Zac Foteff

Dr. DePalma

CPSC 353: 01

21 February 2021

Protecting Encryption in the Age of Information

The rapid onset of the information age has presented the United States with many difficult challenges that must be addressed to preserve the security of the nation's people. After the January 6th U.S. capitol riots, much attention was placed on the effect that social media services like Facebook, Twitter, Parlor, and others had in disseminating misinformation to their users that ultimately resulted in multiple causalities and one of the darkest moments in the history of the United States. In the article "*Are Encrypted Messaging Apps the Next Misinformation Hotspot*?", the authors raise two concerns that need to be addressed in order to prevent events like the capitol riots from happening again. The first concern that needs to be considered is the need for consumer privacy. Citizens of the United States enjoy unfettered freedom to express their ideas while retaining the liberty to create their own path in life. The constitution of the United States asserts that no law should ever infringe on or abridge the rights of American citizens. Yet, with the rise of social media many citizens are voluntarily opening their defenses to these Social media companies that extract every possible piece of data that they can collect from every user. Shoshana Zuboff, professor emeritus at Harvard Business School, remarks on the data collection efforts of big tech companies in her opinion piece *"The Coup We Are Not Talking About"* stating that "Surveillance capitalists…claim the authority to decide who knows by asserting ownership rights over our personal information and defend that authority with critical information systems and infrastructure.". Zuboff helps illustrate in this quote that these surveillance capitalists assert ownership over property that cannot belong to them and protect that assertion by lining the pockets of those in power -- like the 50% of the US Senate in 2018 that received a donation from Facebook, Google, or Amazon – and by retaining a very close grip on their proprietary content algorithms that display content to users. New social media and communications applications such as Signal and Telegram offer a solution with privacy, but it is

important to ensure that these new applications avoid the pitfalls that big tech has fallen into. Signal and Telegram offer end-to-end encryption, allowing for almost complete security for user's communicating with each other. While this helps resolve the issue of consumer privacy, there still exist concerns that the privacy these apps offer will create breeding grounds for extremist ideas. We have seen a similar phenomenon to this during the time of the capitol riots with the right-wing app Parlor, which catered exclusively to extremist beliefs and fringe conspiracy theories. Should another app such as Parlor be created that allows for secure encrypted conversations, there is nothing any government body can do to prevent these ideas from coming to fruition other than simply reacting when they do. Encryption is important for allowing citizens to retain control over their personal information, however, it is important to recognize the inherent risk that comes with allowing secure instantaneous communications as the country decides how to regulate these social spaces.