Nikolai Colon
ENC 1102
Professor Ramos
03/2025/26

The Language of Surveillance: The Weaponization of Rhetoric in Surveillance capitalism

Billions of people's data are being collected and processed for corporate profit, by manipulating our actions and emotions through ad algorithms to maximize selling sponsored products. As time goes on we see that the methods of data collection are getting more and more invasive, slowly stripping away our fundamental right to privacy. Data-opolies like Google and Facebook weaponize rhetoric in order to normalize their application of Surveillance capitalism. Through the analysis of multiple scholarly journals and papers, I will demonstrate how these companies use new technologies across various tech fields to expand and legitimize their data collection practices.

Literature Review:

The papers that I have sourced for this essay point to the abuse of data collection and exploitation of the users throughout the world. There were many trends in my sources especially regarding data breaches and lawsuits. Some key cases in the sources 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 are also some companies that made multiple appearances in my evidence 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 I have discovered is that 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 which showed how smart home devices can greatly increase the amount of data collection that companies have on the populous by being able to predict our daily lives which in turn create more accurate data predictions to sell to advertisers at a higher price.

The major gaps that my papers have are a time one. Most of my papers were created around 2018 which possibly rules out some advances in data protection law. However one of my sources does cover the effects of the GDPR (General Data Protection Regulation) in Europe, which I use in my paper but I feel that for most people in the US, data law and corporate responsibility never came. There is one exception where the 2020 Californian data protection act 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 no national data protection law which demonstrates these papers are still applicable. I believe that the situation regarding data collection has gotten much worse since these papers have been published. With the rise of Ai integration in practically every single home appliance, cars, mobile devices, computers, etc. the situation has only exacerbated. With the amount of data breaches in 2023 almost triple since 2018, IoT devices has greatly weakened device security and has only benefited those who collect data off of them.

While my evidence mostly converged on their messages, there was some debate. One of the major debates I saw was the controversy of how far should governments use facial recognition to combat crimes. For example the paper *The Rhetoric of Big Data: Collecting, Interpreting, and*

Representing in the Age of Datafication argued that governments should be able to use facial recognition software to combat major crimes like terrorism and murder. However the topic becomes a gray area when discussing petty crime. While the paper *The ethical application of biometric facial recognition technology* argued that any government that uses facial recognition or software in order to parse through millions of Facebook profiles in order to find possible suspects should be scrutinized since using that software would violate basic human rights regarding privacy.

Fundamentals of Surveillance Capitalism:

Surveillance Capitalism is a political economic concept in where corporations weaponize widespread collection and commercialization of personal data. Surveillance Capitalism fuels data monopolies that have make hundreds of billions of dollars every year utilizing the data they collected in order to feed their prediction algorithms. Companies like Google and Facebook use these algorithms to show “personalized ads” to people. Advertisers will pay much more money if companies like Google can guarantee that a percent of people who see the ads will click on it, so that is where the algorithms come into play. Google and other data monoliths had turned worthless “junk” data (an example would be how someone types) 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, large data corporations took great measures to ensure that those predictions became true through behavioral modification. Many times the consumer does not know just what kind of and what data is being collected, as Zuboff says, “Later those assets were hunted aggressively, procured, and accumulated—largely through unilateral operations designed to evade individual awareness and thus bypass individual decision rights”. That is the reason why companies like amazon have sold “Ai assistants” at a loss in order to get much more data reaped not just from our phones, but from our home, car, hotel, and so on. Consumers are tricked into giving data because of complicated and Illegible privacy policies as well as making it inconvenient to opt out in order to feed big business's prediction algorithms to maximize ad

revenue. As Zuboff further argues, corporations rely on deceptive language to disguise their surveillance tactics:

"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" (Zuboff).

Facial Recognition:

Companies from all over the world use facial recognition in order to push the dystopian future which surveillance capitalism brings. This new emerging technology highlights the slippery slope between the security benefits of facial recognition, such as crime prevention, and the privacy risks it poses, including surveillance overreach and data collection. By analyzing facial recognition policies in countries like the United Kingdom, China, and the United States. All of these countries heavily utilize facial recognition wether that be from the government or corporations the end result is the same, the erosion of the persons privacy. An example of surveillance overreach from the US is:

"*it became widely known that law enforcement agencies in the United States were using a biometric facial recognition algorithm, developed by the company Clearview AI, to search images on the internet to identify suspects"(Smith, Marcus, and Seumas Miller)*

Such surveillance practices emphasizes the need for transparent policies, accountability, and public discourse to prevent the misuse of biometric surveillance. Smith, Marcus, and Seumas Miller also make a point to note that not only was ClearviewAI offering its algorithm to law enforcement but to companies including Walmart, AT&T, the NBA, Bank of America and Best Buy as well. Clearview AI's widespread sharing of its algorithm shows a massive privacy breach to the public in which the

ability to digitally recognize faces and attach them to profiles which can be exploited by retail companies in order to copy that which Google is doing and track all of their customers. While this quote relates to government use of facial recognition it also heavily applies toward to corporate use as well:

"the utilisation of this data to identify and track citizens, (e.g. via live CCTV feeds) has the potential to create a power imbalance between governments and citizens, and risks undermining important principles taken to be constitutive of the liberal democratic state, such as privacy"(Smith, Marcus, and Seumas Miller)

We already see corporate use of biometric data happening in authoritative countries like China where they employed millions of cameras in public areas to locate, track, and even establish a social credit score based on a persons actions. Sadly we can see that companies like Google, and Amazon are utilizing the same guidebook but operating much more discreetly. By integrating IoT devices, smart home assistants, and other smart home technologies, they can track and collect data from within the home, often without raising suspicion.

IoT Devices:

The paper "User perceptions of smart home iot privacy" by Zheng, Serena, et al. describes 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 the paper is from 2018, its qualitative research is still prevalent today. An example of the research is the authors findings that a many of their participants consider themselves "early adopters" when talking about home

assistants which is not the case in modern times, 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 then what was demonstrated in the paper. The survey group was a more wary customer base because of the unfamiliarity of the technology where as today the amount of data collected is dramatically increased compared to 2018. In the survey many people were unaware that non A/V (audio/visual) IoT devices still collect data and in modern day pairing these IoT devices with ai, this turns into a major source of data and money for those companies with prediction algorithms. Companies like Amazon even pay hotels and such in order to glean information even when people are away from their home. One item I would like to draw attention to is the fact that one of the biggest sources of data in the home that is in about 79% of homes is Smart TV's. Many do not consider that Smart TV's are in fact IoT devices and many times companies will sell these devices for dirt cheap or even at a loss in order to lure shoppers into giving even more data.

Privacy Policy: Privacy policies really just serve as a formality since many users never read these because of the long, hard to read nature that was specifically crafted in order to deter customers in seeing what data is being collected. The paper “The Role of Privacy Policy on Consumers’ Perceived Privacy” by Chang, Younghoon, et al. 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. However many large companies would actually prefer to keep their privacy policies as illegible as possible in order to keep their customers in the dark, since they can make much more money that way. Chang et al.'s findings are crucial in understanding how tech companies use language in privacy policies to shape consumer perceptions. While the study

highlights the role of clarity and transparency in fostering trust, it does not fully address the deliberate use of misleading rhetoric to obscure data collection practices. Many corporations craft their policies to appear transparent while strategically concealing the extent of their data exploitation. With users in the dark about not knowing what data is being collected about them, its much easier to keep the train of surveillance capitalism continuing while generating the least amount of backlash.

AI:

Artificial intelligence is often presented by tech companies as a neutral or benevolent force, however it is used daily to deepen surveillance capitalism. It all starts with how they train their AI and where they procure their data. There have been numerous cases exposing tech companies for harvesting user data when using ai to train their models, most of the time without the knowledge of the user. An example of this is:

"the University of Chicago and multiple healthcare organizations granted access to countless patient medical files for AI data-mining to a company called DeepMind. The data was then used by Google to train its AI via machine-learning diagnostics and search algorithms in support of a proposed potential patent that would allow the search behemoth to create a subscription or pay per use service" (Husain)

This happens because without massive amounts of data AI is not nearly as effective but buying tons of data legitimately is much too expensive and could risk the brand image since much of they data they collect is highly invasive and person. So AI companies collect or steal many of peoples personal data to train their AIs only to sell it back to them. As Morgan sullivan shows "With the pervasive use of AI systems like ChatGPT, data collection has become more extensive than ever … These users often do not fully understand what data is being collected and how it will be used, raising concerns about data privacy and true consent" She goes on to explain that Large models like ChatGPT and Googles' Gemini are useless without large amounts of data to constantly fed to them. So companies use clever rhetoric

and sleazy tactics to obscure what data they are collecting, how much data, and how the data will be used.

Use of rhetoric:

Large companies use rhetoric to cover actions that they do to further their own personal gain through surveillance capitalism while normalizing the fact. In the paper “The Rhetoric of Big Data: Collecting, Interpreting, and Representing in the Age of Datafication” by Mehlenbacher, Brad, and Ashley Rose Mehlenbacher, 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. As the authors state, “The Cambridge Analytica case thus contributes to an undermining of trust among (purported) technical experts and publics,” highlighting how low companies lower themselves when they lean heavily into surveillance capitalism, by having experts lie to the people, helping the companies militarize rhetoric by manipulating the masses. 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. As the authors argue, “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 authors insight demonstrates how corporations use rhetorical strategies to present data as an indisputable truth while avoiding scrutiny of the biases and motivations behind its collection. Ultimately, the paper reveals how rhetoric is weaponized to control narratives around data privacy and influence democratic processes. These insights helps expose how companies abusing rhetorical devices allows them 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. The discussion of Cambridge Analytica aligns with my main topic on how persuasive techniques shift attention away from privacy violations.

Law:

Big tech companies collect large amounts of user data through third-party tracking. The practice of data collection of data collection can be a competition issue, not just a privacy concern, because it gives companies too much control over the market. In the paper “Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data” by Viktoria Robertson, she uses The German Facebook Decision to show how companies use their power to force users into accepting unfair data policies. She suggests that stricter rules are needed to stop companies from using data collection as a way to dominate the industry. One example of how data collection is exploited is “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. The author especially highlights different opportunities to so so offering multiple angles utilizing current GDPR and the TFEU to establish large 3rd party data collectors as offering an unfair trade to consumers. “It also allows for micro-targeting, meaning that messages (be they political or commercial) tailored to a specific individual can be delivered”. Overall, it explains how tech companies take advantage of users by making data collection seem normal and necessary. “Where third-party tracking is based on an ‘unreasonable expansion of the data use 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.

Conclusion:

The unchecked expansion of surveillance capitalism has led to an unprecedented erosion of privacy, with tech giants exploiting user data under the guise of convenience and personalization. Through the manipulation of rhetoric, corporations have successfully normalized invasive data collection, making it difficult for the average consumer to grasp the true extent of their exploitation. The scholarly works analyzed in my paper demonstrate a clear pattern: major tech firms employ deceptive language, obscure their practices behind illegible privacy policies, and weaponize algorithms to shape consumer behavior—all while avoiding meaningful regulation. Despite mounting evidence of harm, legislative efforts in the U.S. remain fragmented, leaving millions vulnerable to unchecked data exploitation. While policies like the GDPR and California's data protection act provide some safeguards, they are far from a universal solution. The rapid integration of AI and IoT devices has only exacerbated the issue, further embedding surveillance into daily life. Without stronger regulatory oversight and increased public awareness, the dominance of data-opolies will continue unchallenged, solidifying their control over both digital spaces and personal autonomy. The future of data privacy hinges on whether governments and consumers can resist these exploitative tactics or remain complicit in the ever-growing machinery of surveillance capitalism.

WORKS CITED

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

Husain, Osman. “7 AI Privacy Violations (+what Can Your Business Learn).” *Data Privacy Compliance Software for Apps, Websites, & SaaS*, Enzuzo, 14 June 2024, www.enzuzo.com/blog/ai-privacy-violations.

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.

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.

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.

Sullivan, Morgan. “Ai and Your Privacy: Understanding the Concerns.” *Transcend*, transcend.io/blog/ai-privacy-issues. Accessed 26 Mar. 2025.

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.

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