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. Scenarios and Dilemmas

The spread of practices surveillance capitalism, mostly by gathering vast quantity of user data without their knowledge and consent, has steered to numerous ethical dilemmas. Before going to real life case scenarios, this section is going to explore various general cases where the benefits of data-driven technologies clash with ethical considerations. These scenarios mark the challenges of finding a middle point between innovation, user convenience, and privacy.

A. Personalised Advertising

Dilemma: Let's take the case where a social media platform uses detailed user data to deliver highly targeted ads, improving ad effectiveness and enhanced user experience.

Issue: Personalised advertising involves collecting vast amounts of user data through a large variety smart devices, like smartphones and home assistants, which gather information such as voice commands, usage patterns, location data, and biometric information. While these targeted ads can enhance user experience by showing relevant content for the users, they may not be fully aware of the amount of data collection or how their information is used, stored, or shared. This lack of transparency raises concerns about informed consent and user autonomy. The ethical dilemma here is whether the benefits of improved user experience and ad effectiveness justify the potential invasion of privacy and the risk of data misuse.

B. Smart Home Devices

Dilemma: Smart home devices, such as smart speakers and security cameras, collect data by use to optimize home automation and improve user convenience.

Issue: These smart home devices practice an active monitoring of activities within the home in a continuous way. This constant surveillance means, there is a significant privacy concern due to the full unawareness of users about the implications of having their personal lives recorded and analyzed by third parties. The collected data can include audio recordings, video footage, and also patterns of daily activities, studied and analyzed by the algorithms these devices processes the data with. It is true that these devices offer enhanced convenience and security, but they also mean a huge risk related to unauthorized access, data breaches, and the potential misuse of personal information. Therefore, this ethical issue is going to persist until a balance between the convenience provided by smart home devices and the need to protect user privacy and maintain trust is sheltered.

C. Health Data Collection

Dilemma: A fitness app give users the opportunity to collect their health and activity data to provide them personalised health insights and recommendations.

Issue: Fitness and health apps track a large set of personal health metrics, such as physical activity, sport routines, heart rate and sleep patterns. But while users benefit from personalised health advice or reminders to do fitness activities, the detailed monitoring of these health metrics can be really intrusive or not consented and there is the risk that sensitive health data could be accessed or used inappropriately. There issues arise therefore concerns about data security, confidentiality and the exposure of private users based on their health information. For that reason users may feel uncomfortable with the level of surveillance and the risk that their health information could be shared with third parties without their explicit consent.

D. Free Social Media Platform

Dilemma: A platform uses collected data of its users to personalise their feeds and enhance their interaction and experience, showing them content they probably like and ads tailored to their interests.

Issue: Social media platforms use algorithms to personalise content and ads based on previous interactions, influencing what users see and potentially shaping their opinions and behavior. While personalization of these platforms can enhance user engagement and achieve their satisfaction, it also raises concerns about autonomy and manipulation. This is because users might be unknowingly guided by recommendations or publications selected by a fine-tuned algorithm, creating a close space where they are only exposed to information that reinforces their existing beliefs. This can lead to polarization and a lack of exposure to diverse perspectives. That is the problem of this situation, that these algorithmic processes are not transparent and can impact on user autonomy. Additionally, the concentration of power in the hands of platform operators raises concerns about accountability and the potential for abuse, mainly for using this power for political and ideological indoctrination.

III. Case Studies

Has we have seen in the previous section of this paper, there are many scenarios where it is shown that there are benefits as efficiency and enjoyment. But they come at the cost of demanding the user data as an essential part of the architecture of these platforms, whose business model is the surveillance capitalism. For that reason, this paper is going to analyse real case scenarios, where this practice was exposed to the public and what was their reaction.

A. Scandal of Cambridge Analytica

One of the most prominent examples of how personal information was misused for political purposes occurred with the case of Cambridge Analytica, a political consulting firm. Even though it started in 2016, it was first revealed in the year 2018 that the personal data of millions of Facebook users was harvested by Cambridge Analytica [1] without their consent. This data was used to build psychological and demographic profiles to target individuals with personalized political propaganda during the president US election in 2016 [2] and the Brexit referendum. It was then exposed through this scandal how many ethical and legal issues surrounding data privacy was happening without public knowledge and that political manipulation was a reality not many were aware of. The scandal exposed significant ethical and legal issues surrounding data privacy and the use of personal data for political manipulation. Facebook faced then intense regulatory investigations as well as numerous trials for its role in the data breach and its failure to protect user privacy. The incident highlighted the lack of transparency in facebook's platform engines and the negligent oversight in data collection practices. For that very reason, many facebook users deleted their accounts and the platform lost its popularity, particularly the facebook social media app. This was not only because of the lack of integrity and transparency, but also due to the growing mistrust and concerns about the influence and manipulation of social media platforms on democratic processes. The ethical implications of the Cambridge Analytica scandal are many. On the one hand, the social network is presented as a free way to connect with other people and to subscribe to many pages where this people shares their interest. It is about connecting people, as their slogan always said, but on the other hand, it was shown that robust data protection laws and greater accountability for companies that collect and use personal data weren't priority until cases like this happened. The incident also emphasizes the importance of informed consent and the ethical responsibilities organization should follow, if their business model handles sensitive information about users as well as if they can be used for political or ideological manipulation.

B. Incognito Mode Tracking Lawsuit

In June 2020, a class-action lawsuit was filed against Google and its incognito mode by web browsing [3]. These accusations were alleging that the tech-company was tracking the internet activity and behavior of its users, even when they were using Incognito mode. It is important to add that this feature was designed and advertised for private browsing. The lawsuit also claimed that Google was harvesting this user information through various tools and means, such as Google Analytics, Google Ad Manager, and website plug-ins. Those features of the search engine were operating in the incognito modus too without knowledge of users and the plaintiffs argued that this was violating federal wiretap laws and California laws for privacyö With this lawsuit, many people became aware about significant ethical concerns about privacy and deception. Incognito mode was perceived by many users as a way to browse the internet without leaving a tack of their activity, but this promise was contradicted by the these practices now shown to the public, undermining trust among the users. Users who relied on Incognito mode to protect their privacy felt deceived and exposed. The ethical implications of tracking users in Incognito mode are considerable. Not only because the deceiving promise of privacy, but also because it breaches the ethical principles of honesty and respect for user autonomy. Trust is a fundamental component of the user-technology relationship, but trust is eroded when both parties aren't transparent. Furthermore, the lawsuit highlighted issues related to informed consent, because users were not fully informed about the large amount collected of data in Incognito mode. This collection without explicit user consent violates privacy rights and can lead to misuse of personal information. But this case also brought attention to the broader implications of data collection practices by tech companies. For instance, more people were aware of how important it is the need for greater transparency and accountability in how user data is collected and, more important, if it is with consent. For that the lawsuit called for stricter regulations and enforcement to protect user privacy and ensure that companies hold their privacy promises.

C. Apple and the San Bernardino Case

Apple was involved in a legal battle with the FBI for unlocking a device manufactured by them in 2016 [4]. The suite was about whether Apple should help unlock the iPhone of Syed Rizwan Farook. This person was one of the perpetrators of the San Bernardino terrorist attack in December 2015, attack resulted in 14 deaths and 22 injuries. Due to the magnitude of this event, federal investigation was involved.

Apple's assistance in bypassing the iPhone's security features was asked by the FBI in order to access potential evidence, that could be used against Rizwan for the case related to the terrorist attack. The FBI wanted Apple to create was a special version of iOS where certain security features would be disabled, such as the auto-erase function after ten incorrect password attempts. Actually with this modification, the FBI would be able to use brute force to get the iPhone's passcode and access its content. Apple refused the request, citing concerns over user privacy and security. The company argued that creating a backdoor to the iPhone would set a dangerous precedent which could be exploited by many malicious people, hackers and private or government agencies, which could potentially compromise the security of all iPhone users.

The ethical implications of this case were again significant. On one hand, there was a good intention in investigating a serious and dangerous terrorist, which could prevent attacks future incidents. But on the other hand, creating a backdoor means severe risks to user privacy and data security, specially from a company known for its dedication to privacy. Therefore, Apple stood for protecting the security and privacy of its users, even when that implied that the company should give

up helping the society by unlocking this single device for law enforcement purposes. The case started also a nationwide concern on privacy and security as well as how justified is the government authority in accessing private data. Important questions like those and about the balance between national security and individual privacy rights were raised, even though the FBI found an alternative method to unlock the iPhone without Apple's assistance.

Here we could see of tech giants handled collected user data within their ecosystems. While Facebook and Google have faced significant criticism and regulatory scrutiny over their data practices, Apple has taken a more privacy-focused stance. The contrast between these companies remarks different approaches to how user data should be handled and privacy concerns really matter to these companies, with Apple emerging as a proponent of robust data protection and user privacy. But this does not have to be necessarily the best approach, since threats to our society should be avoided. Therefore, in the next section of the paper, these scenarios and dilemmas are going to be discussed through many ethical lenses, reminding the importance of privacy in the digital age but also what is the best for final users.

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 ethical point of view. 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 presents a complex interplay of benefits and ethical challenges. While it has led to significant advancements in personalized services, economic growth, efficient advertisement and technological innovation, it also has shown to threat ethical values as privacy, autonomy, and democratic practices.

The analysis through various ethical lenses as deontological contractualism, consequentialism, and hedonism reveals that the main issues of surveillance capitalism revolve around the lack of transparency, informed consent, fair conditions and the potential misuse of personal data. For contractualist ethics, the unfair agreements, lack of true mutual consent between users and companies and violation of individual rights to privacy and autonomy are condemned neglect practices. Consequentialism raises concerns about the negative impacts on the society, such as growing distrust and increasing anxiety. Finally, hedonism points to the total pain caused by constant surveillance outweighing the pleasure of personalized and targeted services.

But the implications of surveillance capitalism even extend beyond individual privacy concerns. The huge accumulation of data in the hands of few corporations gives them unprecedented power to influence public opinion and behavior, which endanger democratic processes, as seen in cases of data misuse for political advertising. Moreover, the obscure nature of data gathering practices tears down public trust in digital platforms. And it additionally reuses concern about the ethical use of technology.

Therefore, a multi-faceted approach is needed to address these challenge:

Regulatory Supervision: Governments must implement and enforce strict data ownership protection laws that require companies to be transparent about their data collection practices,

what they do with that data and explicit ask for consent from users. Regulations as the General Data Protection Regulation (GDPR) in the European Union should play a role as precedent, but more inclusive and globally consistent structures for this regulation are needed.

Corporate Responsibility: Tech companies must follow ethical data collection practices as part of their social responsibility. This includes minimizing data collection following a need-to-know approach. Ensuring data security for preventing data leaks and being transparent about data use are key for user trust. Companies should also provide users clear and accessible tools to monitor and control, how much of their data is being collected.

High-tech Solutions: Innovation should aim the development of tools and technologies that enhance privacy and security. Techniques and procedures as differential privacy, encryption, and secure multi-party computation can help the security and integrity of 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 and the right of individual for privacy and transparency. This includes exploring new models of data ownership, where users can have a much better control over their data and can choose whether to monetize it themselves or just avoid its collection. In conclusion, while the business model of surveillance capitalism has pushed the development of significant technological and economic advancements, it comes with keen ethical challenges and issues that must be addressed to ensure a fair digital society. By fostering a culture of ethical data collection practices, enhancing regulatory oversight, and giving users power over their own data, we can create a digital ecosystem that respects individual rights and enhances trust.

REFERENCES

[1] C. Cadwalladr and E. Graham-Harrison, "Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach," *The Guardian*, March 2018. [Online]. Available: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[2] M. Rosenberg, N. Confessore, and C. Cadwalladr, "How trump consultants exploited the facebook data of millions," *The New York Times*, March 2018. [Online]. Available: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

[3] N. Autor, "Google settles 5 billion dollar privacy lawsuit over tracking users in incognito mode," *The Hacker News*, January 2024. [Online]. Available: https://www.thehackernews.com/2024/01/google-settles-5-billion-privacy.html

[4] K. Benner and E. Lichtblau, "Apple fights order to unlock san bernardino gunmans iphone," *The New York Times*, February 2016. [Online]. Available: https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html