Class Management System for the Staunton Makerspace
(Technical Paper)

The Need for Federal Privacy Laws
(STS Paper)

A Thesis Prospectus Submitted to the
Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia
In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Pranay Dubey
Fall, 2019

Technical Project Team Members
Damon Cestaro
Hunter Williams
Kane Lee

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

Signature Pranay Dubey Date 12/12/19
Pranay Dubey

Approved Ahmed Ibrahim Date 12/11/2019
Ahmed Ibrahim, Department of Computer Science

Approved Date 12/14/19
Thomas Seabrook, Department of Engineering and Society

Introduction

Since the creation of the World Wide Web, organizations across the spectrum have been racing to adapt their strategies with respect to how they provide services to customers. On one end, government entities have been able to convert many of their operations from physical to electronic (Violino, 2018). Large corporations are similarly able to solicit and satisfy customer needs online. On the other end, small non-profit organizations are able to spread awareness, reach communities, and organize themselves with the use of email, social media, and their own websites. With sensitive data being trafficked over the internet *en masse*, adequate legislation and security measures should be in place to ensure user privacy is not compromised and user data is not used without prior consent. Despite being a global leader in internet based companies and services, the United States lacks explicit federal legislation to protect these rights (Brooks, 2019). If the United States wishes to protect its constituents from having their personal data harvested and used without consent, the federal government will have to bring about new legislation directly addressing these issues.

The STS research will consider the current political and technical landscapes as they relate to the federal government, individual states, and foreign entities. The findings will be used to analyze potential actions to be taken by the federal government and the effects they would have on industry. While not directly related to the STS Research Paper, the Technical Report focuses on an example of a smaller organization benefiting from the modernization brought about by the internet. The report will detail the process whereby a new system for organizing, managing, and joining classes is created for the Staunton Makerspace, located in Staunton, Virginia. As it exists now, the system is outdated, rigid, and inefficient. The final product will

free up resources and streamline the process by which members join the community and maximize the utility the makerspace offers.

Class Management System for the Staunton Makerspace

The Staunton Makerspace will benefit significantly from a new class management system. Makerspaces are collaborative work spaces, often with a variety of technical and maker equipment, where people can come and learn new skills or pursue their own projects. The makerspace's current system is old-fashioned and outdated. Development and implementation of a new system will improve several areas of the Staunton Makerspace's organization and management. Specifically, the main issues being addressed are the process of registration with the makerspace and sign-up for classes. If a community member wanted to register at the makerspace or sign up for a class with the current system, they would have to physically be at the makerspace and find the volunteer responsible for handling registration and sign-up.

However, hidden beneath this issue is another layer of complication that leads to inefficiency. The makerspace has a variety of machinery that requires training to use. In order to keep track of the training members have received, organizational structures called "guilds" were created, with each guild focusing on a certain skill set and the implication that members of a guild are trained on the machines used for that particular skill set. Currently, a volunteer must manually check that an individual trying to add a class is a member of the relevant guild before the individual can be added to the class. Moreover, once a member registers and enters class, their standing within the class is not readily available to them, making it difficult to track their own progress and growth.

To address these issues and improve efficiency at the makerspace, the incoming system will be a web portal accessible by all members and prospective members of the community. Under this new system, members will be able to register and sign up for classes from their own accounts. Volunteers will not need to manually add people to courses, manually confirm if a member has the necessary training, or even worry about class size. All of this information will be implemented within the system, thus automating it and freeing up volunteers to engage more with the community and undertake fewer menial tasks. Additionally, members will be able to track their performance in a class and receive instructor feedback directly through the portal system as well, thus maximizing what they get out of the makerspace.

The web portal will be developed using Django, a python-based web framework. Such frameworks provide a template for different components needed for web-based applications, allowing developers to focus on adding features and functionality. All relevant data and relationships, such as guild membership, will be stored in a database and processed when required by scripts within Django. The framework is modular and allows for modifications to be made to page functionality and the addition or removal of existing pages to be done without needing to restructure the rest of the project significantly. Furthermore, since Django is python-based, the portal can be easily hosted on most servers. The final product will create a more dynamic workflow for the Staunton Makerspace, freeing up resources and facilitating the continued growth and development of the makerspace community.

The Need for Federal Privacy Laws

The concept of technological determinism focuses on the idea that once a society creates and adopts technology, technology goes on to shape society. Though once widely accepted, the

mid-20th century saw an increase in skepticism surrounding the theory of technological determinism, and leading scholars began to turn on the theory. In 1992, Andrew Feenberg wrote his article "Subversive Rationalization: Technology, Power, and Democracy," in which he shows the claim that technical decisions are bound by "rationality" to be groundless. That being said, technological determinism can be used to illustrate certain relationships and proves to be useful in this analysis. Most notably, the way the internet continues to shape the lives of most Americans exemplifies technological determinism. If citizens continue to push for improvements to the internet and to the ways in which their data is handled, then the model changes from technological determinism to technological momentum. Technological momentum, a variant of technological determinism and as defined by Thomas P. Hughes, "infers that social development shapes and is shaped by technology" (Hughes, n.d.). As the government begins to act on the wishes of American constituents regarding their online privacy, the model described by technological momentum will illustrate the dynamic that exists between the internet, internet service providers, and users. The framework provided by technological momentum will thus be used to analyze the ongoing cycle of how the internet affects constituents, the reactions and effects felt by those constituents, and how these are in turn used to further guide the development of technologies used over the internet.

User data privacy has become a significant issue in American society today. This is especially true regarding IT companies, which claim ownership of user data as well as the ability to store, access, and sell any information posted using their services (O'Connor, 2018). Recent controversies, such as the Equifax data breach of September 2017 and the Cambridge Analytica scandal of 2018, have shown how much data companies have accessible to them as well as the risks associated with having access to that data. This gives rise to a predicament; companies

reserve the right to preserve and use data as they please if individuals agree to use their services, thus leaving them vulnerable to any breaches those companies may face. Certain state governments have begun trying to address these issues to protect their own constituents. California passed the California Privacy Rights and Enforcement Act, for which enforcement is to begin on January 1, 2020 (Quinn, 2019). New York attempted to follow suit with the New York Privacy Act, which failed to pass (Brooks, 2019; Ropek, 2019). There is still a very large gap left where the federal government should be implementing legislation for unification and creation of consistent data privacy legislation across the country. A patchwork of separate, and more likely than not, unequal data laws throughout the states will make enforcement of said laws more difficult (Gregersen, 2019; Schryver, 2019). Additionally, a scheme with competing laws will lead to inconsistencies across states, thus diluting the potential effect they could have as a whole. Finally, while larger tech companies will have the means to comply with new state-by-state regulations, smaller businesses with fewer resources available will struggle to keep pace. American citizens are more susceptible than ever to having their data used harmfully or without permission, and it is time for the federal government to take responsibility and pass data privacy legislation.

The rise of the internet has provided users with many new services and has fundamentally changed how people interact with each other. Before the rise of email, physical mail was used far more than today. That means of communication is protected since opening another's correspondence is illegal. However, this changed with the rise of social media and digitization with companies reserving the right to claim ownership of any and all data users submit to their services. The world today is highly dependent on internet services including social media. To not use these services means missing out on news, events, online services, and social interactions,

amongst other things. Yet, in order to access these, people must give up their privacy. The European Union has instituted the General Data Protection Regulation to combat this, which, at a high level, gives users more control over their personal data (Meyer, 2018; "GDPR Explained," 2018; Team, 2019). The United States federal government has yet to implement such legislation, leaving users exposed and with a difficult choice to make (Shepardson, 2018).

Beyond privacy, another looming concern for providing companies with personal data is the risk of a data breach. In the past five years alone, personal information of millions of people has been stolen by those who seek to do harm (Cobb, 2016). Many people affected by these breaches were not informed of the attack until days or weeks after. Once again, the United States federal government has refrained from adding legislation to protect constituents from such scenarios, and while certain state governments are trying to enact laws, a mosaic of different state laws will make enforceability difficult (Gregersen, 2019). If the federal government were to take control and enact their own laws, there would be a more unified and organized approach to solving the issue whereby companies are held accountable for their actions and users, as well as their data, are protected.

Research Questions and Methods

This paper seeks to address how the United States progresses its legislation in order to protect American citizens from having their online privacy invaded and their data harvested and sold by corporations. In order to answer this question, several methodologies will be employed. The first of these methodologies will be policy analysis, specifically, an analysis of current federal policy and current legislative procedures, including policies that will be introduced on the floor in the 2020 congressional session. Research and analysis will also be conducted on the

General Data Protection Regulation put into place in Europe. Wicked problem framing will also be used to explore and understand the current situation surrounding user data privacy in the United States. There are many different actors with their own motivations, many of which oppose legislation that would protect people from having their data exploited. This methodology will be used to explore the problem and interpret it in such a way that makes the connections between these actors more apparent and allow conclusions to be drawn accordingly. To provide background on the topic, historical case studies will be conducted on relevant services such as the United States Postal Service and the privacy laws employed to keep mail secure and private. The comparison between keeping physical mail private but not the electronic services that are replacing mail is an important one to draw and highlights the hypocrisy of the federal government in not drafting legislation to protect personal privacy from being invaded online. The combined effect of these research methodologies will provide a clearer view of the different parties involved, their vested interests, comparisons with other nations that have passed their own legislation, and historical background into ways the United States has protected the privacy of citizens in the past.

Conclusion

Once completed, the website being created for the Staunton Makerspace will allow increased flexibility and improved functionality regarding class creation, organization, and registration. Volunteers will be able to create classes that they wish to teach and provide any information they deem relevant. Members of the community will similarly be able to access the course listing and sign up for classes using the web service. The new system, once in place, will

allow for modifications to course details to be viewed by all, and make the entire process far more dynamic.

The STS research paper will detail the situation surrounding internet data and privacy laws and why they do not currently protect Americans from having their information harvested. Analysis will be done on actions being taken by states as well as other countries to address these same issues, and then a solution for the federal government will be constructed. This solution will focus on ways the federal government can limit the power of corporations, improve cybersecurity practices, and emphasize the rights of the individual at a time in history when user data is essentially a currency in itself.

References

Brooks, R. (2019, August 27). Data Privacy Laws by State: The U.S. Approach to Privacy Protection. United States of America. Retrieved September 29, 2019, from https://blog.netwrix.com/2019/08/27/data-privacy-laws-by-state-the-u-s-approach-to-privacy-protection/

Cobb, S. (2016). Data privacy and data protection: White Papers. Retrieved September 29, 2019, from https://www.welivesecurity.com/wp-content/uploads/2018/01/US-data-privacy-legislation-white-paper.pdf

Feenberg, A. (1992, July 20). Subversive rationalization: Technology, power, and democracy. Retrieved October 12, 2019

GDPR explained: How the new data protection act could change your life. (2018). Retrieved September 29, 2019, from https://www.youtube.com/watch?v=acijNEErf-c

Gregersen, C. R. (2019, August 19). The US Is Leaving Data Privacy to the States — and That's a Problem. Aarhus, Denmark. Retrieved September 29, 2019, from https://www.brinknews.com/the-us-is-leaving-data-privacy-to-the-states-and-thats-a-problem/

History of Data Privacy in the United States. (n.d.). Retrieved September 27, 2019, from https://www.clarip.com/data-privacy/us-history/

Meyer, D. (2018, November 29). In the Wake of GDPR, Will the U.S. Embrace Data Privacy? Retrieved September 29, 2019, from https://fortune.com/2018/11/29/federal-data-privacy-law/

O'Connor, N. (2018, January 30). Reforming the U.S. Approach to Data Protection and Privacy. Retrieved September 29, 2019, from https://www.cfr.org/report/reforming-us-approach-data-protection

Quinn, M. (2019, July 22). California data-privacy law may become the model for Congress. Washington D.C., United States of America. Retrieved September 28, 2019, from https://www.washingtonexaminer.com/news/california-data-privacy-law-may-become-the-model-for-congress

Ropek, L. (2019, July 15). NY's Data Privacy Bill Failed; Is There Hope Next Session? Retrieved September 28, 2019, from https://www.govtech.com/policy/NYs-Data-Privacy-Bill-Failed-Is-There-Hope-Next-Session.html

Schryver, K. (2019, August 1). The Future of Data Privacy in the United States. Retrieved September 28, 2019, from https://www.cpomagazine.com/data-protection/the-future-of-data-privacy-in-the-united-states/

Shepardson, D. (2018, July 27). Trump administration working on consumer data privacy policy. Washington D.C., United States. Retrieved September 29, 2019, from https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK

Team, S. E. (Ed.). (2019, June 10). Ask the experts: Should the US have a data privacy law similar to GDPR? Retrieved September 29, 2019, from https://www.synopsys.com/blogs/software-security/us-data-privacy-law-gdpr/

Thomas P. Hughes, "Technological momentum," in Merritt Roe Smith and Leo Marx, ed., *Does* Technology Drive History?: The Dilemma of Technological Determinism, Massachusetts Institute of Technology, 1994, pp. 101–113.

Violino, B. (2018, October 10). Large enterprises are adopting emerging tech at much higher rate than small companies. Retrieved October 17, 2019, from https://www.zdnet.com/article/large-enterprises-are-adopting-emerging-tech-at-much-higher-rate-than-small-companies/