Android Development for an e-Commerce Company

General Data Protection Regulation Impact on Small to Medium Sized United States Based Enterprises with European Union Users

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Parul Goswami

Friday, October 27th 2023

Technical Team Members: Parul Goswami

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

MC Forelle, Department of Engineering and Society

Briana Morrison, Department of Computer Science

Introduction

In a world where technology is advancing and the internet continues to be highly connected, maintaining privacy and ownership of one's data becomes increasingly difficult. From comprehensive cookies to data privacy leaks, to the selling of one's data collected by a third party company sold for advertising purposes, there is a growing concern amongst consumers of technology around the ability to safeguard their data – or at the very least consent to its use. Internationally, legislation has emerged with the intent of helping this growing subset of society protect their own data. The General Data Protection Regulation (GDPR) for residents of the European Union (EU) is a legislation of interest helping users gain more autonomy in how their personal identifiable data is stored and kept by entities (Marini et al., 2018).

In effect since May 25th, 2018, GDPR is one of the most comprehensive data protection policies in the world, aiming to protect individual's personal data by applying to businesses that collect said data on or offline (Marini et al., 2018). Since the regulation applies to all EU residents, companies operating internationally such as e-commerce companies offering their goods and services are also required to abide by these constraints (Singh, 2020) . Especially for companies with a primary influence in the United States of America and Canada but with a growing interest in and transition into the EU, these constraints can be difficult to manage as they are geo specific. Especially since such extensive data protection regulations are not present within the United States to the same extent, other than the California Protection Act which provides different coverage and consequences, having to offer different data protection policies based on different geographic regional operations can be intensive for certain companies with limited resources such as small to medium sized enterprises.

The research question of interest for this portfolio is: how does GDPR compliance uniquely impact United States based small to medium sized businesses that have a presence in the European Union? ? For my technical project, I will discuss work I did during my past internship this summer as a mobile app engineering intern for a particular e-commerce company. My STS portion will dive into one of the tickets I took on during this internship, tying my technical and sociotechnical project together only through this past ticket.

Technical Topic

During the summer before 4th year, I interned with a prominent, US-based international E-Commerce company that specializes in home goods based in Boston, Massachuesetts. There, I interned as an android app engineering intern, working on their codebase on bug and feature fixes that are deployed to their main and specialty retail brand apps, servicing as many as 22.1 million users.

In general, e-commerce companies utilize three main customer-facing avenuesfor customers to purchase their products: their website from a typical machine like a computer (Web), their website from a mobile device (mWeb), and their app from a mobile device (app). To encompass changing regulations, requirements, research, and products, changes on the app must be fast, effective, and comprehensive to maintain customer demand, especially during in-app promotional periods like holiday sales (for example, Labor Day Sale). To satisfy these requirements, the company's technology division used Agile methodology, a project management technique with an emphasis on doing work in short periods (Coursera, 2023), working in sprints.

As an intern working on the company's android app, I had to balance stakeholder interactions with backend engineers, international geos geams, UI/UX designers, and IOS

engineers on my team to make sure progress developed on the android app was in parity with the company's IOS version. Tickets represented portions of work that were do-able for the software developer with the task within the sprint.

Tasks/tickets I took during my time as an intern were smaller bug fixes associated with app localization needs, GDPR requirements, and a larger project associated with fixing the Write a Review Page. Language localization is associated with the process of adapting a product's translation to the user's country or region, accounting for differences in different geographical markets (Ishika & Miller, 2005). The company I interned for has a presence in the United States, Canada, Ireland, Germany and the United Kingdom, requiring language translations for French-Canada, English-Canada, United States, German, Irish-English, and United-Kingdom-English. I conducted said translations using an internal localization tool to ensure the text present within the app was properly associated with intended cultural context and meaning.

One such translational tool usage was for a GDPR ticket. The specific string displayed for particular products was "excl. delivery and handling", linking to a new page that would detail the exclusions that applied to a product. In non-North American regions, there was no mention of 'handling' of the product in the secondary page the string sends the user to. Since the intent of GDPR is for data and fee transparency, the removal of 'handling' was important as the linked page failed to mention it in the non-North American regions.

My solution to the given ticket revolved around running the internal translation task differently based off of the geo the app was being run in, and was coded in android's native language, Kotlin. Major outcomes included an App page modification to comply with General Data Protection Regulation compliance (GDPR) and fixed image upload functionality for the App's 'Write a Review' Page. Future work includes further learning android app development to

move on to more advanced tickets related to refactoring old modules present within the codebase.

This project relates to the sociotechnical project of GDPR compliance within small to medium sized enterprises based in the United States but with a presence in the European Union in that both are related to the GDPR regulation. While the technical project related to deliverables in maintaining functionality and driving profits for the company I interned for's profits, my STS project is to investigate how GDPR uniquely impacts small to medium sized enterprises based in the United States but with a presence in the European Union while maintaining compliance with European Union users' data.

STS Topic

GDPR has uniquely impacted businesses and institutions within the European Union, and companies operating in the European Union with its strict regulations highlighting user privacy. Comprised of 99 articles and 173 recitals, some authors have analyzed the contents of the regulation to distill its essence in three distinct facets: lawful processing, data user's rights, and data controller's obligations. Each of these buckets relate to at least two of the principles of GDPR: legitimacy, proportionality, empowerment, transparency, accountability, and security (Irwin, 2022).

Looking deeper into the regulation, it becomes apparent how wide the definition 'data controller' is, and how it does not just limit itself to profit seeking entities like companies and institutions. One lesser known group affected by GDPR is researchers. Researchers working with biometric, genetic, and other personal health data fall under GDPR compliance (Chassang, 2017). In general, researchers working with human subjects and thus data points that may contain personal identifiable information must be under compliance with GDPR, specifically in

data wrangling methodologies to include pseudoanyomization or anyomization to protect the individual's data and still glean research results (Crutzen et al., 2019). Many reports have already been released on methodologies that can be used to pseudo-anonymize personal identifiable data, one case study including techniques that have been used on mobile device information (Štarchoň & Pikulík, 2019). Researchers can work under a variety of institutions from political advocacy groups to institutions, with varying sizes and resources available for them to remain compliant under these data controller specific aspects of the regulation, and as such, can be considered small to medium sized enterprises based on their circumstances.

Rather than only affecting internal business and institutional practices internally in terms of protecting a user's data, GDPR has forward, public-facing impacts on a business. When a business goes public, other individuals may obtain stock of the company, investing in the company's progress and potentially reaping the benefits if the company does as well as it claims. GDPR impacts a company's investment risk disclosure as companies define direct and indirect ways GDPR compliance affects their business (Wong et al., 2023).

In general, the advent of GDPR and the consequent requirement for affected companies to remain compliant has had widespread affects on companies of all sizesCompliance requires major data changes and reworking to internal and customer facing infrastructure that larger companies have the resources to dedicate towards compliance that smaller enterprises lack (Brodin, 2019). Thus, many authors have developed frameworks to help smaller data controllers effectively reorganize their institutions.

In my STS Topic, I will explore how GDPR legislation uniquely impacts small and medium sized businesses that are based in the United States but have operatings in the European Union while still maintaining privacy of a user based in the European Union's data. Specifically,

I will be exploring the various concepts discussed above in context of how artifacts, even regulations, have politics and the techno-regulatory imaginary of privacy engineering.

Research Questions and Methods

To answer the STS question, how does GDPR compliance uniquely impact United States based small to medium sized businesses that have a presence in the European Union?, I intend to look at technical papers, publicly facing company documentation and articles, the GDPR in its entirety to gain an understanding on how United States based companies are affected by the regulation. I will also utilize any research studies I find analyzing the regulation and the regulative's different frames of impact For company specific documents, I will do broad research on which companies have an international European presence with a deciding upon boundary to filter through which companies to research to narrow down which companies I will look into more extensively to find their stance and any publications about GDPR they may have. Ideas on possible metrics for me to evaluate when deciding to research a company or not include viewing the company's revenue and number of employees. For all the resources I intend to look at, I expect them to be in anticipation of GDPR's release (before 2018 by a few years) to today as the policy is still in effect. I will look at articles before GDPR's official release as there was a lot of discussion and articles created in anticipation of the legislation's official release that still contain pertinent information helpful to information gathering.

To make sense of the information I will be gathering, I will make use of stechno-regulatory imaginaries of privacy as seen by the GDPR policy decision in the European Union(Rommetveit & van Dijk, 2022) and how artefacts have politics by Winner (Winner, 1980). In general, privacy is considered a techno-regulation which is "the conscious deployment of technology to regulate people's behavior" (Rommetveit & van Dijk, 2022). The techno-

regulatory imaginary theory will help establish the advent of GDPR and its particular reinforcement of data protection for individuals present within the European Union, even if a company is not based in the European Union, and how, like imaginaries, privacy is becoming a fundamental right that is going to be part of the future (Rommetveit & van Dijk, 2022). The theory on how artifacts have politics will help me establish that apparent politics to GDPR and how that uniquely impacts small to medium sized businesses based in the United States.

Conclusion

My technical project was successfully deployed into production on the company's app. Users of the company's android app see the appropriate 'delivery' text if they are based in the Ireland, United Kingdom, or Germany. Additionally, android users of the app, if they have purchased a product from the company, can successfully upload a product image, upload many product images, and delete said images with the thumbnail remove button on the Write a Review Page. My STS project aims at understanding the impact on United States based small to medium sized companies who have a presence in the European Union and must abide by GDPR compliance. I hope that my project will help in the European migration/integration work that many companies may pursue if they are interested in broadening their user base internationally in Europe. Overall, I hope my findings and analysis will help to build more information on the implications of European expansion in terms of GDPR compliance.

Works Cited

Brodin, M. (2019) A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. *Eur J Secur Res* 4, 243–264.https://doi.org/10.1007/s41125-019 00042-z

Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. *Ecancermedicalscience*, *11*. https://doi.org/10.3332/ecancer.2017.709

Coursera. (2023, July 27). *What is agile? and when to use it*. https://www.coursera.org/articles/what-is-agile-a-beginners-guide

Crutzen, R., Ygram Peters, G.-J., & Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. *Psychology & Health*, *34*(11), 1347–1357. https://doi.org/10.1080/08870446.2019.1606222

Irwin, L. (2022, April 27). *The GDPR: Understanding the 6 data protection principles*. IT Governance Blog En. https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles

Ishida, R., & Miller, S. K. (2005). *Localization vs Internationalization*. Localization vs. internationalization. https://www.w3.org/International/questions/qa-i18n

Marini, A., Kateifides, A., Bates, J., Zanfir-Fortuna, G., Bae, M., Gray, S., & Sen , G. (2018). *Comparing privacy laws: GDPR v. CCPA*. Future of Privacy Forum. https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison Guide.pdf

Rommetveit, K., & van Dijk, N. (2022). Privacy engineering and the Techno-Regulatory Imaginary. *Social Studies of Science*, *52*(6), 853–877. https://doi.org/10.1177/03063127221119424

Singh, N. K. (2020, February 6). *What you need to know about the CCPA and the European Union's GDPR*. American Bar Association. https://www.americanbar.org/groups/litigation/committees/minority-trial lawyer/practice/2020/what-you-need-to-know-about-the-ccpa-and-the-european-unions gdpr/

Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones. *Procedia Computer Science*, *151*, 303–312. https://doi.org/10.1016/j.procs.2019.04.043

Wong, R. Y., Chong, A., & Aspegren, R. C. (2023). Privacy legislation as business risks: How GDPR and CCPA are represented in technology companies' investment risk disclosures. *Proceedings of the ACM on Human Computer Interaction*, *7*(CSCW1), 1–26. https://doi.org/10.1145/3579515

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1), 121 136. http://www.jstor.org/stable/20024652?origin=JSTOR-pdfLinks to an external site.