Thesis Portfolio

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

Framing Public Policy for Internet Data Privacy
(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

Saiteja Bevara
Spring, 2021

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

The popularity of the internet and the development of new technologies and communication tools has allowed for the rapid growth of internet data. Along with the growth in the amount of data has come concerns over protecting this data, particularly following revelations of its misuse such as the Cambridge Analytica scandal. This thesis explores the issue of protecting internet data from both a technical perspective and a social one. The technical project involves the creation of a web-based end-to-end encrypted messaging platform (E2-Chat). The research paper discusses the issue of framing comprehensive internet data privacy policy in the United States.

The technical project, E2-Chat, is a complete web-based end-to-end encrypted messaging platform. End-to-end encryption (E2EE) allows for the encryption of content during communication, such that content is only readable by communicating parties. E2EE services are especially relevant today as communication platforms such as social media messaging services are a large contributor to the growth of internet data. The majority of these messaging services do not offer E2EE, or are only mobile-based services which excludes those without smartphones from encrypted communication. E2-Chat implemented a completely web-based messaging service that allows users to communicate with others on the internet without fear of third parties accessing their messages.

The research paper discusses the issue of framing public policy for internet data privacy. There is currently a lack of comprehensive data privacy legislation in the United States. However, internet data as a technology is shaped by many social groups in individuals, companies, and governments. This paper analyzes how internet data is shaped by these social groups using the Social Construction of Technology (SCOT) framework. Then, the GDPR is

analyzed from a SCOT lens as example legislation to understand how it affects each of the relevant social groups that interact with internet data. This analysis is used to discuss how the US can proceed in crafting data privacy legislation, and the likely direction of privacy moving forward.

These two projects in conjunction are beneficial in researching how to protect internet data. From a technical perspective, technologies such as E2EE services provide one avenue to increase data privacy for individuals as their messages become encrypted and thus only readable by those in direct communication. However, delegating all data privacy to technological solutions is not practical and cannot be guaranteed, and thus policy is a necessary complement. Policy specifically related to E2EE services is also a concern, as some argue for technological workarounds into encrypted communication called backdoors to be a legal mandate for national security reasons. Understanding how data privacy policy can be appropriately formulated is necessary to create a fair internet data environment for all stakeholders in ways that technology cannot. Therefore, completing both these projects together allowed for valuable insight into how technology and policy can provide varying approaches to the common goal of protecting internet data.