Thesis Project Portfolio

The Multi-Arm Bandit Problem in the Federated Context

(Technical Report)

Consumer privacy effects on the momentum of the social media

(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

Aaron Parson

Spring, 2024

Department of Computer Science

Table of Contents

Executive Summary

The intense use of social media platforms and information technology has increased the value of privacy in the modern age. These research papers dive into two distinct yet interconnected domains of privacy: Federated Learning (FL) in machine learning and the impact of consumer privacy on social media platforms. FL, a distributed system addressing challenges like data sharing, privacy concerns, and infrastructure costs, is investigated within the context of the Multi-Armed Bandit problem (MAB). FL operates by distributing machine-learning models across client devices, sending updates to a central server for aggregation. The MAB problem aims to identify the most rewarding slot machine while minimizing regret. Placing MAB within an FL framework allows for information sharing among players, which enhances privacy in a distributed recommending system. Additionally, the paper explores how consumer privacy affects social media platforms, focusing on Facebook and TikTok as case studies. By employing Thomas Hughes' technological momentum framework, the study highlights how privacy concerns shape the trajectory of these platforms with societal demands and regulatory pressures. Both of these topics have major relevance to the concept of privacy and its effect on people. One discusses a privacy-enhancing technology that maintains the desire for increased information. The other discusses how social media technologies are affected by the desire for privacy.

The research paper investigates the application of Federated Learning (FL) to address challenges in machine learning, including data sharing, privacy concerns, and infrastructure costs while enhancing data diversity. Specifically, the study focuses on the Multi-Armed Bandit problem (MAB) within an FL context. FL operates as a distributed system where client devices run local machine-learning models on their data, sending updates to a central server for aggregation. The MAB problem aims to identify the slot machine with the highest true reward while minimizing

regret. Placing MAB in an FL context enables information sharing among players, creating a distributed recommending system that better protects privacy. The project involved a comprehensive literature review, evaluation of the Intel federated machine learning (FML) package, and implementation of the distributed linear Upper Confidence Bound (UCB) algorithm within the FedML platform. The outcomes of the projects indicate the need for the algorithm's successful integration and further validation and scalability testing. Related works explore FL's potential in medical imaging and address security concerns such as data poisoning attacks on federated machine learning networks.

The research paper explores the impact of consumer privacy on the momentum of social media platforms, focusing on Facebook and TikTok as case studies. Using Thomas Hughes' technological momentum framework, the study analyzes how privacy concerns influence the trajectory of these platforms. It examines how societal demands and regulatory pressures related to privacy have shaped the evolution of Facebook and TikTok. The results suggest that while government responses have attempted to regulate these platforms, technological momentum often prevails, leading to continued innovation and growth. The paper highlights the complexity of technological advancement, regulatory frameworks, and consumer preferences in shaping the trajectory of social media platforms and their impact on digital privacy. It concludes by discussing the importance of collaboration between policymakers, technology companies, and consumers to address privacy challenges and align technological evolution with societal values.

By delving into Federated Learning (FL) in machine learning and examining the impact of consumer privacy on social media platforms concurrently, I gained a holistic understanding of privacy-related issues spanning different domains. Firstly, exploring FL within the context of the Multi-Armed Bandit (MAB) problem gave me an appreciation for the intricacies of distributed

systems and privacy-preserving techniques in machine learning. By implementing the distributed linear Upper Confidence Bound (UCB) algorithm within the FedML platform, I gained practical experience in addressing challenges such as data sharing, privacy concerns, and model aggregation. This hands-on approach complemented the theoretical understanding gained from the literature review, enabling me to grasp FL's potential applications in diverse domains like medicine, advertising, and finance. Moreover, its susceptibility to security threats like data poisoning attacks has helped me understand the future needs of FML networks. Simultaneously, analyzing the impact of consumer privacy on social media platforms using Thomas Hughes' technological momentum framework provided a broader perspective on privacy dynamics in the digital age. By focusing on Facebook and TikTok as case studies, I discerned how societal demands, regulatory pressures, and technological innovation interact to shape the trajectory of these platforms. This analysis presented the importance of balancing privacy concerns with the imperative for technological advancement and user engagement. Juxtaposing these two projects revealed parallels and contrasts between privacy-enhancing technologies like FL and the privacy challenges inherent in social media platforms. While FL uses distributed systems to enhance privacy and data diversity, social media platforms often face scrutiny regarding their data practices and privacy policies. Understanding these features deepened my appreciation for the complexity of privacy issues and the multifaceted approaches required to address them effectively.