SCRIPTA
Volume 1, Number 2, Fall 2022
ISSN: 2769-9242

Does Data Privacy Even Exist Anymore?

Yujun Kim*

Abstract

Facebook. Google. Zoom. Names such as these dominate today's digital world. As the role technology plays in people's lives continues to increase, concerns regarding personal privacy have become more prevalent than ever before. From the mining of personal data to targeted content and product placement, it appears that every aspect of a consumer's digital use is monitored, tracked, and viewed as a potential source of profit. This has resulted in significant consumer distrust as the multitude of scandals involving major corporations continue to come to light. Consumers must implement strategies to protect their private data and companies must take steps to rebuild trust with their customers.

1 Introduction

In an age where the use of technology is inescapable, concerns over personal privacy have been rising tremendously. From apps harvesting personal data for research purposes to targeted advertisements analyzing every minute detail of a consumer's history for targeted product placement, it seems as if nothing one posts or searches for online is untraceable, or even unprofitable. Such endeavors have caused significant civilian distrust in major corporations, leading to the volatile exposés of some of the technology industry's most influential leaders. Over the past two decades, multiple studies have been conducted exposing the extent to which this distrust plagues everyday lives. Furthermore, legal scandals regarding the proper usage of consumer data against major companies such as Facebook, LinkedIn, and Google have made headline news.

*Junior Student, Fulton Science Academy.
Contact: ykim@fultonscienceacademy.org

These bizarre and oftentimes unethical strategies corporations employ in harvesting consumer data for their own research purposes caused more consumer disdain, garnering media attention and calling for a change of an unsafe system that is becoming increasingly ingrained in people's lives. Nonetheless, there are steps consumers can take to protect themselves from having their information leaked.

Understanding the importance of such issues will facilitate a crucial discussion regarding user privacy, and create a new browsing era based on trust between the hosts and consumers of internet media.

2 Controversy

Over the past few years, many analyses have been conducted to research the extent to which companies protect user privacy; the results were surprising. When cross-referenced with data discussing the degree of trust between the users and corporations, an apparent yet alarming painting started to come into view.

On the business side, companies are continuously escalating the amount of data they collect from their online customers. According to KPMG, nearly 70% of the companies analyzed had expanded their collection of personal consumer data [1]. With technology consistently on the rise, a meteoric uptick in collected information from everyday users can be concerning, especially when the companies themselves are not even trying to hide how their data collection methods are suspicious. In fact, nearly 29% of companies admitted that the strategies they use to collect data are "sometimes unethical," and another 33% stated that consumers should be worried about such methods [2].

Large corporations such as Google and Facebook are conscious of the damage data mining can bring to the general population. When interviewed, executives at these companies were privy to this fact, as 70% of them insisted that the amount of personal information their businesses collected has skyrocketed over the past few years without much intervention [2]. Nevertheless, these titans agree that mediation is crucial, as 62% of executives indicated that their companies needed to do more to protect their users' data in an ethical and understanding fashion [2].

However, this is not the message that is being spread to their customers. When engaging in client relations, these same corporations painted a different picture of the uses of personal data in their workforce. While 51% of U.S. adults

were fearful of their data being sold, only 17% of the companies interviewed admitted to participating in this practice, insisting that this consumer fear was unreasonable, and not a major cause for concern [1].

With such extreme miscommunication between corporations and the public, it seems apparent that the average American has developed a lingering distrust for the companies whose services they utilize every day. While consumers are generally aware of the unethical practices used against them, they feel powerless to stop the spread of their personal data. When interviewed, about 60% of American adults insisted that it is nearly impossible to go through a daily routine without having some form of personal data collected by private or government-funded companies [3]. The potential usage of the data is also concerning. 79% of consumers report feeling as though they have little or no control over how their information is spread and utilized [3]. Furthermore, consumers feel as if they have no idea what the government does with the data it collects, with 78% expressing this as a cause of concern [3]. Nearly 84% of consumers attest to feeling this way and can justify their fears through the extent of targeted advertisements they receive on their personal devices [3].

Targeted advertising has been a topic of discussion for many years now, as companies often use the data they collect to deliver personalized advertisements to their customers in hopes of increasing revenue. Through analysis of search history and prior purchases, companies use targeted advertising in hopes of attracting customers back to the business. The precision of targeted advertising is quite astounding. When asked, 61% of constituents who saw curated ads based on their personal data insisted that they accurately reflected their interests and characteristics to some extent [3].

With such expansive data mining, it is no surprise that the trust between citizens and corporations is on extremely thin ice. Furthermore, with the various instances of data breaches in major companies, citizens' privacy continuously dwindles as technology advances further into the future.

3 Examples of Data Privacy Breaches

Over the years, many companies have been subject to severe litigation due to malpractice regarding private consumer data. Industry giants such as Zoom, LinkedIn, Facebook, and Google have come under scrutiny for allowing client data to be leaked, leading to severe negative consequences for their customers.

Case studies regarding examples of such businesses have been conducted, and the results are horrifying.

According to The New York Times, Zoom secretly engaged in data mining during conversations, transmitting personal data to match the consumer's LinkedIn profile. While this only occurred with the help of a subscription-based tool named LinkedIn Sales Navigator under the premise of assisting with marketing, clients soon found out that even under supposed anonymity, their account details were not private [4]. This is because even when someone signed into a Zoom meeting under an anonymous alias, this extension still uncovered their LinkedIn profile [4]. While Zoom promised to disable and remove this tool, it goes without saying that the effect it had on people's trust in the company was detrimental Not only was this tool uncovering the identities of the users, but it was also cross-referencing it to another social media platform, indicating that it truly held none of the clients' data in a safe place unable to be penetrated by other corporations.

Unfortunately, LinkedIn has experienced issues with privacy, as a data breach involving over 165 million accounts was brought to light. This data was allegedly reported to be up for sale on the dark web marketplace, leaving users vulnerable [5]. If such influential companies cannot protect the integrity of their client's data, it is no wonder that trust has dwindled to such an extreme degree. As social media companies know much about their users due to the posting of highly sensitive and personal information, any breach or scandal can have damaging consequences including wide-scale data leaks. If placed into the wrong hands, knowing this information may lead to increased global instability and political conflicts.

LinkedIn was not the only social media company struck by a data scandal, as Facebook's role in its Cambridge Analytica Data Harvesting legal suit was also consequential. In this landmark case, an investigation carried out by government officials exposed that Cambridge Analytica utilized a third-party app to collect data from a Facebook Quiz for political purposes [4]. Such blatant dishonesty regarding the use of data came as a complete betrayal to many consumers who have extensively used this social media platform. Nevertheless, this led to the Federal Trade Commission fining Facebook $5 billion for this violation, which was the largest sum ever paid as a fine for a consumer privacy scandal [4].

Political opinions are not the only form of data at stake and adults are not the only ones impacted. Recently, Google was accused of violating children's

privacy laws by disregarding the Children's Online Privacy Protection Act that required parental consent before gathering data from minors less than 13 years old [4]. In this case, students asserted that the G Suite for Education platform collected biometric data without consent, possibly affecting millions of students trying to learn online [4]. Significant measures must be taken to ensure that children's information is not used for purposes not outlined in user contracts, especially for school-mandated services and educational tools.

In fact, companies prioritizing the security of their clients have been caught in similar schemes, violating the values they believe in. One example is the Ring Doorbell, a product that allows users to see all of the guests coming into their homes, as well as monitor the activities going on around their homes. However, the system itself is riddled with multiple trackers. When the Electronic Frontier Foundation investigated the Android version of this application, they discovered that many of these tracking programs came from third-party companies [4]. Ring sent this data to four outside entities, giving them access to personally identifiable information about their clients [4]. According to the article, "the transmitted details include names, IP addresses, and data from users' device sensors" [4]. With such extensive knowledge, it remains incredibly easy to get a full picture of the clients' lives, habits, and personal details. As a company primarily concerned with home security and safety, the carelessness with which they sell the data of their users to other companies completely undermines their initial goal, as this "unlawful data-mining" makes their consumers more vulnerable to threats and compromises their protection.

4 Consumer Mitigation Strategies

With so many companies abusing their user privacy rights, it may be increasingly difficult to determine which are trustworthy and which are not. Therefore, there are a variety of strategies consumers can employ to remain safe and mitigate the various effects that data mining can have on them in the future. While browsing, consumers can implement different solutions to protect their online privacy. For example, turning off ad personalization removes the permission for companies to participate in invasive tracking [6]. In return, consumers can browse the web without their search history being cataloged for specific product placement. It is also helpful to use the browser whenever possible, as apps participate in a lot more tracking than most websites do [6]. Removing unused

apps from personal devices significantly decreases the risk of being tracked.

Furthermore, consumers can utilize advanced and downloadable security software to reduce the risk of obtaining a virus on a personal device. Even though viruses have become less common over the years, setting up antivirus software, especially on Windows computers, can preserve the privacy and integrity of users [7]. Through these solutions, internet users can feel a lot safer, removing possible trust issues they accumulated in the company's websites of the companies that they most visit. Employing these techniques minimizes the risk of personal data becoming leaked, and fights against the increasingly unethical strategies websites used to obtain personal information.

5 Conclusion

As the Internet is integrated into most people's daily social and work lives, the discussion of Data Privacy cannot be taken lightly. The multitude of scandals involving influential corporations undoubtedly instilled fear and distrust in the eyes of the masses, causing outbursts regarding the security of private data these companies have been entrusted with. From social media companies inadvertently selling information on the dark web to home security companies violating the personal privacy of the very people they vowed to protect, much improvement is necessary to rebuild trust between the consumer and company. Nevertheless, these consumers must invest in different strategies to keep themselves safe from having their private data pillaged. From anti-virus software to minimizing the utilization of data-tracking apps, there are always ways to ensure that information remains private despite the grip that the digital age has placed upon society.

References

[1] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. 2019.

[2] J Kahn. Be afraid: Executives warn about personal data harvesting and use. https://fortune.com/2021/08/24/eye-on-a -i-data-privacy-unethical-kpmg-survey/, Aug 2021.

[3] Staff T. R. Shein E. Miles B. Eckel E. Asay M. Whitney, L. Data privacy is a growing concern for more consumers. https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for- more-consumers/, Aug 2021.

[4] Doherty. These real-world data breach examples will make you rethink your data strategy. https://www.doherty.co.uk/blog/data-breach-examples-rethink-your-data-strategy, Sep 2022.

[5] Cybernews. 6 examples of online privacy violation. https://cybernews.com/privacy/6-examples-of-online-privacy-violation/, Sep 2021.

[6] L Wamsley. Your technology is tracking you. take these steps for better online privacy. https://www.npr.org/2020/10/ 09/922262686/your-technology-is-tracking-you-take-these-steps-for-better-online-privacy https://www.npr.org/2020/10/ 09/922262686/your-technology-is-tracking-you-take-these-steps-for-better-online-privacy, Oct 2020.

[7] The New York Times. Guides. https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy.