USER EXPERIENCE DESIGN TO REVOLUTIONIZE DATA ANALYTICS FOR BUSINESS INTELLIGENCE

WHAT PRIVACY CONCERNS AND CHALLENGES DO ARTIFICIAL INTELLIGENCE AND DEEP LEARNING PRESENT FOR USER DATA?

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 Systems Engineering

By
Anika Sharma

October 9, 2023
Technical Team Members: Parker Schell, Stacy Meng, Rebecca Dollahite, Anmol Kaur, Ghislain Ventre

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
Joshua Earle, Department of Engineering and Society
Gregory Gerling, Department of Engineering Systems and Environment

Introduction:

In this increasingly interconnected world, new technologies have the potential to bring individuals closer, even across the far reaches of the globe. However, this increase in data sharing poses a potential threat for breaches in privacy and personal data security. One of the most prominent technologies on the rise that poses such a threat is also a buzz word in these current times: Artificial Intelligence, or AI. In terms of my technical project, this also draws on the use of introducing artificial intelligence in the form of a chatbot to assist the user in using a cloud-based log management platform. With my STS topic, I am working to explore the bounds of this integration to ensure that there is no breach in user privacy and data. Specifically, I would like to focus on the users within the private sector and their surrounding communities. This corresponds to larger government bodies that individuals belong to as well. Privacy and technology are also intertwined further with the policy that manages the boundaries as to which user data can be used for innovative purposes. Thus, I would like to analyze various user groups for this project but using the government as the highest level and then further segmenting into use cases. In order to accomplish this, I will be laying the foundation for both my technical topic and STS project, I will then provide the methods to achieve my desired results, and finally investigate current literature to gain more insight into trends and the research space.

Technical Project:

My research project's main goal is to create an artificial intelligence integration on an existing platform. The platform is a cloud based log analytics platform which aids companies in monitoring, troubleshooting, and securing their apps in a scalable manner. There exists a gap in user experience for the platform, as persons of various skill levels seek to use the interface, but find the "low-code" platform to not match their level. Highly experienced developers may find the interface too basic while novice coders may find the website's coding portions to be beyond their capabilities. This gap creates space for the utilization of artificial intelligence as a means to provide support to individuals on the entire spectrum of experience. In this project, our group has complete reign on the design on how the artificial intelligence will be used within the current interface and how it will fall into place with the existing features. Our group has opted for a chatbot route, which involves using the current technologies from OpenAI.com, an open source platform with some of the most up-to-date artificial intelligence software that can be easily incorporated to fit a user's needs.

Our group has taken an iterative approach to design this integration. To start off, we took a look at the current industry landscape by investigating what sorts of steps and visualizations the company's competitors have taken. We discovered that many of them have already taken paces into the space of incorporating artificial intelligence within their customer servers. We made a note of the features that made a positive note on customers and also the features that may have lost their original functionality in translation of the user experience. This helped us to make a model of the descriptive scenario as well as the current gains and losses with the current system that the company employs as well.

Next, our group worked within the design sphere of the project. Working in small divisions of two members each, our group generated several versions of wireframes that included novel ideas and features. Many of these designs were “far out”, or had rather unrealistic capabilities given the state of the current technology. However, these types of designs were critical from a creativity standpoint and also assisted in weeding out different iterations of thought processes. After every iteration, our group discussed the common themes and elements that we liked as well as lessons from the ideas that were discarded. This helped us to develop a cumulative design that seamlessly blended the best of each design iteration.

Throughout the process, our team consistently met with representatives from the company itself on a bi-weekly basis. Each design iteration was therefore met with feedback from stakeholders to aid in the decision criteria. These meetings also aided in getting a sense of the direction that the company wanted us to approach the problem with and their thoughts on the industry trends. We realized that we needed to prioritize a customer-centric approach in regards to privacy and data of the users.

Still working through the design phase, our group hopes to present a high-fidelity and thorough walkthrough of our design to the stakeholders. Upon approval, this design will then undergo integration, feasibility, and security testing. Within the scope of the STS paper, I hope to learn more about the privacy aspect and the risks that this project may present for the company’s clients and users. This will provide for an in-depth exploration of the balance between an accurate, data-trained model and the protection of data on an individual user level.

STS Project

The technology I am investigating is artificial intelligence or AI. Artificial intelligence refers to a machine's ability to perform cognitive functions that we usually associate with human minds (*What Is AI?*, 2023). This technology has been significantly adopted in recent times due to its accessibility. In fact by 2024, there will be more AI assistants than people in this world (Simplilearn, 2023).

But with all this growth, there is also a concern of whether or not individual privacy can be protected. The main issues lie in the capabilities of artificial intelligence to replicate human behavior beyond what is considered "public data" and crossing the line into personal information. There is also the matter of the manner in which artificial intelligence builds its model through profiling a user based on the information they give. Thus, I seek to ask: what privacy concerns and challenges are posed by artificial intelligence and deep learning in regards to user data? As discussed, I seek to look at this question both from the perspective of how the model uses and stores the information provided as well as its capabilities to replicate human behavior enough to be a threat to personal security.

While this topic may be a concern for most citizens in terms of use of their personal data, I do think that certain government or regulatory agencies would also be interested in it for the purpose of ensuring national security. Starting on a broader scale, it is individuals themselves that would have the greatest concern over their own personal privacy. However, it is then important to identify that citizens belong to larger, overarching systems that possess their own related concerns (*The economics of artificial intelligence*, 2019). Thus some of these other systems or social groups would be the large corporations or employers whose business practices become transformed with the introduction of artificial intelligence. As a result of these

large-scale transformations to processes, the landscape of a society's government system may also be altered to account for the new standards. Other regulatory bodies such as the FTC (Federal Trade Commission) may also have to become involved in the privacy upheaval. The most recent legislature in the United States relating to citizen's privacy is the Privacy Act of 1974 (*Privacy Act of 1974*, 2022), which establishes the code of fair information practices, as well as the systems of record that consists of information about individuals by federal agencies. This act is an example of the regulation that governmental bodies may put forth and alter in the face of new privacy issues and concerns. Interestingly enough, different government structures can also allow different forms of policy regarding privacy and user data to arise. For example, China takes a different strategy when it comes to developing its artificial intelligence strategy, using an "omni-use" potential to increase the breadth of actors involved in furthering advancements (*Deciphering China's AI Dream*, 2018). Thus, the three levels of social groups impacted by this research as identified are the individual citizens, large corporations, and the government and regulatory bodies.

The framework I will apply to this situation could be actor network theory (ANT), which provides some insight into how technology, society, and human actors interact and shape each other (Jóhannesson & Bærenholdt, 2020). In this case, the human actors would consist of the government and regulatory bodies that have their own interests and agendas regarding privacy in ensuring compliance with laws and protection of the privacy of citizens. Meanwhile, artificial intelligence would serve as the non-human actors since it has the capability to collect, process, and analyze large amounts of data. This, in turn, influences and shapes the way that privacy is observed and practiced. Some other non-human actors could also take the form of the privacy concerns and privacy regulation that form as a result of them. These actors influence government

and regulatory bodies by setting the boundaries for data sharing and also influence behavior between the human actors. In terms of the network, there are many ways that the actors shape and influence each other. Due to the different types of agendas and interests, there will be a constant interplay between them in the form of negotiations and evolving dynamics. Thus, actor-network theory will be a great method to evaluate and conduct my research, as well as develop the relationships between the relevant social groups, or actors.

In terms of the timeline, my first step will involve collecting data from multiple sources. The first of these sources will be primary journal articles that will be useful in gaining insights pertaining to the current trends in both the privacy and artificial intelligence technology development spaces. These trends and patterns will then be sorted in order to draw conclusions on both the current and future states of development and what sorts of privacy concerns will rise alongside it. The focus will then be to map the privacy concerns to that of the stakeholders or social groups, using ANT as a framework. The changes in the relationship between the actors due to the technological shifts will be mapped out for the future.

Another method of data collection would involve surveying and interviewing members from each of the social groups. From experts in the field all the way to the common citizen that cares about their individual security, the scope of familiarity with the subject will be interesting to explore for each social group. The data collection from primary sources will take about two months while the questions drafting and identification should take another additional month. After this, the actual surveying and gathering of answers will be conducted over the course of two weeks. The rest of the period of time will be dedicated to synthesizing findings and connecting the dots between the various data gathering methods. This will then aid me to finalize

and draw conclusions to determine the extent to which artificial intelligence will drive privacy concerns for the surveyed social groups.

Key Texts

The first text that I will investigate will be "The Economics of Artificial Intelligence: An Agenda", which provides an overview of the current landscape of artificial intelligence in the lens of economics and its relation to societal issues. It provides a good baseline for gathering facts about the nature of AI as a disruption in individual privacy, as well as insight into how different social groups are impacted within the economic scheme. In terms of the agenda, the paper now seeks to find uses in public spaces and institutions such as within the squares of inequality, the political economy, economic growth, jobs, and the meaning of work. In the scope of my project, this article serves as a great starting point for gaining insight on the current scheme of what uses are possible with artificial intelligence, as well as a general understanding of the developments.

The second text that will be utilized is "In AI we trust? Citizen perceptions of AI in government decision making" which instantiates that Governments are responsible for carrying out a number of tasks, and this paper explores how artificial intelligence can be used as a direct tool in assisting with these tasks. With the combination of Big Data, the text shows that citizens usually positively respond to increased efficiencies in required tasks such as filing taxes and even registering for educational programs. However, it is important to note that decision making has an entirely different spot on the spectrum compared to routine and tedious tasks. Decision making requires a cognitive element that is difficult to completely leave at the hands of technology. While AI has been advancing at amazing rates, there is still a high degree of uncertainty when it comes to implementing the technology at a level that affects so many

constituents. From the scope of my project, I would want to analyze the privacy elements of such tasks too, ranging all the way from simpler to developmental ones that affect the face of a nation.

As mentioned before, I'd like to further analyze the collisions between different government structures strategize towards technological advancements in lieu of privacy concerns through studying "Deciphering China's AI Dream". This text emphasizes that traditionally, the East has always taken a different approach when it comes to technology development and implementation. This could be due to a variety of different reasons such as the difference in government structures or types of programs that benefit from new R&D in technology. This text expands on China's, powerhouse of the East, long-term strategy when it comes to artificial intelligence. With this, the paper relates the key drivers of China's AI strategy to the drivers of AI development within the economic sphere, while also examining China's current capabilities as opposed to a novel index measurement of the country's AI potential. Moreover, the article debunks many myths in the space, especially stating that substantial discussions about AI and ethics are emerging in China as opposed to the preconceived notion that this may be an afterthought in the struggle to get ahead. In the context of my project, I think it is crucial to look at how countries with different government structures tackle the ethical dilemmas that arise, especially when trying to make advancements at a rapid rate.

The final key text is "Bias Optimizers", which takes a deep dive into how biased data produces biased results, and how these tools are translated to front-facing interfaces. With the creation of these interfaces being integrated so heavily into company operations, it becomes the image and message of the company themself. With this, it is clear that many of these GPTs have a direct reliance on a set of assumptions they work with. Due to this, Williams emphasizes artificial intelligence's role in promoting humanity's "worst qualities". With this overemphasis on

the negativity of human emotions, many social issues are magnified in the process of drawing conclusions. With an already crumbled foundation, it seems clear that the actual work will have its own cracks. This source has a very clear relevance for my project, as I do want to drill down on how the data is produced.

Citations

Agrawal, A., Gans, J., & Goldfarb, A. (2019). *The economics of artificial intelligence: An Agenda*. University of Chicago Press.

Bias Optimizers. (2023, October 30). American Scientist. https://www.americanscientist.org/article/bias-optimizers

Ding, J. (2018). Deciphering China's AI Dream. *Future of Humanity Institute*.

Ingrams, A., Kaufmann, W., & Jacobs, D. (2021). In AI we trust? Citizen perceptions of AI in government decision making. *Policy & Internet*, *14*(2), 390–409. https://doi.org/10.1002/poi3.276

Jóhannesson, G. Þ., & Bærenholdt, J. O. (2020). Actor–Network Theory. In *Elsevier eBooks* (pp. 33–40). https://doi.org/10.1016/b978-0-08-102295-5.10621-3

Mehr, H. (2017). Artificial Intelligence for Citizen Services and Government. *Harvard Ash Center Technology & Democracy*.

Privacy Act of 1974. (2022, October 4). https://www.justice.gov/opcl/privacy-act-1974

Simplilearn. (2023, November 7). *Top Artificial Intelligence Stats You Should Know About in 2024*. Simplilearn.com. https://www.simplilearn.com/artificial-intelligence-stats-article

What is AI? (2023, April 24). McKinsey & Company. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai