Annotated Bibliography

Reflective Cover Letter:

I chose this topic since it is an issue which I believe is a critical issue that is being mostly ignored by the mainstream. Poor data privacy and the rate of data collection is getting to massive levels, where those companies only get a slap on the wrist. Billions of people's data are being collected and processed for companies to get richer and influence our actions through targeted ads. As time goes on we see that the methods of data collection are getting more and more invasive, slowly stripping away our choice of privacy. In this paper I want to make people realize what really happens in the back rooms of data monopolies, and show how they lie to the public using rhetoric manipulation. I see my audience as anyone who has accepted a privacy policy or bough an home assistant, anybody should be able to see what companies do with their collected data. Considering the audience has made me focus more on 'shock' value instead of deep analysis of policies as I first intended. I want to make this paper readable for everyone.

My writing process for this annotated bibliography has undergone many changes and forced me to consider how I will construct my essay. At first I thought I should focus on rhetoric alone especially in privacy policies and terms and conditions, but then I realized that if I had done that my essay would be as bland and unreadable as the exact thing I was trying to expose. So I decided to pivot into writing about multiple areas of data collection and evaluate how rhetoric is used in each. I believe this will make it much easier t read since every topic gets its own section and thus majorly improving the flow. The topics I have decided to talk about are as followed: Big data and Ai, Surveillance Capitalism, Biometric data collection (heavy emphasis on facial recognition), and finally Internet of Things devices. While I have a basic understanding of what I will do I still do not see the full plan yet so I suspect I will shift topics and ideas around quite a bit (this includes finding more sources which require updating of annotated bib, introduction of new topics not talked about here, or removal of topics talked about here). One practice that really helped me was actually the Wikipedia search activity. It really helped me find related topics that I could talk about since I had to completely ditch some of my original sources.

This has really helped me understand some of the SLO's much better that I had though I understood before. Especially Information Literacy. I thought that is was just finding evidence that supports your claim but it is much more than that. Many pieces of evidence that supports your claim is not the best choice for a specific part or interrupts the flow of the essay. For example one source I was considering was a 74 page analysis of Californian Cyber law, which could've definitely supported my claim but I feel that it would have interrupted the focus of data collection and opening an entire new topic of Privacy laws that I felt were not in scope of this essays main theme. Another SLO that I had much more experience with was Research Genre Production. Since midway of writing my bibliography I had pivoted my main focus I also had to re-define who was my audience and what evidence would impact them the best. Switching from a very technical audience with technical sources to the public as my audience forced my to look at my evidence from a new light and restructure my essay from the ground up.

Literature Review:

All of my papers that I have sourced for this essay all point to an abuse all the way to the CEO's, regarding data collection and exploitation. There were many trends in my papers especially in the way of data breaches and lawsuits. Some key cases cropped up in the articles including the Facebook / Cambridge Analytica scandal where it was found that Cambridge Analytical was scrubbing Facebook accounts and pushing advertisement for political parties unto those who were undecided. There were also some very common companies that made multiple appearances in my selected articles, such as: Google, Amazon, Apple, and Facebook. These companies (especially Google) are the main offenders when it comes to surveillance capitalism and collecting data. Another trend is that these companies exploit users by using rhetoric to obscure that they are using collected data in order to make behavioral predictions which they sell to advertisement companies.

The themes of these papers generally coincide with the idea that there needs to be more overarching government intervention when it comes to laws safeguarding users online privacy. They also mention that users should be better educated about how each of their data is being utilized and collected. Some papers that I have chosen specifically pointed out devices like the Amazon Echo Dot and talked about how smart home devices like this can greatly increase the amount of data collection that companies have on us by being able to gauge our daily lives and then create more accurate data predictions to sell to advertisers at a higher price.

The major gaps that my articles have are a time one. Most of my articles were created around 2018 which could rule out some advances in data protection law. However one of my articles do cover the effects of the GDPR (created in 2018) which I can use in my article but I feel that for most people in the US, that data law and responsibility never really came. There is one exception which was the 2020 Californian data protection act, which gave people in California almost the same rights as those under the GDPR in Europe. However for the other 300.67 million us citizens that are not Californian there has been practically no national data protection law so most of these articles still very much apply. Actually I believe that the situation regarding data collection has gotten much worse since these articles have been published. With the rise of Ai integration in practically every single home appliance, cars, mobile devices, computers, etc. the situation has only decayed. With the amount of data breaches in 2023 almost triple since 2018(source: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/), IoT devices has helped greatly weaken device security and has only benefited those who collect data off of them.

While my papers were mostly convergent on their messages, there was some debate. One of te major debates I saw was the controversy of how far should governments use this new technology to combat crimes. For example the paper about the rhetoric of big data said that governments should be able to use facial recognition software to combat major crimes like terrorism and murder but becomes a grey area when it comes to not so serious crimes like petty crime. While another paper said that any government that uses facial recognition or uses software in order to look through millions of facebook profiles in order to find possible suspects should have their software immediately revoked since it violated basic human rights regarding privacy.

Annotated Bibliography:

Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data.

Robertson, Viktoria H.S.E. "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data." *SSRN*, 2019, papers.ssrn.com/sol3/papers.cfm?abstract_id=3408971.

The paper looks at how big tech companies collect large amounts of user data through third-party tracking. It argues that this kind of data collection can be a competition issue, not just a privacy concern, because it gives companies too much control over the market. The author uses The German Facebook Decision to show how companies use their power to force users into accepting unfair data policies. The paper suggests that stricter rules are needed to stop companies from using data collection as a way to dominate the industry. The author especially highlights different opportunities to so so offering multiple angles utilizing current GDPR and the TFEU to establish large 3rd party data collecors as offering an unfair trade to consumers. Overall, it explains how tech companies take advantage of users by making data collection seem normal and necessary.

Since this paper regards Current law and data collections by "data-opolies" it is highly relevant to my topic. I plan to utilize key parts of the text, for example, "Further uses that personalized data is put to include the provision of individualized services, price discrimination and the selling-on of data sets to third parties" where the author mentions how collecting personalized data can cascade into multitude of different issues. Another quote I plan to use is "It also allows for micro-targeting, meaning that messages (be they political or commercial) tailored to a specific individual can be delivered". I also plan to use some quotes like "Where third-party tracking is based on an 'unreasonable expansion of the datause policy' – even if perhaps not reaching the threshold of a data protection violation – then antitrust intervention may be warranted" where the author talks about potential solutions to massive companies hording data, by establishing anti-trust laws against third party data collectors.

Surveillance Capitalism and the Challenge of Collective Action

Zuboff, Shoshana. "Surveillance Capitalism and the Challenge of Collective Action." *Sage Journals*, 2019, journals.sagepub.com/doi/full/10.1177/1095796018819461.

This paper is a gold mine when it comes to data collection and rhetoric. By utilizing capitalism surveillance as a midpoint, how companies are uses all the rhetoric they possess in order to keep the public in the dark about what they really know about their data. Zuboff analyzes how google and other data monoliths had turned worthless junk data and turned that raw data into behavioral predictions that advertisers utilize in order to generate more profit. As time went on, it became not enough to ensure that a prediction might happen, so Zuboff showed that large corporations like google and Amazon, took great measures to ensure that those predictions became true through behavioral modification. That is the reason why companies like amazon have sold "Ai assistants" at a loss in order to get much more data gleaned not just from our phones, but from our home, car, hotel, and so on.

This paper is highly correlated to my topic since Zuboff describes how consumers are tricked into giving data into prediction algorithms to enhance ad revenue. This is mostly done using long and confusing policies filled with corporate rhetoric which many people are practically trained not to read.. One prevalent quote that i would like to use is “Later those assets were hunted aggressively, procured, and accumulated— largely through unilateral operations designed to evade individual awareness and thus bypass individual decision rights” as well as “In the case of surveillance capitalism, camouflage, euphemism, and other methodologies of secrecy aim to prevent interruption of critical supply chain operations that begin with the rendition of human experience and end with the delivery of behavioral data to machine intelligence-based production systems”

The ethical application of biometric facial recognition technology

Smith, Marcus, and Seumas Miller. “The ethical application of biometric facial recognition technology.” *AI & SOCIETY*, vol. 37, no. 1, 13 Apr. 2021, pp. 167–175, https://doi.org/10.1007/s00146-021-01199-9.

This paper goes over examples of government use of biometric data (specifically facial recognition) from all over the world. It highlights the balance between the security benefits of facial recognition, such as crime prevention, and the privacy risks it poses, including surveillance overreach and potential misuse. The authors argue that strong legal frameworks are needed to regulate the technology and ensure it aligns with democratic values and ethical principles. By analyzing facial recognition policies in countries like the U.S., U.K., and Australia, the paper examines how different governments handle the trade-off between security and personal rights (which many abuse). Ultimately, it emphasizes the need for transparent policies, accountability, and public discourse to prevent the misuse of biometric surveillance.

This paper uses examples from around the world of government use of facial recognition software, which can help add to my argument of people having their data harvested without proper knowledge. This also feeds into the topic of AI since many of these facial recognition cameras funnel their data into large AI processing. I will utilize this article by enhancing the section on biometric data and especially focus on police and government use and how governments will use this gleaned data in order to further prop up surveillance capitalism, and use that to modify and alter our own behaviors through large exploitation of rhetoric and data collection. And example of a quote that I might use is “Biometric technologies are part of a shift taking place in society towards automated decision-making processes that involve limited human intervention”

The Rhetoric of Big Data: Collecting, Interpreting, and Representing in the Age of Datafication

Mehlenbacher, Brad, and Ashley Rose Mehlenbacher. *The Rhetoric of Big Data: Collecting, Interpreting, and Representing in the Age of Datafication*, pubs.lib.uiowa.edu/poroi/article/3303/galley/112137/view/. Accessed 11 Feb. 2025.

This Paper covers how large companies use rhetoric to cover data collection and illegal use. It particularly looks at the case of Cambridge Analytica and how data is not only a “construct” but a tool that corporations weaponize to push specific publish opinion. By presenting data as objective and

neutral, companies deflect ethical concerns while continuing exploitative practices when in reality much captured data is actually biased since the ones collecting the data were inherently biased. The study also emphasizes the role of data experts in legitimizing these practices and the challenges in holding them accountable, as well as how large companies are utilizing ethos in order to push their "experts" reliance that data is safe unto the public. Ultimately, this paper reveals how rhetoric is weaponized to control narratives around data privacy and influence democratic processes.

This Paper effectively illustrates how using rhetorical devices allows companies to evade scrutiny while maintaining their data-driven business models. Its analysis of Cambridge Analytica offers a concrete example of how corporations manipulate public understanding of data collection. This analysis directly supports my research on how major tech companies use rhetoric to obscure predatory data collection. The discussion of Cambridge Analytica aligns with my main topic on how persuasive techniques shift attention away from privacy violations. Some quotes I plan to use are " The Cambridge Analytica case thus contributes to an undermining of trust among (purported) technical experts and publics" and as well as "However, as we have argued, data, big data, and the entailments surrounding big data, are not merely matters for reason, or fact, etc., but rather firmly in the domain of rhetorical appeals".

The Role of Privacy Policy on Consumers' Perceived Privacy

Chang, Younghoon, et al. "The Role of Privacy Policy on Consumers' Perceived Privacy." *Sciencedirect.Com*, 2018, www.sciencedirect.com/science/article/pii/S0740624X17301946.

The paper investigates how privacy policies shape consumers' perceptions of privacy, focusing on the role of clarity, length, and accessibility in building trust. It argues that overly complex or lengthy policies often lead to consumer mistrust, while clear and concise policies can enhance confidence in a company's data practices. The study emphasizes the importance of transparent communication, suggesting that well-crafted privacy policies can act as a tool for fostering trust between companies and consumers. However, it also raises questions about whether these policies are genuinely designed to inform or simply to comply with legal requirements. Overall, the research provides valuable insights into how companies use privacy policies to influence consumer attitudes, which connects to broader discussions about corporate transparency and ethical data practices.

This paper is highly relevant to my research question because it provides a framework for analyzing how tech companies use language in privacy policies to shape consumer perceptions. However, it doesn't fully address the predatory aspects of data collection or the intentional use of rhetoric to obscure these practices. While it offers insights into consumer trust, it could be strengthened by exploring how companies exploit this trust through manipulative language. I will use this paper to support my research by drawing on its findings about how privacy policies influence consumer perceptions. Specifically, I'll incorporate its discussion of clarity and transparency to analyze how tech companies use rhetoric to create an illusion of privacy. This will help me argue that even seemingly clear policies can be part of a broader strategy to obscure predatory data collection practices.

User perceptions of smart home iot privacy

Zheng, Serena, et al. “User perceptions of smart home iot privacy.” *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, no. CSCW, Nov. 2018, pp. 1–20, https://doi.org/10.1145/3274469.

This paper is a survey of 8 different homes and their view on IoT device security and privacy. It finds that users prefer convenience over privacy, often trusting manufacturers blindly. Many users were completely fine with their data being recorded by select sources (company of device, advertisement) while resistant to others (ISP’s and governments). Many are unaware of the risks posed by inference algorithms that analyze non-audio/visual data to extract sensitive information. The study finishes with recommendations for better device privacy features with user expectations and industry standards.

While this paper is from 2018, its qualitative research is still very prevalent today. While they mention that a many of their participants consider themselves “early adopters” the findings still correlate today where IoT devices are practically everywhere. If anything I feel that people have shifted to more accepting of IoT devices and what we say in this paper was a more wary customer base even though the amount of data collected today is dramatically increased compared to 2018. I will use this to explain the more human sign of the understanding of how secure people perceive themselves in IoT devices. Specifically in the survey where many people were unaware that non A/V (audio/visual) IoT devices still collect data and using ai can figure out even more data and use that to trigger more targeted advertisement. I will most likely tie this into my section about surveillance capitalism and how corporations can use IoT to create an even more invasive data collection.