Social Media Changed the Notion of Privacy

Wanyi Fang
School of Communication, University of Ottawa, Ottawa, Canada
delanceyfang@gmail.com

Abstract. This article analyzes the impact of social media on traditional and contemporary notions of privacy, and discusses how the evolution of the web from 1.0 to 3.0 has influenced privacy trends and applications. With the advent of Web 3.0, users are expected to have greater control and ownership over their digital assets and personal information. While this shift presents opportunities for increased data autonomy and value, it also raises concerns about potential privacy violations. The paper explores both positive and negative consequences of this changing privacy landscape, and highlights the need for privacy protection measures. Moreover, the authors suggest that privacy will continue to evolve in the future, with users potentially viewing privacy as a personal asset. The analysis draws on a range of scholarly sources to offer a nuanced and comprehensive perspective on this complex and rapidly evolving issue.

Keywords: Traditional privacy; Contemporary privacy; Safety; Change.

1. Introduction

Social media has been around for a long time, from the papyrus used by ancient Roman statesmen such as Cicero to exchange information, to the propaganda pamphlets printed during the Reformation, American Independence, and the French Revolution, to the advent of the Internet today (Standage 4). In modern society, online social media has become such an integral part of our lives that we cannot imagine what it would be like to communicate with people without it. Online social media allows us to send and receive information from many sources and is a way for us to receive many updates from the people we follow. Some people also see social media as part of a new marketing strategy.

On the other hand, privacy has known a long development throughout history; it is as old as mankind. What is considered to be private differs according to the era, the society, and the individual (Adrienn 256). Indeed, the notion of privacy is difficult to define, some philosophers have defined privacy as a function of accessibility to a person (Abril 1007). One might stress that the right to privacy is a personal right of a person to enjoy the peace of private life, and to have private information protected by law from unlawful interference, knowledge, collection, use and disclosure by others. However, as the communication channels of people continue to change, traditional notions of privacy are under attack, and rapidly evolving online communication technologies have changed how people understand privacy. In this article, I will first compare the traditional notion of privacy to the contemporary notion of privacy. Second, I will analyze why the notion of privacy has changed because of shifts in how the media collects information, which I will explain using news events in China. Next, I will explain how the change in the notion of privacy affects users, and I will use the Facebook breach as an example. Finally, I will offer some methods to protect modern privacy and make predictions about future notions of privacy.

2. Comparison between traditional privacy and contemporary privacy

According to the “The Stanford Encyclopedia of Philosophy”, early privacy treatises emerged in the 1890s as privacy protections in U.S. law developed, with privacy protections based in large part on ethical grounds. Traditionally, some viewed privacy as a notion with moral value, while others viewed it as a moral or legal right that should be protected by society or the law. Now, we protect our privacy for more reasons than ever, to keep ourselves safe from harm and to protect our own interests. Contemporary privacy differs from traditional privacy in terms of the way information is protected, the consequences of information leakage, and other events. Let us elaborate on this shift.

In the early twentieth century, people's private information could be better protected. As long as they did not disclose it to others, it would be difficult for anyone to learn about their private information. Furthermore, people used to focus more on personal information such as address, workplace, and phone number. In the era without the internet, people usually communicated by letters and verbal communication. Therefore, even if someone peeked at one's mail, not many people would know the content of that mail. Today, when social media software requires users to enter private information, users will undoubtedly give their address, phone number, email address, and other personal information to social media. In theory, private information will only be known to the social media platform, but there have been many user data breaches in recent years. Hence, it is not safe to give private information to the platform. Not only that, but because users are spreading their information on public platforms, anyone can see it. So once someone has malicious intent, he or she can learn a lot of information about users from the internet and spread it on other public platforms. Therefore, many people will see other users' private information, which may cause serious trouble in these users' lives. This is a result of the subject and object of privacy violation in the social media environment having changed. There has been a shift from the infringement of one's own rights by others in times of traditional privacy, "self-inflicted suffering" caused by one's own initiative to provide information, in a time of contemporary privacy (Li and An 39).

According to Chinese jurisprudence, the right to privacy on the Internet refers to the personal information and personal activities of citizens on the Internet, which are protected by law from illegal infringement, knowledge, collection, copying, disclosure, dissemination and use by others. The traditional right to privacy, as a specific personality right, refers to the right of a natural person to be protected from unlawful interference, knowledge, collection, use and disclosure of private life and private information (Wang 9). In my opinion, internet privacy is based on the traditional right to privacy and has been given new content in contemporary times, as internet privacy expands the content and form of traditional privacy rights.

3. The notion of privacy is continuously evolving

3.1 New changes in the way information are collected

The Internet model is constantly being iterated and upgraded as platforms and users are increasingly in demand. The change occurred from web 1.0 with only static web pages, to web 2.0 with direct user interaction, and now to web 3.0 with independent user control of data. In the web 1.0 era, people thought they were socializing anonymously online, so they thought their privacy could be well protected in the web 2.0 era, people found that their information was no longer in their hands, but in the hands of the platform. We are currently in the era of web 2.0, which is the second phase of the World Wide Web revolution from 2004 to the present. In this era, people can share their views, opinions, ideas, and experiences; it highlights user-generated content, usability, and interoperability. According to Hao Wu's research on personal privacy protection under social media, the implementation of social media as an emerging medium that changes the way people access and share information is based on the development of web 2.0 technology, which focuses more on user interaction (2). Therefore, media platforms at this stage need a lot of user information and even private information, so a variety of information data collection methods are created. Moreover, in the future, we will enter the era of web 3.0, in which content is created by users and data is owned by users. Web 3.0 will hopefully lead us one step closer to an efficient, fair, trustworthy and valuable Internet world.

It appears that the way in which information is collected today has become diverse in several ways, which is one of the reasons, and arguably the most important reason, why the notion of privacy is evolving. First, there is data tracking: the most common form of data collection on social media platforms. Social media platforms use user search history, listen to daily conversations, and follow other platforms' browsing history to suggest content users are interested in. These tracking behaviors are often carried out without the users' knowledge or consent, but there is no way to oppose them. Although some people use web tools such as untraceable web browsing and other protection software

to protect their privacy, they still cannot stop all of the privacy leakage. Consequently, most people have come to accept that it is reasonable and customary for platforms to have access to their private information. Although in the past, this was considered unethical under traditional notions of privacy, people who have embraced the notion of modern privacy consider it a commonplace thing. Second, the emergence of some third-party apps has changed the way people view privacy. According to a 2018 study by the International Computer Science Institute, eight of the top ten global advertising and tracking companies "reserve the right to sell or share data with other organizations" (2). This shows that user privacy is not only stolen by these media companies, but also stored and sold by them. A Chinese ride-hailing app called Didi Chuxing has repeatedly stolen user information and trafficked it to other countries. According to Tencent News, on July 21 this year, Didi was again fined 8.026 billion Yuan by the state for leaking riders' personal information. Didi violated the Network Security Law, the Data Security Law and the Personal Information Security Law, and the facts are clear and well-documented. When these incidents occurred, most people's first reaction was not that their privacy had been compromised but that it was an incident that jeopardized national interests. This also reflects that most people are subconsciously not surprised by the sale of private information on the platform.

3.2 The impact of the changing notion of privacy

The essence of Big Data is to obtain products and services with great value and gain deeper insights by analyzing the huge amount of user data. Simply put, all the data collected through various software over a long period of time, after filtering and processing, can provide information for platform decision making. Furthermore, while the era of web 2.0 has brought a lot of convenience to people's life and work, there are two sides to everything. In the long run, big data brings convenience to production and life, but it also makes people worry about whether or not there will be hidden dangers relating to information security and other risks.

On the one hand, let us discuss the advantages of a change in the notion of privacy. First, daily life will become convenient. For example, by binding one's bank card, identity information, cell phone number, and other private information to a third-party payment service platforms in mainland China such as Alipay, one can use Alipay to buy airline tickets, bus tickets, to pay utility bills, and to pay bills when shopping. All this spending can be done with just one software. Second, when uploading an address and other location information to Google Maps will facilitate travel. When going out, one may need to look at the Maps app to know what road congestion is like. This is related to big data, in that the Maps application needs to collect traffic data, then track and predict the road congestion, to offer better route. Without big data support, one will only find the road congested after leaving home, wasting a lot of time.

On the other hand, the changing notion of privacy has also had a negative impact. In the age of big data, users acquiesce to platforms stealing their private data. This is because 'surveillance capitalism' allows users to acquiesce to this behavior in order to gain access to more information themselves. For example, Facebook's business model represents this new form of capitalist accumulation known as surveillance capitalism. According to Professor Patrick Baert's lecture, "surveillance capitalism" claims private human experience as a resource, whereas nineteenth-century capitalism claimed nature resources. Private human experience is turned into a commodity, enabling hidden commercial practices of extraction, prediction, and sales. Under the slogan of advocacy and liberation, the surveillance capitalists have made great use of the anxiety of contemporary society, making it seem as if the masses can gain power from the Internet. And they keep claiming that this is an inevitable development—all factors that allow the surveillance capitalists to succeed in getting information. However, even if the non-compliant use of data by Internet service providers is still excusable to users, once the data is leaked or illegally traded, it will cause unpredictable consequences. Today's leaks are countless, and private information may flow into the wrong hands at any time. When user information is acquired by fraudsters, illegal organizations, and even unsuspecting people, it can lead to serious physical and mental harm. The New York Times reported that data on more than 50 million

Facebook users was leaked by a company called Cambridge Analytica and used to push targeted content to sway the U.S. presidential election in 2016 From its early "Newsfeed" to its "Beacon" social advertising system, and from its "location data visible to others" to its "secret tracking of users' logged-out pages" privacy settings, Facebook has continued to push back the boundaries of user privacy (Gou 221). This shows that although a platform such as Facebook is a sophisticated social platform, user private information still can easily fall into the hands of others and become a weapon.

4. Ways to protect modern privacy

As shown, any information users post online can be used maliciously. Therefore, there is a need to protect modern privacy. With current modern privacy, privacy protection mainly relies on national laws to bind platforms and individuals to reduce the risk of privacy leakage. I will provide a few methods individuals can use to reduce privacy violations. First, for example, trying to save data and information to a mobile hard disk and use fewer internet disks, in order to avoid information theft. One should not lend their mobile hard drive to store important data, and should not plug it into a public computer. Other methods include timely updates to antivirus and security softwires on computers and cell phones, and from time to time, eliminating the virus after using a computer and cell phone to erase any traces. Second, one should not disclose private information on platforms which do not have security certification. Except for the necessary registration information, one should not leave too much accurate personal information on the Internet. Third, many cafes, hotels, and public places offer free Wi-Fi, making one want to login wherever one travels. However, public Wi-Fi poses a significant security risk. If it does not include strong authentication, it is easy to log-in, but just as easy a target for hackers. Last, one should not use public Wi-Fi for banking transactions or other sensitive Internet applications. If one is worried about website tracking and monitored browsing history, one can try to use a traceless website.

All of these approaches to privacy protection point to a huge privacy problem that needs to be solved. Nowadays, we often see the impact on our lives as a result of privacy breaches. For example, personal data is sold to other countries, harassing and fraudulent phone calls become more frequent, and users' personal safety and property are threatened. And modern privacy is under greater threat than traditional privacy. If we want to have a normal life, we must take proactive and conscious measures.

5. The future of notion of the privacy

As mentioned previously, we are in the era of web 2.0 and are moving towards the era of web 3.0. In the web 3.0 era, the digital content created by the user should be owned by the user: the user should own the control and management of their information and data, and the value created by it is distributed according to the agreement signed between the user and other users. The notion of the metaverse, which has been popular recently, is an application based on the technology of web 3.0. In the metaverse, users participate in the interaction of the network world through avatars, and the collection of avatars is the user's identity, which the user owns. The mastery of the digital products held by the user is only in the hands of the user. Compared with the web 2.0 era's user identity, web 3.0 is very different in terms of identity control, openness, security, and privacy. For one, users have a more thorough way to protect their private information, and the transfer of data ownership and value will be more thoroughly protected. Moreover, users will enjoy genuine data autonomy. Personal information will become a data asset under the user's control. Users can truly benefit from the data flow and transactions so that their data is no longer a free resource of the Internet platform. According to "A decentralized social network architecture," different encryption mechanisms are used in decentralized networks to address data privacy issues. Blockchain, on the other hand, is able to digitally identify and track transactions and share this information across a distributed network of computers, thus creating a distributed network of trust (Sarathchandra, Tharuka, and Damith 252).

As a result, the notion of privacy will change again in the future, and I suspect that when web 3.0 comes, users will see privacy as a personal asset.

6. Conclusion

In general, there are some differences between the traditional notion of privacy and the modern notion of privacy. The main development is that the private information users used to care about is now unknowingly monitored by the platforms, and users can only accept the unethical behavior of these platforms because big data has made their lives more convenient. In addition, the feeling of users sharing on social platforms has changed. Web1.0 users shared their lives, but the platform on a large scale rarely or never leaked their information. Whereas nowadays, users in the web 2.0 period have become accustomed to privacy leaks. Furthermore, users are now focusing more on their content than whether or not their lives are private. The changing notion of privacy has brought convenience to life while exposing personal information to everyone. Even the most private information is sold as an asset by platforms to other platforms or organizations.

In today's world, if one wants to protect one's privacy, all one can do is try not to leak private information on the Internet. Nevertheless, in the coming web 3.0 era, I think the notion of the privacy will change again. Because web 3.0 will protect our private information, our data will be in our own hands, not in the hands of the platform.

References

[1] Abril, Patricia. Two Notions of Privacy Online. Jan. 2009, Vanderbilt Journal of Entertainment and Technology Law, vol. 11.
https://www.researchgate.net/profile/Patricia-Abril/publication/228226759_Two_Notions_of_Privacy_Online/links/53d7ad2a0cf2a19eee7fcbdb/Two-Notions-of-Privacy-Online.pdf.

[2] Adrienn, Lukács. [PDF] "What Is Privacy? The History and Definition of Privacy: Semantic Scholar." Undefined, 1 Jan. 1970. https://www.semanticscholar.org/paper/What-is-Privacy-The-History-and-Definition-of-Adrienn/430bfacbabb89c0033b6dceddc18ba9bbc02c5f.

[3] Baert, Patrick. "Media & Society Lecture 5—Social media, disclosure and privacy," 21 Aug. 2022, EastWest Education Group, Lecture.

[4] DeCew, Judith. "Privacy." Stanford Encyclopedia of Philosophy, Stanford University, 18 Jan. 2018.

[5] https://plato.stanford.edu/entries/privacy/#:~:text=Others%20suggest%20that%20privacy%20is,to%20be%20self%20expressive%20and.

[6] Gou, Hongjing. "Discussion on Citizen Privacy Leakage in Online Media Environment — A Case study of Facebook user data leakage." Communication Power Research 2.15 (2018): 221-222.

[7] Razaghpanah, Abbas, et al. Apps, Trackers, Privacy, and Regulators. 2018.
https://people.cs.umass.edu/~phillipa/papers/ndss18.pdf.

[8] Sarathchandra, Tharuka, and Damith Jayawikrama. "A Decentralized Social Network Architecture." 2021 International Research Conference on Smart Computing and Systems Engineering (SCSE), vol. 4, IEEE, 2021, pp. 251–57. https://doi.org/10.1109/SCSE53661.2021.9568334.

[9] Standage, Tom. Writing on the Wall: social media—the First 2,000 Years. First U.S. edition. Bloomsbury, 2013.

[10] Tian, Li and Jing, Jing. "Research on Social Media Users' Privacy Concerns." News & Writing. 01(2015): 37-40.

[11] Wang, Liming. "Redefinition of the notion of privacy." Jurist .01 (2012): 108-120, 178. doi:10.16094/j.cnki.1005-0221.2012.01.007.

[12] Wu, Hao. "Research on Personal Privacy Protection under Social Media." Master's Thesis of Chongqing University, Apr. 2015, https://cdmd.cnki.com.cn/Article/CDMD-10611-1015970642.htm#.