The International Conference on Interdisciplinary Humanities and Communication Studies
DOI: 10.54254/2753-7048/5/20220424

"Taking Down the Monitoring": Privacy Protection for Social Media User in the Era of Big Data

Jiaqi Jin[1,a,*]

[1]*School of Journalism, Media and Culture, Cardiff University, CF10 3AT, The United Kingdom*
a. jiaqijin777@gmail.com
**corresponding author*

Abstract: In the era of big data, the development of technology has promoted social progress and given rise to various types of social media. The popularity of social media has made it an essential platform for information sharing and communication. However, the monitoring, collecting, and using of personal information on social media platforms have exposed users' privacy to risks. While technology has greatly facilitated people's lives, it has also brought about many ethical challenges to privacy. A balance is needed between the development of information technology and the protection of personal privacy. Through in-depth interviews with nine social media users, this paper discusses three situations where user privacy is compromised: user profiling, precision marketing and fraud. It also gives some strategies for protecting privacy based on the need for three different subjects to work together: individuals, platforms and governments.

Keywords: Big Data, Social Media Users, Privacy Leakage, Privacy Protection

1. Introduction

With the gradual arrival and rapid development of the big data era, social media has become a crucial platform for information sharing and communication on the Internet. According to statistics, there will be more than 983.3 million social media users in China by 2022, which means that 68% of the population uses social media. The average time spent online in China is 5 hours and 15 minutes per day, of which social media accounts for 1 hour and 57 minutes [1]. The connection between social media and users has become extremely close. However, while users share information and communicate about their lives on the platforms, they are also at risk of privacy leakage. In 2018, the New York Times revealed that a data company called Cambridge Analytica had leaked the data of over 50 million Facebook users. By targeting audiences with different political biases, it accurately pushed campaign messages about the U.S. election to influence its result [2].

Big data has driven social progress and promoted the development of the times. However, while it brings convenience, it also exposes many challenges. According to the China Internet Network Information Centre (CNNIC), in 2021, the proportion of Internet users who experienced personal information leakage and Internet fraud will be 22.1% and 16.6%, respectively [3]. Although with the implementation of the Personal Information Protection Law and other related laws, personal information security has been ensured to a certain extent. However, the increasing popularity of social media still exposes users' privacy to risks, and their personal information and privacy are threatened.

DOI: 10.54254/2753-7048/5/20220424

In the face of increasingly rapid technological and product iterations, it is essential to find a balance between the development of information technology and the protection of personal information.

Therefore, based on previous research, this paper will discuss three types of situations that face the threat of privacy leakage during social media usage from the perspective of social media users, and propose some strategies for privacy security protection from users, platforms, and the government.

2. Literature Review

2.1. Privacy

There is no agreed definition of privacy in academia Tavani defines four types of privacy: physical privacy, decisional privacy, psychological privacy, and informational privacy [4]. Information privacy is the right to control the access of others to private information. In this article, the discussion of privacy will focus on this aspect. Samuel D. Warren and Louis Brandeis asserted the "right to be let alone" and its use as a definition of privacy [5]. From personal space to personal information. Privacy has also been interpreted as restricting access to others, "either physical access, personal information, or attention" [6]. In addition, privacy can also be the ability and right of individuals to control their information and to decide when, in what way, to whom, and to what extent it will be disclosed [7][8].

At a legal level, the definition of personal information has similarities in international legislation, with all information relating to the identity and behaviour of individuals being included within the scope of personal information. The European General Data Protection Regulation (GDPR) defines personal information as including any information that directly or indirectly identifies or identifies a data subject [9]. Similarly, the California Consumer Privacy Act (CCPA) also considers direct or indirect identification, including consumer and household, biological and informational information [10]. The Civil Code of the People's Republic of China includes the protection of human dignity, the private sphere and personal information processing activities within the scope of the right to privacy and personal information [11].

2.2. Big Data and Privacy

Big Data is currently used to describe data sets that are larger than mainstream software tools and have the ability to capture, manage and process and organise data in a reasonable amount of time [12]. Big Data depicts the context of an era of data explosion, where more data is becoming more accessible with modern technology [13]. Despite his generally positive attitude towards big data, privacy concerns remain. In May 2014, a white paper released by the US White House discussed how to balance the utility of big data technologies with human concerns about privacy and other value norms [14]. Richard Spinello also suggested in his book that the era of big data has not been fully resolved, but has exacerbated the information ethics issues of privacy, intellectual property and information security that emerged at the end of the last century [15]. Similarly, O'Hara and Shadbolt revealed the threats to personal privacy posed by big data technologies in the current environment and explored the dialectical relationship between profit and personal privacy. They argued that people may have entered a surveillance mode where people's activities on the Internet result in personal information being stored, tracked and used in ways that challenge privacy [16].

2.3. Social Media and Privacy

Social media provides a way to create and share information, ideas, interests and other forms of expression [17]. Platform engagement serves as a data trace as well as a source of value creation and monetization [18]. At the same time, the panoramic digital prison has become a reality, and the

DOI: 10.54254/2753-7048/5/20220424

commodification of privacy has made it more common for users' privacy to be violated [19]. The problem of privacy leakage on social media requires the efforts of many parties.

Legal regulation is one response to privacy concerns. Wang pointed out that the right to privacy should be protected by the constitution and civil law [20]. According to Lin and Cai, privacy in the era of big data includes information and data with property value, which needs to be guarded by law in terms of both the protection of personal interests and the commercial value of personal information [21]. Lu and Xiong stated that protecting privacy requires both laws and ethics [22]. Consistently, Meng examined Facebook's industry regulation and platform self-regulation in response to user privacy protection issues and suggested that Chinese social media platforms could learn from this industry self-regulation [23]. However, Wang et al. pointed out that industry self-regulation is insufficient to protect user privacy and that social media platforms must also be held responsible [24].

In response, scholars have examined the informed consent terms on platforms. By comparing the content of social media informed consent terms with user expectations, Custers et al. found that not all privacy policy standards are important to users [25]. Wang argued that although informed consent is used as a general guideline, the moment a user signs a consent code to use a platform, he or she is providing implicit consent to data collection [26]. In comparing privacy policies in Western social media, Kim discovered that increasing the vividness of the presentation of privacy policies could enhance users' understanding of and willingness to read privacy policies [27]. Tang and Lai also compared the privacy policy texts of Facebook and WeChat. They proposed suggestions for improving the social media privacy policies in four aspects: content, perspective, format and regulation [28].

Research on big data technologies and privacy issues has covered a wide range of fields including ethics, law, science and technology. However, previous studies have mainly discussed privacy issues from a theoretical perspective on a macro level. This paper addresses the advent of the big data era by examining the latest perceived personal privacy and information security issues from the user's perspective, to find a balance between big data technology and privacy and information protection. It also attempts to comprehensively analyse the path of social media privacy protection from three different subjects.

3. Methodology

In order to obtain insight into users' perceptions of privacy and security on social media, this paper used semi-structured interviews as part of a qualitative study. Considering the different types of social media platforms, a random sample of nine social media users were interviewed, covering several important social media platforms, including Weibo, WeChat, QQ, Douyin, Bilibili, Zhihu and Xiaohongshu. The outline was designed before the interview, and the interview was conducted according to the outline set in advance. Based on the interviewee's response to a particular question, the writer followed up and explored the valuable information in time to obtain more in-depth information for the interview. The questions in the interview outline included, basic information about the respondents, attitudes towards privacy protection, issues related to social media privacy, and perceptions of current issues and policies. Each interview lasted approximately 1 to 1.5 hours and was conducted by telephone or WeChat message. The interview data was collected mainly through audio recordings, supplemented by notes taken during the interviews. After the interviews were completed, the author converted the audio recordings into transcripts. This paper uses numbers rather than respondents' names in the interview information and research analysis based on anonymity and confidentiality, by establishing a respondent numbering system. **Table 1** reflects the basic information of the respondents.

DOI: 10.54254/2753-7048/5/20220424

Table 1: Information of respondents.

No.	Gender	Commonly used social media	Average social media usage time
1	F	WeChat, QQ, Weibo, Xiaohongshu, Bilibili	6h/d
2	M	WeChat, Douyin, Bilibili, Zhihu	4h/d
3	F	WeChat, Weibo, Douyin, Xiaohongshu, Bilibili	5.5h/d
4	F	WeChat, QQ, Weibo, Douyin, Xiaohongshu, Bilibili	7h/d
5	M	WeChat, Douyin, Bilibili	3.5h/d
6	F	WeChat, Weibo, Douyin, Bilibili, Xiaohongshu	6h/d
7	F	WeChat, Weibo, Bilibili, Xiaohongshu	4.5h/d
8	M	WeChat, QQ, Douyin, Bilibili	4h/d
9	F	WeChat, QQ	2.5h/d

4. Results

Table 2: Respondents' perceptions of privacy.

No.	Personal information concerns	Privacy concerns	Privacy protection behavior
1	Yes	Yes	Yes
2	Yes	No	No
3	Yes	Yes	Yes
4	Yes	Yes	Yes
5	Yes	Yes	Yes
6	Yes	Yes	No
7	Yes	Yes	Yes
8	Yes	Yes	No
9	Yes	No	No

According to the results of the interviews regarding users' perceptions of privacy (see **Table 2**), social media users value personal information and already have a degree of privacy concern. Most of them are more concerned about privacy and security on social media (7), while a few respondents are not yet aware of privacy protection (2). It was also noticeable that despite social media users being concerned about their privacy issues, some did not take measures to deal with them. Therefore, based on the issues mentioned in the interviews, we will focus in this section on the issues related to users' perceived privacy and security on social media and their suggestions for solutions to these issues.

Privacy invasion and algorithm abuse were widely cited by interviewees, who expressed a feeling of being monitored when using social media. With big data technology, everyone has become transparent, and it seems they have lost their privacy.

DOI: 10.54254/2753-7048/5/20220424

4.1. User Profile and Digital Identity

Empowered by big data technologies and algorithms, social software can track, monitor, collect and even use user data, including user identity attributes such as age, gender, and the geographical location where they are located. Moreover, this fragmented information can potentially be pieced together on the web to create a complete picture of the user. According to one Weibo user (Respondent 1): "This user profile is valid. It is possible to determine the name, gender, approximate age, and city of residence through posted content. Even home address, study or workplace are all possible if the user does not consider privacy. This integration of this fragmented information into a personal information network is terrifying".

4.2. Algorithm Pushing and Precise Marketing

In addition to the user's personal identifying information when registering for access, the user's search, browsing content, time spent, interests and preferences and even chatting content are also captured in real-time by the background. Based on this information collection, the algorithms are no longer simply monitoring but can also analyse and predict themselves. They predict user preferences based on their models and attributes to push specific messages and advertisements that match their preferences for personalised pushing and precision marketing. Respondent 3 indicated, "My conversations with friends on WeChat can be scanned that they are pushed relevant content when jumping to other platforms." However, respondent 6 argued, "This push function is more of a commercial marketing tool for the specific social platform, which is caused by the type of platform and not all social software does this." It is also important to note that this type of user-based behavioural prediction can increase attention and appeal based on user preferences to enhance user stickiness. As a result, users become dependent on the social platform and unconsciously increase their usage time (Respondent 4).

4.3. Fraud and Spam

The user information that users fill in when registering on social media platforms is also at risk of being compromised, and an easy outcome is fraud. Fraud is a more direct manifestation of information leakage, including account theft, impersonating users to commit fraud, such as QQ account theft (1, 8, 9) or Weibo user impersonation (7). Or, more directly, phone or SMS fraud through phone leaks (2, 4). Additionally, the transparency of phone numbers can also lead to harassing messages or spamming platforms, a problem that almost all respondents have faced.

5. Discussions

The high incidence of privacy information infringement in recent years has also led to a further increase in awareness of privacy information protection. It is vital for each entity to update the concept of privacy protection for social media users and to take effective measures to protect the privacy information rights of users. Based on the results of the interviews, this paper summarises some suggestions and strategies from three parties: individuals, social media platforms, and the government.

5.1. Users: Privacy Protection

Social media users need to improve their privacy protection and information security literacy [29][30]. Many social networking platforms now tend to over-solicit user information permissions. Users should pay attention to permission reminders and set permissions cautiously; read the platform's privacy protection policy carefully and pay attention to third parties in the privacy policy for personal information sharing. At the same time, they should set strong passwords and not apply the same

DOI: 10.54254/2753-7048/5/20220424

username and password to log in to different social media platforms. Moreover, avoid clicking on random web links from unknown sources on an account.

5.2. Platforms: Social Responsibility

As the responsible subject, social media platform operators should, on top of strictly fulfilling their responsibilities and obligations under laws and regulations, take up social responsibility and establish data security and privacy protection mechanisms within the platform [31]. Scientific and legal privacy protection policies should be formulated to limit the scope of information collection. Information should be collected with the informed consent and the agreement of users to respect and protect their rights [32]. In the meantime, complaint mechanisms and channels should be improved. Furthermore, platforms must strengthen security and privacy encryption technologies and provide more comprehensive and detailed privacy protection measures for users [33].

5.3. Government: Regulation by Law

The government needs to improve laws, regulations, and rules on the protection of social media users' privacy, to regulate and guide social media to formulate and comply with user privacy policies; at the same time, vigorously crack down on the sale and processing of users' private information by criminals [31]. GDPR is an important document on the protection of data and personal information in the EU, which attaches great importance to the protection of users' informed consent and provides for the collection and processing of data. Drawing reasonably on the legislative experience of the GDPR, China has responded positively to the issue of information privacy protection in the era of big data in the Civil Code, from the definition of privacy and personal information, principles of protection, legal liability, and information processing [9][11][30].

Along with the refinement at the legal level, the national authorities should accelerate the improvement of the regulatory system for social media privacy policies. Policies include clarifying the legal responsibilities of data users and further refining standards related to data security and personal information protection; establishing long-term supervision of user privacy protection and data security testing mechanisms; and using credit supervision mechanisms to focus on monitoring social media platforms with poor credit records [29][34][35]. Furthermore, the penalties for privacy violations by offenders should be increased. Given the inadequacies of the current policy, there is a need to continue to improve the regulation of liability for illegal data leakage from platforms and the secondary use of data in the integration and mining of data [36].

6. Conclusion

To sum up, this paper has examined the privacy issues of social media users in the context of the development of big data technology. Compared to previous studies on privacy, this paper focuses on the privacy issues of individual social media users. Interviews reveal three types of problems related to privacy invasion and algorithmic abuse encountered by social media users. Miscreants can piece together a complete user profile and target digital identities through information on identity attribute that users fill in or disclose on social platforms, posing a security risk to individuals. Social media collect and utilise behavioural information and identity attributes, acting to personalised push and precise marketing for subsequent commerce. In addition, personal privacy left on the platform by users can be trafficked, stolen, and used by unscrupulous individuals to commit fraud.

Therefore, this paper discusses some strategies to address these three issues from the perspective of users, social platforms, and the government. Users need to raise their awareness of personal information and privacy protection, pay attention to their information disclosure, and not ignore the privacy policies and related permissions of social media. Social media platforms should take

DOI: 10.54254/2753-7048/5/20220424

responsibility for formulating and enforcing privacy protection policies and respecting and protecting users' right to know. The government should improve relevant laws, regulations and rules at the legal level. While guiding the platforms to regulate them, it should increase its efforts to crack down on privacy trafficking and theft miscreants.

However, this study also has some limitations. The interviews used a random sample to select social media users, which may not be fully representative of all user groups. In addition, this paper focuses the research on privacy and personal information issues and lacks some discussion on social ethics, which could be a direction for subsequent research.

References

[1] *The Global Statistics. (2022) "China Social Media Statistics 2022: Most Popular Platforms." www.theglobalstatistics.com/china-social-media statistics/#:~:text=The%20number%20of%20social%20media,up%2036%20million%20from%202021.*

[2] *Rosenberg, M., Confessore, N. and Cadwalladr, C. (2018) "How Trump Consultants Exploited the Facebook Data of Millions." The New York Times, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html*

[3] *China Internet Network Information Center. (2022) The 49th Statistical Report on China's Internet Development. www.cnnic.com.cn/IDR/ReportDownloads/202204/P020220424336135612575.pdf.*

[4] *Tavani, H.T. (2012) Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing. Wiley Publishing, pp. 144-152.*

[5] *Warren, S.D., and Brandeis, L.D. (1890) The Right to Privacy. Harvard Law Review, 4(5), pp. 193–220. doi:10.2307/1321160*

[6] *Sissela, B. (1989) Secrets: on the ethics of concealment and revelation. New York: Vintage Books.*

[7] *Fried, C. (1968) "Privacy." Yale Law Journal,77:477-478.*

[8] *Westin, A.F. (1970) Privacy and Freedom. Michigan Law Review, 66(66):123-142.*

[9] *General Data Protection Regulation. (2018) https://gdpr-info.eu/.*

[10] *California Consumer Privacy Act. (2018) https://oag.ca.gov/privacy/ccpa.*

[11] *The Civil Code of the People's Republic of China. (2021) http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf.*

[12] *Snijders, C., Matzat, U., and Reips, U.D. (2012) "'Big Data': Big gaps of knowledge in the field of Internet." International Journal of Internet Science, 7: 1–5.*

[13] *Cukier, K. (2010) "Data, Data Everywhere: A Special Report on Managing Information" The Economist, February 25pp. 3-5.*

[14] *The White House. (2014) Big Data: Seizing Opportunities, Preserving Values. https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.*

[15] *Spinello, R.A. (1994) Ethical Aspects of Information Technology. Pearson.*

[16] *O'Hara, K. and Shadbolt, N. (2018) The Spy In The Coffee Machine: The End of Privacy as We Know it. Oneworld Publications.*

[17] *Mayfield, A. (2007). What is Social Media? Icrossing e-book. Publish, Spaimerworks.*

[18] *Alaimo, C. and Kallinikos, J. (2017) Computing the everyday: Social media as data platforms, The Information Society, 33(4), 175-191. doi: 10.1080/01972243.2017.1318327*

[19] *Li, W. and Hang, M. (2019) Privacy Dilemma in Social Media: Privacy Boundaries and Big Data Concerns. Editorial Friend, 2019(01):55-60. doi: 10.13786/j.cnki.cn14-1066/g2.2019.1.009*

[20] *Lin, A. and Cai, M. (2020) Privacy flows and personal information protection in big data. Modern communication. 2020(4): 79-83.*

[21] *Wang, X. (2017) Study on the Public Law Protection of Individual Privacy in the Information Society. Beijing: Press of Chinese Democratic Legal System.*

[22] *Lv, Y. and Xiong, J. (2012) Ethical defence of the protection of privacy in China. Jiangxi Social Sciences, 32(03):157-162.*

[23] *Meng, R. (2017) Research on the Self-regulation and Supervision Mechanism of Users' Privacy Protection at Social Media Platform in the United States. Editorial Friend, 2017(01):104-112. doi: 10.13786/j.cnki.cn14-1066/g2.2017.01.020*

[24] *Wang, S. and Zhu, N. (2013) A Study of Mobile Social Media Users' Privacy Protection Measures, 36(7): 36-40. doi: 10.16353/j.cnki.1000-7490.2013.07.003*

[25] *Custers, B. and van der Hof, S. and Schermer, B. (2014) Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy & Internet, 6(3): 268-295.*
[26] *Wang, L. (2018) The Rational Use of "Date Privacy" in Big Data Era: Informed Consent, Uninformed Consent and Participative Consent. Editorial Friend. 2018(10): 36-39. doi: 10.13786/j.cnki.cn14-1066/g2.2018.10.007*
[27] *Ko, Y., Choi, J., and Kim, B. (2014) The Impact of Privacy Policy Layout on Users' Information Recognition. International Journal of Radiation Biology & Related Studies in Physics Chemistry & Medicine, 2014, 24(1):343-350.*
[28] *Tang, Y. and Lan, X. (2018) Social Media Privacy Policy Text Study - A Comparative Analysis Based on Facebook and WeChat. News and Writing, 2018(8): 31-38.*
[29] *Luo, L. (2020) Research on the Privacy Protection of Social Media Users in China through the Personal Information Leakage Affair of Facebook Users. Computer & Telecommunication, 23-26.*
[30] *Zou, X. (2018) A Study of the Use of Social Media and Privacy Protection of Social Media Users. MA Dissertation, Shandong Normal University.*
[31] *Li, M. (2012) On the Protection of Personal Privacy in the Era of Big Data. Today's Mass Media. 2021(3): 41-43.*
[32] *Xi, J. (2021) Security Strategies for Protecting Social Media Users' Private Information in the Age of Big Dat. THUSHUGUANCUEKAN. 2021(8): 85-89.*
[33] *Sun, W., Song, W., Gong, F., and Gong, Z. (2020) The Path to Protecting User Data and Information Privacy in the Big Data Era. Public Communication of Science & Technology 2020(12): 124-126. doi: 10.16607/j.cnki.1674-6708.2020.24.044*
[34] *Jia, J. (2018) The research of personal privacy information security in the era of big date. MPA Dissertation. Inner Mongolia University.*
[35] *Wang, H. (2021). Research on the privacy protection of social media users in the era of Big Date. MA Dissertation, Xiangtan University.*
[36] *Chen, C. and Wang, T. (2020) Research on Privacy Protection of Precise Advertising in Big Data Era. Academic Exploration, 2020(4): 105-112.*