Thesis Project Portfolio

Machine Learning: Use ML Models in Helping Garbage Classification in Virginia

(Technical Report)

The Ethical Implications of User Data Privacy in Web Development

(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

Hanzhang Zhao

Spring, 2024

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

This research is to discuss the increasingly pertinent issue of user data privacy within the realm of web development. It is an area of study that lies not only between technological advancement but also between ethical responsibility. In essence, the study has sought to answer the question of how developers can build web applications that ensure the user data privacy of the respective organization without compromising either the cost of the procedure or its functionality. This question is motivated by increasing social and academic concern over the exploitation of private information in the digital era, characterized by too frequently data breaches which really worn out people's trust in digital platforms.

Based on a systematic literature review and case studies that include, but are not limited to, the difficulties of Oslo Analytics in complying with GDPR, this study adopts a mixed-methods approach. It looks into the current landscape in data privacy, insisting that a paradigm shift is needed to make to the adoption of more rigid ethics in web development. That will include the review of the current available privacy protection tools, ethical framework, and setting up the framework of Cost-Effective Privacy-focused Development Lifecycle (CEPDL). In this approach, the CEPDL framework will marry the cost-effective methodologies with the best practices of the industry to strive to embed data privacy within the software life cycle.

After the review of the current available privacy frameworks, the results, unfortunately, show that there is an obvious yawning gap between the available mechanisms of data protection and the ethical standard recommended in ideal terms and those recommended by academic and philosophical discourses. At the same time, serious vulnerabilities in the technological, conceptual, and legal aspects of privacy protection continue to persist despite the elaboration of appropriate tools and directives, including the notorious GDPR. The case of Oslo Analytics, therefore, vividly denotes the very practical challenges of aligning big data analytics with very strict privacy laws, highlighting innovative solutions that do not compromise data utility for research and development.

As concluded by this analysis, the CEPDL framework offers a viable way forward in balancing the need for strong data protection with the realities of modern web development. It implies that developers can create more secure and trusted digital environments if the considerations are imbued from planning to deployment processes. This approach looks at not only what is required by law but also a culture of ethical responsibility and user empowerment in the digital domain. Furthermore, the research suggests that it's crucial to increase user awareness and cybersecurity education, since users play a key role in a comprehensive data privacy strategy. This entails raising public awareness about digital risks and protection measures, enabling individuals to effectively safeguard their personal information and enhance overall web application security.

There is hence a call through this paper for there to be further research on the integration of ethical consideration in practice while developing applications that are user-centric, like social media and the rest. It puts an argument that a collective effort of the developers, policymakers, and users' community is important for forging a digital future with core values of privacy, security, and ethical responsibility.