Thesis Portfolio

E2-Chat: A Web-Based End-to-End Encrypted Messaging Service
(Technical Report)

The Limitations of Consumer Data Agency Under the California Consumer Privacy Act
(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

Ashwin Pathi
Spring, 2021

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Internet data collection has made corporations and society more productive, but at the expense of individual privacy and control over personal data. Public perception regarding data privacy has slowly gained prominence in public discussion, especially in the wake of recent data privacy and security incidents. As such, many new technologies have sought to build their product with end user privacy in mind by using techniques such as end-to-end encryption.

The technical portion of this paper aims to create a fully end-to-end encrypted web messaging service that is easily accessible on a myriad of devices, and supports the transfer of a variety of file types. The app, called E2-Chat, would fill a niche not supported by other end-to-end-encrypted messaging applications, which rely on the usage of an auxiliary mobile device. E2-Chat, uses end-to-end encryption to ensure that only the devices of the end users of the service have the ability to decrypt content, meaning the server does not have access to any user-generated content. This would prevent administrators of the messaging server and potential third parties from parsing user messages. This would preserve user privacy, while still providing a service with all the key components of a modern chat application.

The sociotechnical portion of the paper aims to analyze how privacy legislation in the California Consumer Privacy Act (CCPA) may have fallen short of allowing consumers to have more agency over their internet data. The Social Construction of Technology (SCOT) is used to analyze how the first iteration of the CCPA was formed, and to elucidate how various key social groups ascribed their meaning of privacy into the legislation. From this analysis, the paper discusses how privacy issues brought up by the CCPA's legislative process can be mitigated,

how legislation can be improved moving forward, and the implication of enhancing data privacy for end users.

Both the technical and sociotechnical projects focus on enhancing user privacy and data protection. The technical portion of the project focuses on how privacy can be practically and technologically implemented, and to show that privacy conscious technology can be as accessible as normal internet services. However, full end-to-end-encryption is not viable for all types of internet services, and in cases where data is not guaranteed to be inaccessible by third parties, consumers should be aware of what information is being collected on them. The sociotechnical portion of the paper discusses this aspect of privacy, specifically through the analysis of the CCPA and the legal ability of consumers to handle their own data. Both the sociotechnical and technical aspects of the project allowed me to learn about the shortcomings and advantages of current legal and technological privacy solutions.