Wright State University

Technology Providers and Personal Security

Alex Yeoh

CS 1000-90

Professor Richter

10 December 2021

Even before the class started discussing the security of electronic devices as one of the weekly discussion topics of *Your smartphone is a civil rights issue*, I had already been thinking on this subject. Due to me having started reading news before being able to vote, the topics I read about tended to skew more towards news about technology and confronting the idea that technology providers may not be protecting my personal information as well as I had assumed. Prior to when the class discussed the topic, I had believed that at least my primary technology provider has been working hard to protect my information; however, I have since changed my stance on that after having read about the failings of my primary technology provider.

Initially, I had believed that my primary technology provider, Apple, was doing all they could to protect my personal information. This belief was primarily predicated on an article I had read about Apple refusing to decrypt a person’s iPhone for the government (Anthony). They had done so on the belief that it would be government overreach and would be dangerous for all Apple consumers if they made a backdoor into their system (Anthony). Although the government was able to break through the iPhone’s security without Apple’s help, I retained my faith that they had at least tried (Farivar).

I have since changed my stance on this matter. During the days that led to the weekly discussion topic on this subject, I had read about Apple’s lackluster bug bounty program. I had read about various instances of Apple not responding to and underpaying security researchers who reported bugs in their system for the bounties they had promised (Salter). I had read about how Apple would have a backlog of bugs they knew about but weren’t fixing and how these issues pushed some security researchers into selling this information to the grey market instead (Salter). All these failings had led me from being hopeful to becoming jaded and doubtful of the lengths that technology providers would go to secure my personal information.

Although initially I would have simply put my faith in some of the technology providers that I believe would safeguard my information, I now know that I need to be more proactive in this matter. I have since decided that simply updating all my systems with the newest security updates would not be enough and am being more careful of what I am downloading and where they come from.

Works Cited

Anthony, Sebastian. “Tim Cook Says Apple Will Fight Us Gov't over Court-Ordered IPhone Backdoor.” *Ars Technica*, 17 Feb. 2016, https://arstechnica.com/gadgets/2016/02/tim-cook-says-apple-will-fight-us-govt-over-court-ordered-iphone-backdoor/.

Farivar, Cyrus. “Feds Break through Seized IPhone, Stand down in Legal Battle with Apple.” *Ars Technica*, 28 Mar. 2016, https://arstechnica.com/tech-policy/2016/03/feds-break-through-seized-iphone-stand-down-in-legal-battle-with-apple/.

Salter, Jim. “Infosec Researchers Say Apple's Bug-Bounty Program Needs Work.” *Ars Technica*, 9 Sept. 2021, https://arstechnica.com/information-technology/2021/09/infosec-researchers-say-apples-bug-bounty-program-needs-work/.

Yeoh, Alex. “Your Smartphone Is a Civil Rights Issue.” *Pilot*, 17 Sept. 2021, https://pilot.wright.edu/d2l/le/607793/discussions/threads/1435273/View.