Proceedings of the 3rd International Conference on Business and Policy Studies
DOI: 10.54254/2754-1169/80/20241833

Analysis of Principles and Tactics Behind Data-Tracking

Zijun Zhao[1,a,*]

[1]*Business of College, City University of Hong Kong, Tat Chee Avenue, Sham Shui Po, Hong Kong S.A.R China*
a. zijuzhao3-c@my.cityu.edu.hk
**corresponding author*

Abstract: As the applications and their scope developed by several major technology firms such as Alphabet and Meta advance, these companies are found to be facing compliance issues due to increasing user concerns about privacy. The research investigates the tactical strategy utilized by these companies in addressing the relevant problems and allegations and then offers recommendations for effective tactics. Based on the principles of novel and previous tracking tools, the research analyzes the disadvantages of current innovative tools and discovers a developing orientation according to the main dimensions of user psychological analysis, transparency issues, and problems linked to advertising arrangements. The implication highlights the possible factors that contribute to users' concerns and the essential aspects to enhance the safety measures of these extensively utilized platforms.

Keywords: Data, Track, Privacy Concern, Compliance, Strategy

1. Introduction

Ever since the wide availability of computers, electronic devices have consistently been impacting the daily lives of individuals. Emerging technologies such as data, software, apps, and social media continued to gain awareness and flourish rapidly. The increasing use of the Internet has led to a corresponding rise in concerns regarding the online collection and usage of consumer data[1].

Aiming to enhance convenience in individuals' lives, various companies have developed a wide range of apps based on the platform provided by electronic devices. These apps have been adopted in practically every dimension of people's daily routines. With the increased maturity of electronic devices and data, these gadgets and relevant apps have evolved to be more intelligent and convenient. Furthermore, in order to further develop their comprehension of users' preferences and subsequently offer improved services according to the examined preferences, the majority of apps started to actively gather users' information through app usage.

However, individuals are observed to be concerned about privacy issues while using intelligent apps when the awareness of the condition that their private data had been collecting by these large-scale companies raise in the present era. In addition, some upper companies that have prospered by developing widely used apps also have been facing legal liability-related issues recently, which has also amplified the public's concern about relevant privacy issues. As a reaction to this circumstance, several companies have wisely modified their approaches for monitoring users' data and made efforts to prevent such circumstances from occurring again.

DOI: 10.54254/2754-1169/80/20241833

This essay argues that these dominant players' extensive data-driven marketing practices benefit from the monopoly, copious crucial alternations of intelligent tools, and cunning evasion of legal sanction. Additionally, it will focus on the strategic recommendations for these companies in light of the current circumstances.

2. Historical Context of Data Collection

2.1. Initial forms of data collection

Even though the public has just begun to focus on personal privacy recently, collecting users' data is not a novel concept. HTTP cookies, virtually known as cookies, have been utilized since the late 1990s[2]. As Hormozi points out[3], "A cookie is a small text file that is saved on a user's hard drive by a Web server". Cookies serve the purpose of tracking user activities and gathering this information as stored data. Typically, cookies can be divided into two types: First-party cookies and third-party cookies.

First-party cookies are installed on the website by their owner, and the collected data is used to memorize user settings and preferences[3].For instance, a customer accidentally leaves the website after selecting an option. When he reopens the website, it may be perceived that the option is still chosen. Apparently, the notion of a first-party cookie is based on the action taken by the owner of the website.

Meanwhile, the third-party cookie is often created by individuals rather than the owner, mostly to achieve advertising purposes. Its main objective is to facilitate adware and data-gathering platforms in targeting potential customers with customized advertisements as website users move across different websites, utilizing their online activities as a basis[4].

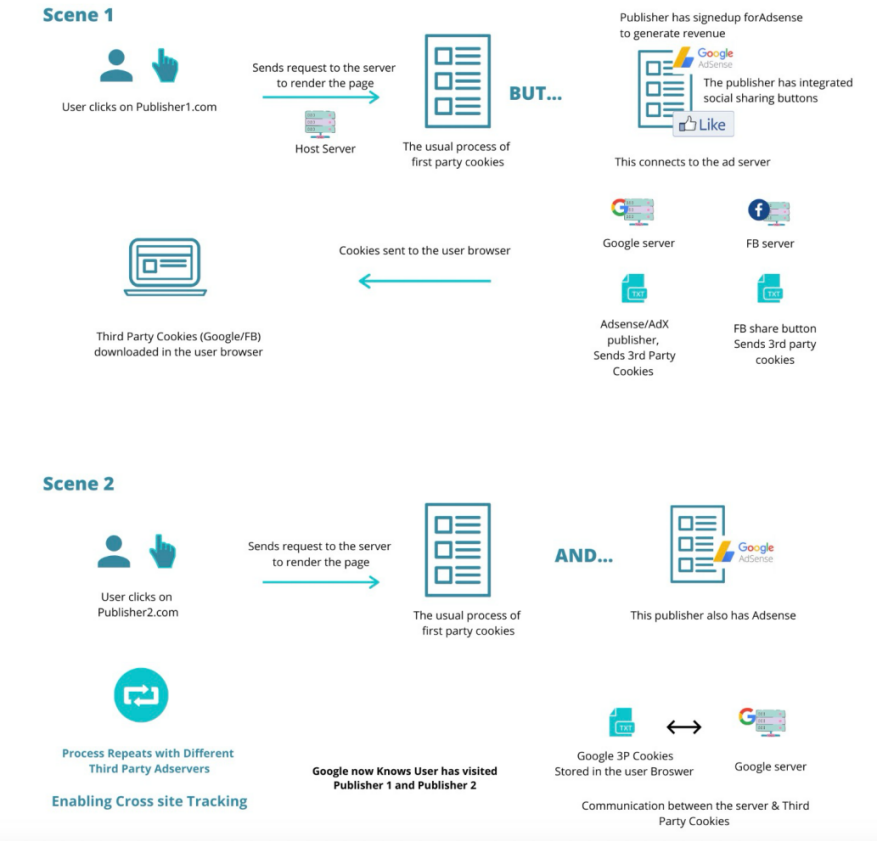

Figure 1: The principle of third-party cookies (Source: Madmartech)

DOI: 10.54254/2754-1169/80/20241833

2.2. New Era

Initially, various companies engaged in the most widely favored websites as third-party cookies users with the aim of advertising and promoting brand images. However, the phasing out of third-party cookies for advertising has already begun. With the increase in mobile website browsing, it becomes increasingly difficult to track users penetrating different devices, which means the data needed for analyzing users' profiles is challenging to gather [5]. According to prevailing perceptions, online advertising organisations have made efforts to enhance the dependability of their tracking mechanisms [6].

3. Modern Innovation of User Behavior Tracking Framework

Since technological innovation took place in the modern world, to address individuals' growing concerns of privacy problems simultaneously, leading technology companies have modified their tracking methods to more effectively track users' behavior and ensure their policies and strategies are more compliant to a certain extent. Despite significant alterations of monitoring strategies that some leading companies have already taken, several relevant circumstances are still perceived to be problematic for the further development of companies, mainly involving two key dimensions -- public perception and legal considerations.

4. Deep Dive into Current Leading Approaches

4.1. Meta

4.1.1. Background

Meta, which used to be known as Facebook, is one of the major technology companies around the world that has exerted a significant impact on individuals' daily lives ever since the founder, Mark Zuckerberg, first created Facebook at Harvard University during his college years. Zephoria's analysis reveals a 16 percent increase in monthly active users of Facebook compared to the previous year[7], which demonstrates Facebook's prevailing position in the current software business. In 2018, Facebook faced a formidable issue that the data of users, which had been collected by the company, was gained by a voter-profiling company. The startling truth that 87 million users' data had been gathered by this upper company was first brought to this unprecedented level of exposure as long as Zuckerberg went to Congress to illustrate the event's details. "It doesn't matter whether you have a Facebook account", from Ms.Dingell, a congressional district from the Democratic Party.

4.1.2. Innovative tool

In contrast to cookies, Meta employs specific software tools to track its users, which is virtually known as Pixel -- invisible code inserted into other websites to enable Meta and the website to monitor users' actions [8]. The principle of Pixel is not obscure to interpret. Similar to third-party cookies, Pixel enables Meta to achieve the tactic by designing the "Like" and "Share" buttons system. Meta has the capability to collect data regardless of whether users click buttons or not: The user's option to click the button means whether the page appeals to the user or not.

DOI: 10.54254/2754-1169/80/20241833

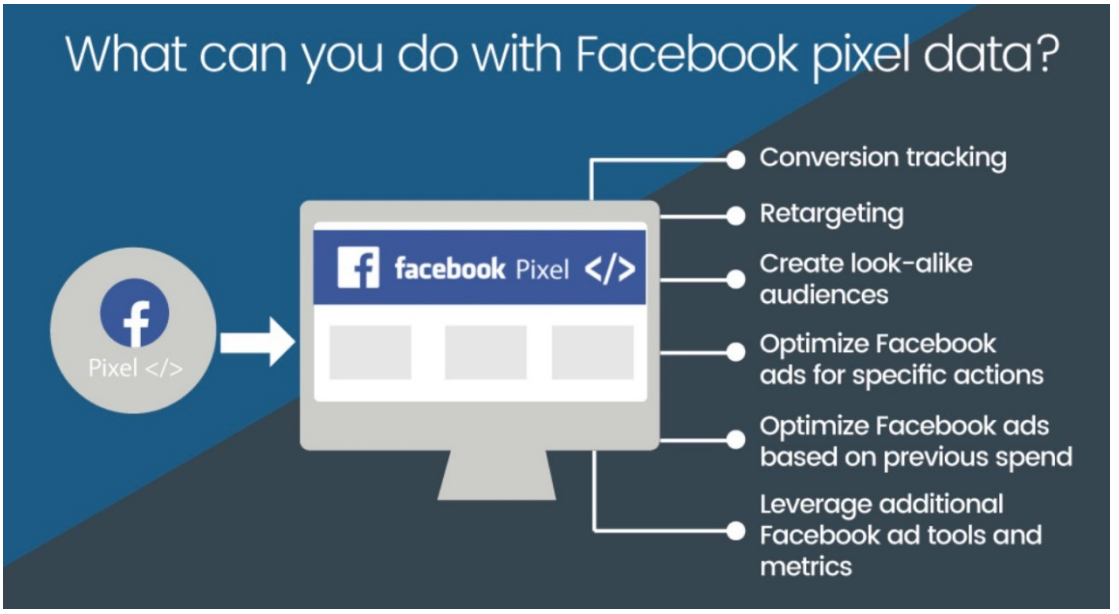

Figure 2: The function of Facebook pixel data

4.1.3. Impact

As Meta's impact on the ads industry increases, the strategy attracts curious advertisers to invest in Meta to gain potential consumers from the data-collecting system. According to an analysis of Meta's sum of business from Guoxin Security (2023) [8], the total sum of 2022 is 116 billion dollars, and the majority source of operating revenue is Family Apps, of which advertising accounts for more than 95%. The foundation of the strategy and the use of Pixel is the wide use of apps created by Meta, such as Facebook and Instagram. Most advertisers require a platform to gain space to spread the company image to obtain advantages.

4.2. Alphabet and Google

4.2.1. Public concern

Switching the gear to another major technology company -- Alphabet, with a renowned used name, Google. Unlike Meta, when users are engaging in Chrome, the browser invented by Google, they would be asked about their consent to receive advertisements. Alphabet asserted that the firm would prioritize users' public privacy. However, according to Alphabet Announces Second Quarter 2023 Results (2023, p.2), the advertising industry valued 77.93% of all revenues last quarter. In this case, the concern of how the company's can generate such an ocean of revenue and the suspicion of the statement previously cannot be avoidable.

Table 1: Revenues of Google (Source: Alphabet Announces Second Quarter 2023 Results)

	Quarter Ended June 30,	
	2022	**2023**
Google Search & other	$ 40,689	$ 42,628
YouTube ads	7,340	7,665
Google Network	8,259	7,850
Google advertising	56,288	58,143
Google other	6,553	8,142

DOI: 10.54254/2754-1169/80/20241833

Table 1: (continued).

Google Services total	62,841	66,285
Google Cloud	6,276	8,031
Other Bets	193	285
Hedging gains (losses)	375	3
Total revenues	$ 69,685	$ 74,604
Total TAC	$ 12,214	$ 12,537
Number of employees	174,014	181,798

4.2.2. New monitoring strategy

With the increasing remonstrance of privacy issues from users in the past few years, Apple also altered its tracking transparency to transform the advertising landscape. Hence, Google discontinued the application of third-party cookies as other browser companies and instead transformed into the invention of a new technological monitoring tool, first named FLoC. In response to the negative repercussions on the public, Alphabet introduced an innovative novel tool, Topics. In simple terms, the principle of Topics is that it utilizes an individual's browsing history to analyze his preference and then links to the advertising system. As the product manager of Chrome points out, Topics is a platform that allows websites to display targeted advertisements while protecting users' privacy without resorting to converting monitoring methods such as browser fingerprinting [9]. Including decreasing data, noising data, and omitting potentially sensitive topics, Topics announced that Google had already made a significant alteration to protect users' privacy in contrast to third-party cookies. "Today, we're excited to share some of the latest improvements to the Topics API. We believe these changes will make Topics even more useful to the digital advertising industry, without compromising user privacy" [9].

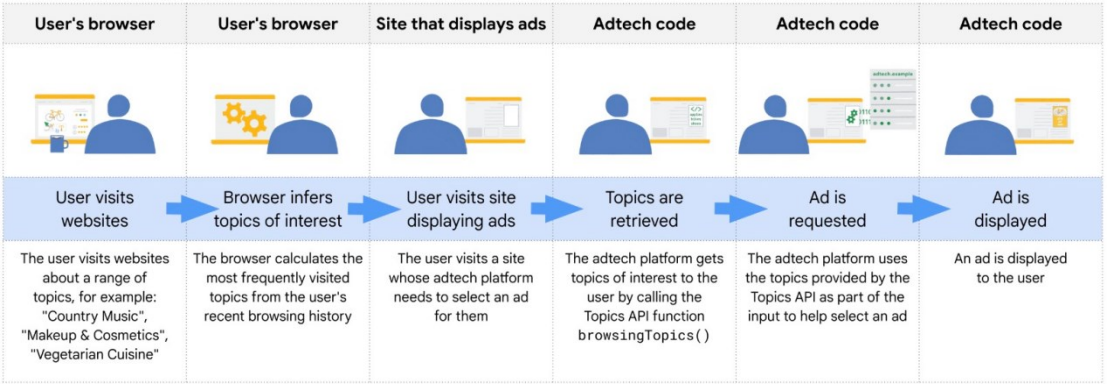

Figure 3: The principle of Topics API

5. Challenges and Public Perception

5.1. Privacy concerns

Nevertheless, even though the efforts made by upper companies such as Alphabet and Meta seem to encounter the privacy issue effectively, further problems still continue to arise. Take Alphabet as an instance, critics indicate that the tremendous fingerprinting of Chrome users had already been widely gathered, and the essence of the privacy-protecting strategy is still user-monitoring. It is perceived

DOI: 10.54254/2754-1169/80/20241833

that advertisements still appear occasionally after Chrome announces the enhanced advertisement privacy in Chrome. Furthermore, the distinction between Alphabet and Meta is the range of products. Alphabet possesses various products nearly among all dimensions of individuals' lives, Google Maps, Gmail, YouTube, and currently the most widely used browser -- Chrome, as mentioned above. Among these apps, users' information such as position history, information from other people (Occasionally combined with significant information such as school or employment information), and website history. Despite the manager claimed about decreasing data and omitting sensitive topics in Topics, the definition of data that is supposed to be decreased and topic which is sensitive remains unclear.

5.2. Inappropriate advertising arrangements

Furthermore, personalized advertisements are emerging on "made for kids" channels constantly. The Children's Online Privacy Protection Act requires websites to gain parental approval preferentially and then can collect children's data legally. As Woollacott reported, a group of children's advocacy organizations is raising an investigation from the Federal Trade Commission of this issue, asserting that advertisements are being illegally served to children [10]. "It's not the first time the company has come under fire over similar issues", in 2019, the company Alphabet paid 170 million dollars to resolve the claims of inappropriately collecting children's data [10].

5.3. Psychological analysis

Moreover, psychologically, individuals are observed to retain the default option when a page with complex concepts and options occurs. Laziness is not the reason behind the action, in the opposite, most individuals launch a website with an intense purpose. In this case, any excess items seem to be unnecessary. In this way, when the privacy issue setting page emerges, most people tend to select the option of remaining default instead of setting seriously as their personal preferences of the privacy item. This is why individuals who had chosen the accepting option still may have unsatisfactory emotion about the issue subsequently. Consequently, despite the fact that the action taken by these companies appears to be innovative, the feedback from the public and the cases had been addressed reveal that the problem of privacy issue is still supposed to be in progress.

6. Legal and Policy Considerations

Furthermore, the presence of relevant policy cannot be disregarded. Prior research has indicated that approximately 70 to 80% of websites in the United States possess privacy policies[11]. According to the policy from the California Consumer Privacy Act, explicit permission is required for major technology companies to collect users' data by 2022. Another requirement is to promote the definition and principle of cookies to consumers because most consumers are unaware of the notion of cookies and how they are applied in the advertising industry.

As a matter of fact, websites face significant civil and criminal consequences if websites lack transparency. Apparently, the implementation of the novel policy limits the application of third-party cookies and also raises the risks of facing punitive consequences while using third-party cookies in a profitable way. In addition, the US's digital advertising industry, valued at around 152 billion dollars, tends to lose access to most third-party data, which means an urgent need for those companies to alter their data-gathering strategy and then develop a new advertising tactic.

DOI: 10.54254/2754-1169/80/20241833

7. Strategic Recommendation for Companies

Hence, to address the derivative problem of the privacy issue, it is necessary to clearly identify the dimensions that have an influence on the approach.

7.1. Enhance transparency

Even though these tactics promulgated have already been modified to be more democratic in contrast to third-party cookies, it is striking to perceive that several definitions and concepts, such as sensitive and private data, are still vague. Apparently, despite the ambiguity, it may not be employed intentionally as one of the strategies. However, it would still be recognized as a cunning action for generating income from users due to the profitability of these wealthy technology companies.

7.2. Compliance

Given the current situation, compliance has the priority of being one of the most crucial issues to be first considered. Many policies have been issued since the privacy issue first emerged in the public eye. Companies should realize that legal sanctions can be exceedingly formidable to a firm's marketing position and public reputation. Privacy concerns, one of the most critical subjects for a company's growth, are expected to persistently emerge in newly published policies. Hence, it is important to conduct periodic checks of compliance inside the organization to ensure vigilance and prevent involvement in investigations, which might potentially result in adverse effects on public perception or, worse still, being outperformed by rivals.

7.3. Address safety concerns

The general belief among the public is that safety concerns are still significant issues that companies must consider. Taking Meta as an example, the reason behind the collection of users' data by the voter-profiling company is still a mystery, with two possibilities that may account for it: The first one is that Meta intentionally sold the data to them as most suspected; And the other one is that there existed a leak of its safety system which led to a theft of the data. Additionally, a large-scale development of firms' safety systems needs to be taken into consideration. If we compare data to jewelry, then the entire company should be treated as a highly secured treasure vault. It is enterprises' responsibility to provide users with satisfying data protection in order to gain faith in them.

7.4. Necessary consumer education

Due to the current situation, it is striking to observe that most individuals still do not fully interpret the notion of private issues. Existing scholarly literature indicates that the key motivations for revealing sensitive information via mobile applications are the acquisition of necessary knowledge and the satisfaction of social requirements [12]. Therefore, relevant companies should be obligated to launch educational initiatives about the privacy practices to consumers based on widely used applications employed by them. According to the psychology study in the last paragraph, a novel version of the private issue announcement should be developed in order to achieve the educational goal. An answer to a crucial problem needs to be emphasized that the purpose of publishing an announcement should not only make it visible to users but to enable users to interpret it. The design of the announcement could be altered into a "Big page, Few words" form with information that could be page-turning. Moreover, it may be beneficial to include a privacy test at the end of these pages as a requirement for consumers to make sure they understand them. This improvement could not only mitigate the potential problems of the use of users but also serve as an intense positive response to the demands of legal and government agencies.

DOI: 10.54254/2754-1169/80/20241833

8. Conclusion

In conclusion, as the most influential companies worldwide, satisfying consumers' demands and fulfilling legal requirements are the prerequisites for generating revenue. Companies should emphasize respecting and upholding user rights while providing convenience and services. They also have a responsibility to strike a balance between advertising strategies and addressing customer concerns. As artificial intelligence advances, electronic devices continue to evolve rapidly and have a lasting impact on people's lives. It is advantageous that individuals are increasing their comprehension of privacy concerns while using intelligent applications. This not only encourages enterprises to prioritize privacy issues, but also facilitates the oversight of company expansion, in case the probable negative impact of technology company monopoly on the industry. Moreover, the ensuing consequences of increased awareness of privacy concerns may also promote the enhancement of relevant laws and legislation.

Furthermore, the latest situations reveal the drawbacks of the current systems employed by organizations. The drawback revealed that there are two obstacles impeding the progress of enterprises: user concerns and legislative organization concerns. To address the limitations, it is necessary to implement a rotation of marketing tactics. Revise strategies to align with recently implemented legislation and improve the transparency of the operational principles of intelligent tools, while reinforcing the essential education for users to safeguard their rights. As the leading enterprise expands and evolves, a multitude of issues will inevitably emerge. The priority should be focused on developing the most effective and reasonable solutions to the difficulties that emerge. Enhancing in this way would not only assist in mitigating difficulties derived from privacy issues but also establish a stable, advantageous system to provide sufficient protection for the longevity of the enterprise.

References

[1] *Sheehan, K. B., & Hoy, M. G. (2000, April). Dimensions of privacy concern among online consumers. Journal of public policy & marketing, 19(1), 62-73.*

[2] *Gilmanov, A. (2023, August 26). What Are Third-Party Cookies and How They Work in Advertising.*

[3] *Hormozi, A. M. (2005, Jan/Feb). Cookies and privacy. Information Security Journal, 13(6), 51-59.*

[4] *Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2010, March). Flash cookies and privacy. In 2010 AAAI Spring Symposium Series.*

[5] *Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021, June 01). Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7(5), 2157-2177.*

[6] *Allen, S. J. (2018, April 11). How Facebook Tracks You, Even When You're Noton Facebook. Consumer Report. https://www.consumerreports.org/ electronics-computers/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook-a7977954071/*

[7] *Singer, N. (2018, April 11). What You Don't Know About How Facebook Uses Your Data. The New York Times. https://www.nytimes.com/2018/04/11/techno logy/facebook-privacy-hearings.html*

[8] *O'Flaherty, K. (2023, September 7). New Google Chrome Targeted Ad Tracking—Here's How To Stop It. Forbes. https://www.forbes.com/sites/kateo flahertyuk/2023/09/07/new-google-chrome-targeted-ad-tracking-heres-how-to-stop-it/?sh=36e2e77d29fa*

[9] *Israel, L. (2023, June 15). Enhancements to the Topics API. https://developer.chrome.com/en/blog/topics-enhancements/#:~:text=Topics%20utilizes%20several%20techniques%20to,compared%20to%20third%2Dparty%20cookies*

[10] *Woollacott, E. (2023, August 23). Children's Groups Call For FTC Probe Into Google's Ad Targeting. Forbes. https://www.forbes.com/sites/emmawoollacot t/2023/08/23/childrens-groups-call-for-ftc-probe-into-googles-ad-targeting/?sh=977b7bc4e34e*

[11] *Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018, Aug 15). We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. ar**v preprint ar**v:1808.05096.*

[12] *Jozani, M., Ayaburi, E., Ko, M., & Choo, K.R. (2020, June). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. ScienceDirect.*