Thesis Project Portfolio

OPAQUE: Protecting User Data during Server Breaches
(Technical Report)

The Ethics of Mitigating Social Media Addiction with Governmental Regulation
(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Maven Kim
Spring, 2023
Department of Computer Science

Contents of Portfolio

Executive Summary

OPAQUE: Protecting User Data during Server Breaches
      (Technical Report)

The Ethics of Mitigating Social Media Addiction with Governmental Regulation
      (STS Research Paper)

Prospectus

Executive Summary

The Internet is ubiquitous in the United States. It is deeply incorporated into its institutions and used by millions of its citizens, ranging from students to company employees. Although the Internet provides many advantages, such as the ability to store large amounts of information and to connect with people around the world, these benefits come with problems that must be addressed. Two such problems are data security and addiction to social media applications. Many companies store user data for an innumerable number of purposes, such as payments, personalization, marketing, and security. These companies must protect this data from bad actors who try to gain unauthorized access. One such method involves designing a system where user passwords are never sent in plaintext to a server and data is encrypted and unreadable even if it is stolen. Companies also can use user data to personalize online experiences and create web applications that attract and retain attention. This is a common practice among social media platforms, which can have addictive consequences. Given how widespread social media is, I argue that the United States government should play a larger role in investigating the addictiveness of social media and devising solutions for this problem.

My technical project involved creating a basic prototype implementation of the OPAQUE protocol. This protocol is designed to protect user data in the event of a server breach, to hide passwords from the server to prevent them from being accidentally stored, and to be robust even when users use weak passwords. Since data breaches can lead to devastating consequences, such as financial loss and a loss of trust in the company that was hacked, companies must preemptively strengthen their security protocols. The OPAQUE protocol is one such way to strengthen database security. I worked with one other intern to create a simple command line user interface with basic user registration and authentication capabilities backed by the OPAQUE

protocol. This prototype used Amazon Web Services (AWS), Python, and Docker, and was demoed to the entire AWS Cryptography team. In the future, other AWS employees can scale this prototype so that it can support multiple servers and can upgrade the user interface to be more user-friendly.

My STS Research Paper examines the current role of the United States government in regulating the addictiveness of social media platforms, as well as whether it should be responsible for addressing social media addiction and its consequences. Social media platforms use strategies such as intermittent variable rewards, the removal of stopping cues, and the targeting of people's need for social validation. These tactics can cause addiction, which can lead to symptoms of depression and anxiety and can take away time from important areas of life, such as school, work, socializing, and sleep. Governments can address social media addiction by utilizing a concept called nudging, which guides people's behavior towards certain decisions without prohibiting them from making other choices. Nudging serves as a compromise between libertarianism, the complete freedom of choice of an agent, and paternalism, which involves a government making decisions on behalf of its citizens. The government has the responsibility to address social media addiction because absent a reason to do otherwise, social media companies will not reduce the addictive harm of their platforms since they directly profit from increased user retention. Additionally, while social media platforms target unconscious cognitive processes to retain users, governments can use behavioral science principles to target active cognitive processes. This enables individuals to truly decide for themselves whether to continue usage of social media applications.

My projects provide a good starting point for both creating a working prototype of the OPAQUE protocol and examining the governmental role in regulating social media addiction.

However, my work in its current state is only a starting point. My OPAQUE prototype needs more rigorous testing and benchmarking so that performance bottlenecks and security vulnerabilities can be identified. Other developers can also add functionality to support multiple users registering and authenticating at the same time. Additionally, to enable seamless integration of the OPAQUE prototype with other companies' services, my project must be combined with a service such as AWS Cognito. This would allow companies to use the OPAQUE protocol at scale without downloading any code or configuring my implementation with their services. Also, although I argue that the United States government should play a role in regulating social media addiction, I do not discuss the specifics regarding how it should go about doing this. Other researchers can identify effective ways of addressing social media addiction, such as the incorporation of reminders that alert users to their social media usage.