ISSN 2706-6827 Vol. 7, Issue 6: 59-63, DOI: 10.25236/IJFS.2025.070610

An Analysis of Privacy Issues and Legal Improvement Strategies for Social Media Platforms: A Case Study of Facebook Advertising Targeting Teenagers

Ruihan Liu

Shaanxi Agricultural Development Group, Xi'an, Shaanxi, China, 710000

Abstract: *This paper examines the growing privacy concerns on social media platforms, with a specific focus on Facebook's targeted advertising towards teenagers. As internet technology advances, users increasingly share personal information online, often unaware of the risks associated with data surveillance and misuse. The study highlights how platforms like Facebook employ algorithms to monitor, collect, and analyze user data, particularly targeting vulnerable groups such as teenagers, thereby raising ethical and legal issues. The analysis draws on existing privacy laws, such as the Australian Privacy Principles (APPs), and critiques the limitations of self-regulation by platforms. It identifies three key areas for improvement: (1) enacting specific laws to protect teenagers' online privacy, (2) strengthening platform-internal codes to regulate data surveillance and third-party collaborations, and (3) enhancing government oversight of surveillance technologies to prevent data misuse. While policies and regulations can mitigate some risks, the paper concludes that complete privacy protection remains challenging due to the inherent trade-offs between connectivity and data security. The recommendations aim to expand the scope of privacy laws and codes, fostering a safer online environment for all users.*

Keywords: *privacy issue, data surveillance, algorithm, social media, online platform, Facebook, Law*

1. Introduction

As long as internet technology development booming, social media and online platforms are occupying the majority of people's everyday life and experiences. People are using social media to communicate with their friends and family and using online platforms to post information about themselves or interesting stories happening to them every day. Due to that common and normal behaviour, they are posting so much personal information wittingly or unwittingly online. Sometimes, personal information wide open to everyone on the internet may have some advantages. Users feel more convenient to reach others, such as to get familiar with others' personalities, hobbies, personal status before actually having an intersection with them in the real life.

Nevertheless, the shortcomings or harms are more serious and eye-catching for sharing information online recently. The most significant disadvantage is that posting personal information online will cause a serious data privacy issue. Personal information is easy to be leaked and monitored, and also some criminal incidents will occur such as hackers having chances to sell the personal information to exchange for money. Thus, the privacy issue and data surveillance online caused by the leak of efficiency control is becoming the major problem that should be concerned.

2. Privacy issue and data surveillance

Privacy is referring as a dignitary interest. What Rolph says in his article from a law perspective, "It is a human right recognized under a wide range of international, national and local instruments." (Rolph, 2012, p.1)[1]. This means it is a basic human right for each one and is determined by local, national, and international domains. However, from Nissenbaum's perspective, privacy is hard to define. Privacy is able to be defined as contextual integrity term, "is preserved when information flows generated by an action or practice conform to legitimate contextual informational norms." She believes privacy is the appropriate flow of personal information which should be depended on five parameters: subject, sender, recipient, information type and transmission principle (Nissenbaum, 2019, p.224)[2]. The essential factor

ISSN 2706-6827 Vol. 7, Issue 6: 59-63, DOI: 10.25236/IJFS.2025.070610

for privacy to be maintained with an appropriate flow of information between these five parameters, and it will be damaged if one of the factors is inappropriate. Thus, privacy is vulnerable and needs to be guarded by each party involved in the information flow process carefully, such as users, platforms and government.

However, the privacy issue online is not been seriously considered by normal users during their everyday online platform experiences. "Applied to privacy, this explanation of the WTA-WTP gap would predict that someone who enjoyed a particular level of privacy but was asked to pay to increase it would be deterred from doing so by the prospect of the loss of money," (Acquisti et al, 2013, p. 255)[3]. As Alessandro indicates, users are more willing to enjoy the free privacy service rather than pay for increasing the level of privacy. Money seems more important than their personal information which causes the online privacy issue is not to be considered and been more accessible for hackers to embezzle or steal.

Furthermore, the privacy issue is becoming more serious and worth being concerned is because people are not aware that their information is been misused or dug online. As same as what Cooper and Whittle claim in their article, "the fact that people are giving away private information about themselves both wittingly and unwittingly, without realizing how it might be used." (Cooper & Whittle, 2009, p.33)[4]. The leak of awareness about their private information is been harmed caused people are not to pay more attention to protect their information online. Moreover, people do not realize their information is been leaked online because the value is hiding under the shares or the original context. "Privacy is violated because the information that was shared in one context is combined with other information in a way that was removed from the original context and can potentially harm the individual" (Ling et al, 2020, p.6)[5]. Ling and his co-editors emphasize the personal information or valuable data are undercover or combined with the original context which will be neglected by people, and it will cause harm to individual's privacy online.

Therefore, this essay aims to uncover how online platforms threaten privacy, analyze how a giant online platform is monitoring personal data and dig deeper meanings of the basic information by introducing the Facebook advertising case study. Finally, this article proposes three ideas for improving and expanding the scope of privacy laws and regulations.

3. Law and regulation

Online privacy issues often occur in leakage the personal information and data. Australian Privacy Principles is also called APPs which is replaced by the National Privacy Principles and Information Privacy Principles on 12 March 2014 (Office of the Australian Information Commissioner, 2021)[6]. In the part one to part three of the principles, it mentioning about personal information privacy, and collection and dealing with personal information. The APPs is regulating how an entity collects or holds personal information and the purpose of holding the information. However, the privacy principle for an online platform is not completed, there are limited principles are connected to the online platform regulation.

To discuss in detail, "If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose)" (Office of the Australian Information Commissioner, 2021). As the privacy principles show above, the personal information is collected for a specific reason, such as fulfilling the person's profile on the platform, will not allow being used for another purpose, such as be dug the deeper meanings of a user through their footsteps online by combining the personal information and other data collected by platforms. Thus, privacy risks frequently occur in this stage of processing personal information by online platforms which is announced by the privacy principal law.

In addition, online information or privacy regulation are divided into two aspects which are internal control and external control. The external regulation is focusing more on local, national and international law. The law essentially protects information that is obviously private such as personal information. As Gorwa says in his article, "The practices of platform companies are subject to local laws, can be scrutinized by regulators, privacy authorities, competition authorities, and other institutional actors at the domestic or international level." (Gorwa, 2019, p.861)[7]. He believes the platform companies are obeying the local laws, privacy authorities, and are sometimes monitored by their competitors which is also an efficient way to maintain their legal behaviour.

ISSN 2706-6827 Vol. 7, Issue 6: 59-63, DOI: 10.25236/IJFS.2025.070610

Nevertheless, the major part of privacy regulation of online platforms is their own regulatory terms of service and codes. Each online platform has its own code of terms or regulatory rules to monitor the behaviour through the platforms. According to Gorwa, "code is law; design decisions made by creators of online services effectively amount to a form of regulation" (Gorwa, 2019, p. 858). The code or terms of service produced by platforms themselves function as a kind of law. They should regulate their own operations and govern others according to their own principles when making decisions and carrying out their activities. Moreover, platforms govern themselves by their own design, algorithm and architecture which are based on fulfilling their interests and profits. People will realize that relying on the self-regulation of online platforms is not realistic and will lead to some serious problems. Thus, the external govern by the laws and internal govern by platforms themselves simultaneously is the most efficient way to ensure the privacy is been protected online.

4. Case study

Facebook's CEO Mark Zuckerberg is announcing that Facebook is rebranded as Meta at the end of 2021. Meta symbols like never ends and Facebook is hoping to have a fresh start and unlimited success. However, researchers found that it keeps continuing its privacy issue without any changes. Facebook is been accusing of making teenagers become the target of their advertising determination. As Lomas posted in her journal, "In the latest problem for Facebook/Meta, the adtech giant has been accused of not actually abandoning ad targeting for teens but, per the research, it has retained its algorithms' abilities to track and target kids" (Lomas, 2021)[8]. Facebook is not stopping retaining its algorithms to target users under 18s which is causing the serious privacy issue on the monitoring and surveillance of teenagers' information and data on the platform. For instance, teenagers' data is collected by Facebook and be used by its AI abilities to track information from the footsteps of teenagers online to analyze the deeper meanings and to determine which ads to provide to them.

According to Lomas, "So Facebook/Meta stands accused of failing to make a meaningful change to protect some of its most vulnerable users from hyper manipulative marketing." Facebook is failing to protect the most fragile users which are teenagers. This accusation shows Facebook is not only facing a privacy issue but also leading an immoral and unethical behaviour as well. Nevertheless, Facebook claims that it will no longer accept advertisers to pick their target, but it is continuing to target the teens by itself as consequence (Lomas, 2021). By either way that Facebook is acquiescence, the damage to teenagers' privacy is occurring whatever by offering the opportunities for advertisers to make target or running through its own AI or algorithm ability to target the teens. Thus, online platforms like Facebook, it has two possibilities to harm the privacy of users online which are surveillance and analysis of the users' data by going through its own algorithm technology or trade information to third parties such as advertisers.

The major online platform privacy issue is caused by data surveillance. As Ling points out, "surveillance is based on the logic of competition and relies on gathering, storing, processing, diffusing, assessing and using data about humans." (Ling et al, 2020, p.3) Online platforms are gathering, storing and processing personal basic information online through algorithm technology which is formed as data surveillance. The Internet makes information easier to get and analyze by giant online platforms such as Facebook which give rise to privacy damages.

In addition, she also claims that "An advertising-centered data-mining corporation like Facebook hoovers up that metadata to understand whom you converse with and for how long." (Ling et al, 2020, p.4) Facebook is using its software or hardware such as algorithms to connect the basic information of users to create a deep understanding of them, and helping the platform itself to do a decision making about which content such as advertisement is suitable for users to watch and even purchase the products. This is running through a surveillance process by collecting the lower-level data of users and combining it with a piece of more valuable information for use afterwards. As Nissenbaum mentioned, the combinations of primary data are able to help develop and discover the deeper and unknown meaning of a subject (Nissenbaum, 2019, p.236). Facebook is obeying this rule to monitor and collect information, and deliver personalized information for each participant. This is a threat to the privacy that should be protected by the online platform.

Sharing data with third parties like advertisement companies is also a possibility to create a privacy issue for an online platform like Facebook. According to Dwyer mentioned in his book, internet governance is shaped in a commercial perspective which is not only modifying for the major new media company: Facebook, Google, Yahoo, and so on, and also some small to medium-sized companies which require the database about people's personal information for capitalism (Dwyer, 2015, p.120)[9]. This

ISSN 2706-6827 Vol. 7, Issue 6: 59-63, DOI: 10.25236/IJFS.2025.070610

means the data surveillance and leakage is occurring during the cooperation between major new media companies and other companies such as advertising companies based on commercial usage. Therefore, an online platform like Facebook is containing privacy issues through data surveillance, data mining and its algorithm technology, such as Facebook identifying the teens by their basic information and delivering personalized content for them by monitoring and calculating their footsteps online.

5. Expanding the extent of privacy laws and codes

For completing the laws or codes to protect privacy online or through online platforms, there are three aspects that should be concerned and paid more attention to. These three aspects are able to help both external and internal regulation efficiently work and to fulfill the empty spots for online privacy guarding principles.

The first aspect which the Australian privacy principle could fulfill is to establish laws or principles to protect online information privacy for teens specifically. According to the Teenage Research Unlimited (2004), in the United States, the teenagers aged 12 to 19 increase to 35 million in 2010, and every one of them spent $175 billion or an average of $103 per week in 2003 (Youn, 2005, p.86)[10]. Internet is becoming an essential part of teens' everyday lives and they are potential customers for online companies and actual stores gradually. Hence, they are becoming the target of the advertisement companies and a direct market in the online public sphere. Coming along with the entertainment that the internet could bring to them, privacy damages are also occurring more frequently in this particular group.

As the research shows, teenagers concerned about their information online is been used by unwanted advertisements and spam, and 63% of teenagers are also worried about online data collection practices (Youn, 2005, p.90-91). This emphasizes that teenagers are worrying about their online privacy and their consideration is including a variety of aspects. Thus, teenagers' online information protection is crucial and vital because teenagers are a vulnerable and valuable group and have been targeted by online platforms and advertising companies easily. Furthermore, government and platforms are able to work together to ensure the protection regulation or laws have a specific genre or category for teenager privacy protection and put more attention on complete regulatory rules for avoiding teenager's personal information from being misused or leaked.

Secondly, the platforms should complete their codes of privacy information online to legally control their own AI or algorithm technology and rule the third-party activities by using or co-working with their platforms. As long as Facebook/Meta is announcing to protect the teenagers online and keep their personal information in a more secure way, the social platforms are gradually aware the online information of their users need to be protected and it is also their responsibility to guard the environment for them. With expanding the company size and gaining more profits from users, online companies should carry heavier responsibilities to protect their participants. As Ling mentioned, "The dominant internet digital communications platform companies, including Facebook, Google, Amazon, Baidu, Alibaba, and Tencent, have built their business models on the mass-scale accumulation of personal data based on the algorithmic power of their personalization interactions." (Ling et al, 2020, p.14) The giant online platforms contain a dramatic amount of personal information within their huge database and possess powerful algorithms, it is offering a test for their moral and legal sense of protecting users' privacy online.

Due to the majority percentage of regulation will depend on the platform itself, it should create a series of more comprehensive codes to regulate the personal information flow within their platform. Moreover, it should regulate platforms themselves to have more self-control for not monitoring and using personal data and not trading users' personal information to third parties as well.

Thirdly, the government should establish specific principles or laws to regulate the surveillance process online which could efficiently eradicate the personal data being monitoring, collecting and leaked in the first place in a dynamic online environment. As the information shows above, data surveillance is the initial step for data collection and algorithm by those online platforms. By monitoring the data that users entered into the system, the platforms are able to collect and combine the primary data to uncover a deep understanding of the users. This is the process that contains the privacy risks or issues inside. As the ALRC claims, more attention is being paid to the surveillance devices rather than the software or networks (Serious invasions of privacy, 2014, p.14)[11]. The law should be put on the surveillance technologies which contain devices, software and networks. Furthermore, with more laws are established to supervise data surveillance by an online platform, the privacy risks which is been created by monitoring users will decrease. This will assist other privacy law principles together to create a more

ISSN 2706-6827 Vol. 7, Issue 6: 59-63, DOI: 10.25236/IJFS.2025.070610

relatively safe online environment.

6. Conclusion

Therefore, these threes aspects of improvement may lead the extent of privacy regulation to become more complete. However, privacy online will not be fully protected. As Ling points out, "While policies, laws, and regulations can offer some controls and are a key part of the solution, as a society we also need to ask in relation to emerging products and services," (Ling et al, 2020, p.14) This means people are using policies, laws, and codes to protect the information, but in a society, people need to make connections to each other. Even though people are noticing the importance of protecting their privacy online, the privacy damage will not be totally eradicated. Personal information is used for trading services and products online, and making connections within society is essential. Thus, the privacy principles are limited to protecting personal information online and do not guarantee full protection for users, it has a large space to be completed afterwards. In conclusion, the privacy laws and codes are efficient to protect the personal information online with expanding their extent by establishing laws specifically protecting teenager's online privacy, creating laws to more cruelly regulate the data surveillance as the first stage to damage the privacy online, and asking online platforms to complete their codes on regulating themselves and third parties. These three suggestions are a beginning to help perfect the laws and codes for protecting people's privacy online.

References

[1] Rolph, D. (2012). The interaction of remedies for defamation and privacy. Precedent (Sydney, N.S.W.), (108), 14–17.
[2] Nissenbaum, H. (2019). Contextual integrity up and down the data food chain. Theoretical Inquiries in Law, 20(1), 221–256. https://doi.org/10.1515/til-2019-0008
[3] Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? The Journal of Legal Studies, 42(2), 249–274. https://doi.org/10.1086/671754
[4] Cooper, S., & Whittle, S. (2009). Privacy, probity and public interest. Reuters Institute for the Study of Journalism, University of Oxford.
[5] Ling, R., Fortunati, L., Goggin, G., Lim, S. S., & Li, Y. (2020). Privacy from your mobile devices? Algorithmic accountability, surveillance capitalism, and the accumulation of personal data. In R. Ling, L. Fortunati, G. Goggin, S. S. Lim, & Y. Li (Eds.), The Oxford handbook of mobile communication and society. Oxford University Press.
[6] Office of the Australian Information Commissioner. (2021). Australian privacy principles. Retrieved November 17, 2021, from https://www.oaic.gov.au/privacy/australian-privacy-principles/
[7] Gorwa, R. (2019). What is platform governance? Information, Communication & Society, 22(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914
[8] Lomas, N. (2021, November 16). Facebook continuing to surveil teens for ads, says report. TechCrunch. https://techcrunch.com/2021/11/16/facebook-accused-of-still-targeting-teens-with-ads/
[9] Dwyer, T. (2015). Data governance. In T. Dwyer, Convergent media and privacy. Palgrave Macmillan.
[10] Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. Journal of Broadcasting & Electronic Media, 49(1), 86–110. https://doi.org/10.1207/s15506878jobem4901_6
[11] Australian Law Reform Commission. (2014). Serious invasions of privacy in the digital era: Summary report. https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/