media Network. https://network.aljazeera.net/en/pressroom/crypto-wars-upcoming-faultlines-documentary-al-jazeera-explores-year%E2%80%99s-apple-vs-fbi#:~:text=%E2%80%9CApple%20gave%20them%20access%20to