Carter Hinkle

Dr. Lin

CSCI 415

29 November 2021

# Privacy and Anonymity: Essential Rights

There are two types of people in the world: those who seek privacy for protection, and those who seek privacy for abuse. As computer scientists, we must provide digital privacy and anonymity to those seeking it while preventing attacks from those who abuse these rights. Digital privacy and anonymity must be maintained for the greater good of humanity and to protect our rights as users. In this analysis, I will first discuss the importance of privacy and anonymity. I will then discuss two ways this privacy and anonymity can enable evil, and why it is so important we protect these rights despite the exploits.

First, let us discuss the importance of privacy. Digital privacy helps us stay protected from cyberattacks and scams. When an attacker attempts to gain access to a bank account or other online services, the first thing they will need is information about the user. By keeping that information private, we minimize the risk of attackers hacking into their accounts. Big tech companies are notorious for subtly getting your permission to share data with others. “When you agree to terms and conditions, you often don't just give your data to that specific app - there's a lot of intra-group data sharing.” (Calver, Tom, and Joe Miller). The reason why using these services is free is because you are paying for the service by signing your rights to privacy away. No one should have to make payment in the form of giving up rights. When big companies pass this information around loosely, we end up losing our privacy as a whole. Personal data that is not kept private is also how phishing scams begin. For this kind of scam, all an attacker needs is

an email or phone number to send spam mail. This leads to non-tech-savvy users struggling with identity theft and even the loss of large sums of money.

Second, let's discuss why anonymity is an essential right on the internet today. Anonymity is the reverse of privacy: instead of hiding everything, you want to be heard but without giving away private information about yourself. This is extremely important for allowing people to bring attention to controversial issues without the fear of being tracked. A prime example of this is in the Steubenville, Ohio alleged rape case. "Anonymous was able to recover a video in which a former Steubenville student, described in the video as Michael Nodianos, made several comments and joked about the alleged victim on the night of the alleged rape." (Abad-Santos, Alexander). An anonymous hacking group was able to shine a light on disturbing events that occurred which gave the alleged victim a voice. The leaked videos and information sparked outrage in the community leading to anonymous protests where other victims of similar crimes were able to be heard by the public. Now, let's discuss two exploits of privacy and anonymity.

Apple enables privacy for those who may not deserve it. "The FBI managed to gain access to iPhones belonging to a gunman who killed three sailors at a Florida naval base in December, revealing new evidence that links the shooter to al Qaeda" (Feiner, Lauren). This situation sparked controversy when Apple refused to make information about the terrorist shooter available to the FBI, many claiming that Apple should've complied with law enforcement. Apple was making a point about privacy: if a backdoor is made for the FBI, that door can be misused and exploited by third parties. By Apple refusing to make a backdoor for law enforcement, they are not supporting a terrorist but preventing data leaks and user

exploitation. Apple is showing us they are a company you can trust and will not sell your information even for the largest amounts of money.

Next, cryptocurrencies enable loads of illegal activity and scams, but still, provide value to individuals and our country as a whole. A clear example of this is the Dark Web: “The Dark Web may be used by people wishing to carry out illegal activities online, such as selling weapons or drugs.” (Ceop). The use of the dark web combined with an untraceable currency is an obvious exploit of anonymity. Users can use a Tor connection to access parts of the web anonymously to do extremely illegal things. Another exploit to currency anonymity is the act of rug pull scams. Many popular YouTubers gain the trust of their followers to get them to buy into a coin so the value goes up and then they sell when they least expect it. This happens quite often and is just a result of allowing this freedom. The best we can do to prevent these scams is to educate users about common scams. So why even allow anonymity through cryptocurrency? As the US dollar becomes more and more volatile, people are finding more hope in coins that could potentially solve our inflation issues in the US. While cryptocurrency and anonymous transactions may not have much current use at the moment, it is an exciting technology that could solve many problems in the future.

To summarize, we have examined the importance of privacy and anonymity rights in the digital age. Lastly, we discussed privacy exploits through the Pensacola shooting and anonymity exploits through cryptocurrency. It is clear through these examples that although bad things occur as a result of having freedom, many problems are eliminated by allowing privacy and anonymity such as preventing identity theft and protecting our citizens’ assets. It is clear that the positives outweigh the negatives for these essential rights and as computer scientists, we must protect these freedoms for the consumer.

# Works Cited

Abad-Santos, Alexander. “Inside the Anonymous Hacking File on the Steubenville 'Rape Crew'.” *The Atlantic*, Atlantic Media Company, 30 Oct. 2013, https://www.theatlantic.com/national/archive/2013/01/inside-anonymous-hacking-file-steubenville-rape-crew/317301/.

Calver, Tom, and Joe Miller. “What Tech Giants Really Do With Your Data.” *BBC News*, BBC, 5 July 2018, https://www.bbc.com/news/business-44702483.

Ceop. “The Dark Web: What Is It and Why Do People Use It?” *Thinkuknow*, Crown Copyright, https://www.thinkuknow.co.uk/professionals/our-views/the-dark-web/.

Feiner, Lauren. “Apple Refuses Government's Request to Unlock Pensacola Shooting Suspect's iPhones.” *CNBC*, CNBC, 14 Jan. 2020, https://www.cnbc.com/2020/01/14/apple-refuses-barr-request-to-unlock-pensacola-shooters-iphones.html.