Surveillance Capitalism

Scientists and Ethics

Alcalde Echegaray, Nadir Williams
Department of Informatics
Technical University of Munich
Email: nadir.alcalde@tum.de

***Abstract*— Surveillance Capitalism refers to the economic system in which personal data is captured through surveillance and then monetized. This term was first coined by Shoshana Zuboff in her paper with the same name. There she explains how this practice has become increasingly prevalent with the rise of giants companies like Google, which collect gigantic amount of user data in order to optimize services and display targeted advertising. This paper is going to explore the ethical implications of such practices, just as Google's data practices and collectors, through various ethical lenses, including deontological ethics, consequentialism, and hedonism. This analysis also reveals issues and concerning topics related to privacy, autonomy and fairness.Furthermore, this paper advocates for stringent regulatory oversight, corporate accountability and increased citizenry awareness to protect user rights in the digital era. Future research should focus on developing frameworks and policies that balance the benefits of data-driven innovation with respect for individual privacy and autonomy.**

I. Introduction

Surveillance capitalism refers to the economic system personal data is monetized captured through digital surveillance. The origins of surveillance capitalism can be traced back to the early 2000s, where internet giants like Google and Facebook have risen. Companies like those were the first to see the huge value of user data, because it was key to predict their behavior and build targeted features and services, as well as ads for income. Then this practice began to take a more concrete shape as these companies developed sophisticates methods and tools to collect, analyze and utilize data of their user. It can be discussed that this practice has also advantages, such as improvement of user experience and service personalization but, it can also quickly become apparent that this data could be leveraged for targeted advertising, leading to significant revenue streams.

The early era of internet was primarily dominated by a collection of static websites and simple services, but as the internet evolved, so did the business models of the companies that dominated it. We are going to take Google as an example to explain how surveillance capitalism took its first steps. Google was founded in 1998, and it was initially focused on creating the most advanced and quicker search engine of its time. However, the company soon realized that the collected data through user searches could have a real useful porpoise, since at the time other search engines just discarded that information. These saved queries could be used to predict user interest and sell this data to other companies and as well as deliver highly targeted advertisements . This realization marked the beginning of surveillance capitalism, a trend which would only grow in the following years

With the introduction of AdWords (now Google Ads) in 2000 and AdSense in 2003 by Google, a new revolution for online advertising took place. These platforms used stored user data to serve targeted ads, which significantly increased the effectiveness and relevance of advertisement the users were displayed. This happened because users were now getting ads that matched with their necessities and curiosity. Therefore, companies like Facebook, which was founded in 2004, took a similar business model, not only because the profitability of data-driven advertising was demonstrated, but also due to the unawareness of users, who kept feeding the collector machines developed by these companies. The fact that Facebook rapidly expanded its user base and began collecting vast amounts of data on user interactions shows how effective this business model was. This collected data the foundation for its advertising platform, which allowed advertisers to target users based on their interests, behaviors, and demographics.

With the evolution of surveillance capitalism, new study fields as data analytics have been developed. In addition to that, the proliferation of mobile devices, other social media platforms and IoT devices has led to an huge boom in the amount of data generated by users. In response to this, companies have developed more advanced and sophisticated algorithms which analyzes this user data and extract valuable insights, which can either be used to profile those users and send them high targeted ads and content based on their behavior, or can be sold to other companies with similar practices.

Today, surveillance capitalism counts as the dominant business model for many of the world's largest and more powerful technology companies. Companies as Google, Meta and Amazon generate significant portions of their revenue through data-driven advertising. Thus these companies have built vast and user-friendly ecosystems which collect data from a wide range of hardware and software interactions, such as physical devices or user behavior in certain social media. For that very reason, surveillance capitalism has got a huge impact on society. On one hand, it has helped with the development of highly personalized services, which enhances user experience. But on the other hand, it has raised significant ethical and privacy concerns leading up to following questions: How private is our life and habits as well as to what extent are we owners of our information.

Therefore, is important to question how well regulation and oversight to protect user privacy and ensure accountability are managed and executed by these companies. The ethical implications of surveillance capitalism are complex and multifaceted, that is why it is important to raise questions about consent, autonomy, and transparency. Furthermore, the use of data to influence behavior raises questions about manipulation and autonomy.

For all those reasons and by analyzing specific cases studies applying them through various ethical frameworks, the paper aims to analyze the critical ethical issues and propose potential solutions to ensure ethical data practices in the digital age.

II. Chapter on Something

blabla

A. Subsection

blabla with some citations [1], [2]

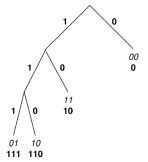

Fig. 1. Tree

TABLE I
SOME TABLE

Column1	Column2
0	1

III. Case Studies

A. Google and YouTube's Data Collection on Children

In 2019, Google and YouTube were fined $170 million by the FTC for violating the Children's Online Privacy Protection Act (COPPA). They had collected personal information from children under 13 without parental consent, raising significant privacy concerns and violating ethical principles of informed consent. This case highlights the vulnerability of children in the digital age and the need for stricter regulations to protect their privacy.

The ethical implications of this case are profound. Children, as a vulnerable population, require special protections. Collecting data without parental consent not only violates legal standards but also ethical norms of safeguarding minors. The lack of transparency and informed consent in this case undermines trust in digital platforms and calls for more robust regulatory frameworks to ensure ethical data practices.

B. Google+ Data Breach

In 2018, Google announced that a software glitch in Google+ had exposed private data of up to 500,000 users. The breach, discovered in March 2018, was not disclosed immediately, raising issues of transparency and accountability. The delayed disclosure prevented users from taking timely actions to protect their data, leading to potential harm and distrust.

The Google+ data breach underscores the importance of timely disclosure in maintaining trust and accountability. From an ethical standpoint, withholding information about data breaches violates the principle of transparency and the duty to protect users' privacy. The incident also highlights the need for better security measures and proactive communication strategies to manage data breaches effectively.

C. Project Nightingale

In 2019, it was revealed that Google had partnered with Ascension to collect and analyze health data of millions of Americans without informing them. This project raised significant privacy concerns and issues related to informed consent. The use of sensitive health data without explicit consent undermines trust in healthcare providers and digital services.

The ethical concerns surrounding Project Nightingale revolve around the unauthorized use of sensitive health information. Health data is inherently personal and requires stringent protections. The lack of informed consent and transparency in this case breaches ethical standards and poses risks to patient privacy and autonomy. This case illustrates the need for ethical guidelines and regulations in handling health data.

D. Google's Location Tracking

In 2018, an investigation by the Associated Press found that Google continued to track users' location even when they had turned off location tracking settings, which was seen as deceptive and a violation of privacy. This practice highlights the discrepancy between user expectations and actual data practices, leading to ethical concerns about honesty and transparency.

Google's location tracking practices raise ethical questions about deception and respect for user preferences. Despite user actions to disable location tracking, continued data collection violates privacy and autonomy. This case emphasizes the importance of aligning data practices with user expectations and ensuring that privacy controls are effective and respected.

E. Google Street View Wi-Fi Data Collection

Between 2007 and 2010, Google Street View cars inadvertently collected data from unencrypted Wi-Fi networks, including personal emails and passwords. This incident highlighted unauthorized data collection and lack of transparency. The inadvertent nature of the data collection does not absolve Google of responsibility, as it indicates inadequate safeguards and oversight.

The ethical issues in this case involve unauthorized data collection and the lack of transparency in Google's actions. Collecting personal data without consent breaches privacy and trust. The incident underscores the need for robust data governance practices and transparent communication with users about data collection activities.

F. Incognito Mode Tracking Lawsuit

In 2020, a class-action lawsuit was filed against Google for allegedly continuing to track users' internet activity even in Incognito mode, designed for private browsing. This raised significant ethical concerns about privacy and deception. The promise of privacy in Incognito mode is contradicted by the continued tracking, undermining user trust and autonomy.

The ethical implications of tracking users in Incognito mode are significant. Promising privacy and then violating it not only undermines user trust but also breaches the ethical principles of honesty and respect for user autonomy. Users rely on Incognito mode for private browsing, and violating this expectation of privacy is a serious ethical breach.

IV. Ethical Frameworks

A. Deontological Perspective

Google's data practices often violate principles of autonomy and consent. Users are typically not fully informed about the extent of data collection, which infringes on their autonomy and right to privacy. According to Kantian ethics, this is inherently unethical as it fails to respect the intrinsic worth of individuals, violating the principle of treating people as ends in themselves. Additionally, Kant's principle of the categorical imperative suggests that actions are only morally right if they can be universalized. The practice of collecting personal data without consent cannot be ethically justified as a universal law because it would lead to a society where privacy is routinely violated, undermining trust and freedom.

B. Contractualist Perspective

The implicit agreement between Google and its users is often unfair, with users not adequately informed about how their data will be used. This lack of transparency undermines trust and the social contract. Contractualists would argue that data practices should be based on fair agreements that all parties, including users, would consent to under reasonable conditions. Furthermore, the principle of reciprocity is violated as users provide valuable data without receiving fair compensation or benefits in return. The imbalance of power and information between Google and its users creates an unethical dynamic where users are exploited for their data.

C. Consequentialist Perspective

Google's services provide significant benefits, including enhanced user experience and economic growth. However, these benefits are countered by privacy invasions, potential for data breaches, and manipulation of user behavior. From a utilitarian perspective, the overall consequences of surveillance capitalism might not justify the means if the negative impacts on individual and societal well-being are substantial. The long-term consequences of widespread data collection include the erosion of trust in digital services, increased anxiety and mental health issues related to privacy concerns, and potential misuse of data by malicious actors. These negative outcomes must be weighed against the economic and convenience benefits provided by personalized services.

D. Hedonistic Perspective

While Google's services increase user pleasure through convenience and personalization, the anxiety and distress caused by privacy concerns and data misuse result in significant net pain. A hedonist would weigh the pleasure and pain resulting from surveillance capitalism to determine its ethicality. If the negative impacts on well-being are substantial, the practice might be deemed unethical. The subjective nature of pleasure and pain also highlights the diversity of user experiences. While some users may greatly benefit from personalized services, others may suffer from the constant surveillance and lack of privacy, leading to a more complex ethical evaluation.

V. Conclusion

Surveillance capitalism, exemplified by the practices of technology giants like Google, presents a complex interplay of benefits and ethical challenges. While it has led to significant advancements in personalized services, economic growth, and technological innovation, it also poses serious threats to privacy, autonomy, and democratic values. The Need for Ethical Frameworks and Regulation The analysis through various ethical frameworks—deontological, contractualist, consequentialist, and hedonistic—reveals that the core issues of surveillance capitalism revolve around the lack of transparency, informed consent, and the potential for misuse of personal data. From a deontological perspective, the intrinsic rights of individuals to privacy and autonomy are often violated. Contractualist ethics highlight the unfair agreements and lack of true consent between users and companies. Consequentialism raises concerns about the negative societal impacts, such as erosion of trust and increased anxiety. Finally, hedonism points to the net pain caused by constant surveillance outweighing the pleasure of personalized services. Implications for Society The implications of surveillance capitalism extend beyond individual privacy concerns. The concentration of data in the hands of a few corporations gives them unprecedented power to influence public opinion and behavior. This concentration poses risks to democratic processes, as seen in cases of data misuse for political advertising. Moreover, the opaque nature of data collection practices undermines public trust in digital platforms and raises concerns about the ethical use of technology. Toward a More Ethical Digital Ecosystem Addressing these challenges requires a multi-faceted approach: **Regulatory Oversight**: Governments must implement and enforce stringent data protection laws that require companies to be transparent about their data practices and obtain explicit consent from users. Regulations such as the General Data Protection Regulation (GDPR) in the European Union set

a precedent, but more comprehensive and globally consistent frameworks are needed. **Corporate Responsibility**: Technology companies must adopt ethical data practices as part of their corporate social responsibility. This includes minimizing data collection, ensuring data security, and being transparent about data use. Companies should also provide users with clear and accessible tools to control their data. **Public Awareness and Education**: Users must be educated about the implications of data sharing and empowered to make informed choices. Public awareness campaigns and digital literacy programs can help users understand their rights and the potential risks of surveillance capitalism. **Technological Solutions**: Innovation should be directed towards developing technologies that enhance privacy and security. Techniques such as differential privacy, encryption, and secure multi-party computation can help protect user data while still enabling valuable insights. Future research should focus on developing ethical frameworks and practical solutions for balancing the benefits of data-driven innovation with respect for individual rights. This includes exploring new models of data ownership, where users have greater control over their data and can choose to monetize it themselves. Research should also investigate the societal impacts of surveillance capitalism and the effectiveness of different regulatory approaches. In conclusion, while surveillance capitalism has driven significant technological and economic advancements, it comes with profound ethical challenges that must be addressed to ensure a fair and just digital society. By fostering a culture of ethical data practices, enhancing regulatory oversight, and empowering users, we can create a digital ecosystem that respects individual rights and promotes trust. As we navigate the complexities of the digital age, it is imperative that all stakeholders—governments, corporations, and individuals—work together to uphold ethical standards and safeguard the fundamental rights of privacy and autonomy.

REFERENCES

[1] P. Pulay, "Convergence acceleration of iterative sequences. the case of SCF iteration," *Chemical Physics Letters*, vol. 73, no. 2, pp. 393–398, 1980.

[2] F. Lindner, M. Mehl, K. Scheufele, and B. Uekermann, "A comparison of various quasi-Newton schemes for partitioned fluid-structure interaction," in *ECCOMAS Coupled Problems*, Venice, 2015.