

---

# Is privacy still possible on social media?

---

## *Chinara Gasimova*

*The highest education title she possesses now is a bachelor's degree in law earned from Baku State University. She is a first-year student of master's degree studies at Lund University. Gasimova is planning to graduate by 2023 with a degree of LL.M in European Business Law. She is one of the Swedish Institute Scholarship for Global Professionals holders.*

### **Abstract**

Because the 21st century has become an age of technology, social media, digital devices, and cloud connectivity have become an integral part of our lives. Especially, in this pandemic era where everything is almost digitized and technology is so deeply surrounded in daily lives which makes to think about privacy. Today, a large amount of information some of which is personal is shared by Internet users on social media platforms such as Facebook, Instagram, Twitter, Telegram, LinkedIn, TikTok, Snapchat, and others. The more the Internet and social networks expand, the more information is being shared online by social media users, and consequently, it seems hard to control social media privacy.

The meaning and value of privacy have become the subject of considerable controversy. The power of

new technology, the Internet, and social media raises problems concerning the law, policy, and ethics on privacy. This essay will investigate the value of privacy and explore the relationship between social media and privacy. We will also analyze the possibility of protection of a person's data collected and stored on social media and identify ways to protect privacy on social media.

The right to privacy increased worldwide with the advent of information technology in the 1960s and 1970s[1]. As the value of privacy depends on society, culture, and context, it is a complex and broad term to define. The concept of privacy is articulated as the individual's "right to be left alone" and it has been defined as "the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate with others" [2]. As an interest and a valuable aspect of the human personality, privacy protects individual's self-determination, independence, dignity, and integrity. Privacy is an important element for a democratic society[3] as a social, public, and collective value.

All persons have a common interest in a right to privacy, so privacy is something we all ought to value. If we do not value our privacy, it may cause us to lose our privacy. Consequently, individuals and society must recognize the value of privacy and take measures to protect it. However, the massive stores of personal data collected and retained by social media make it almost impossible to control privacy. In addition, in some cases, it is difficult to strike a balance between freedom of expression and the right to information, which are among the instrumental values of a democratic political system, and the right to privacy.

Social media is a technology where personal information can be easily collected, processed, and disseminated.

---

[1] Piller C. "Privacy in peril". *Macworld* 10.7. (Jul.1993): 124-130.

[2] Thomas McIntyre Cooley. *Treatise of the Law of Torts*. 2nd ed. Callaghan, (1888): 29.

[3] Kirsty Hughes, *The social value of privacy, the value of privacy to society and human rights discourse*, Published online by Cambridge University Press: (05 July 2015), p 225.

---

The Internet has become a new meeting place for individuals as well as a business hub for corporates and merchandisers for selling and promoting their products and services. The rapid growth and development of social media platforms cause us to disregard the importance of privacy. With technological advancements, it is now possible to invade an individual's privacy without physically accessing his/her place or property. Researchers can obtain vast amounts of high-quality observational data about human interactions and behaviors via social media[4], which shows that such a platform has allowed eavesdroppers to intrude into our privacy. Data at risk can include our location, health information, sexual orientation, religious identification, facial recognition imaging, private messages, personal photos, and more, depending on the social media platforms. Such kind of personal data collected and stored by social media platforms is vulnerable to scraping, hacking, and data breaches, especially if platforms fail to institute crucial security measures and access limitations. Therefore, today, social media is not really the safest place to be and share personal information.

The question may arise that how does social media affect privacy? Data mining, Phishing Attempts, Malware Sharing, and Botnet Attacks are typically social media threats in which criminals are adept at tricking social media users into handing over sensitive information, stealing personal data, and gaining access to accounts that users consider private. Such threats to privacy on social media lead individuals to

suffer harassment and lose their peace of mind. Privacy concern on social media has grown in recent years.

Data breaches, in particular, have worried many social media users, make them reconsider their relationships with the social media platforms and the security of their data on social media. The tragic story of Cambridge Analytica, a consulting firm, is a case in point. This is exactly how Cambridge Analytica used Facebook data in an effort to influence voter behavior in the 2016 presidential election in the United States.[5] The scandal involved exploited Facebook data of 87 million people being used for advertising to influence during elections. [6] One of the recent incidents belongs to LinkedIn which more than 780,000 personal information such as full names, email addresses, phone numbers, and workplace information associated with the leak this year. [7] However, LinkedIn has denied reports of this data breach: "We want to be clear that this is not a data breach and no private LinkedIn member data was exposed".[8] While LinkedIn denies this leak, leastways, this situation makes individuals aware of dealing with their personal information and wake up data sharing in relation to social media privacy. This and other examples have steadily eroded public trust, leaving many people questioning if they have lost control over their personal data. According to a Pew Trust survey, 80 percent of social media users are concerned about corporations and advertising accessing and utilizing their posts on social media.[9] By understanding the value of privacy, the impact of social media on privacy, individuals need to do a lot to protect their data.

Although each individual is in charge of their social media privacy, in reality, it is hardly possible to control social media privacy in your own way. This is because

---

[4] Moreno Mancosu and Federico Vegetti, What You Can Scrape and What Is Right to Scrape: A Proposal for a Tool to Collect Public Facebook Data, SAGE journals, First Published July 31, 2020, p 2.

[5] Granville, K. The New York Times. Facebook and Cambridge Analytica: What you need to know as fallout widens (2018, March 19). Available at <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>.

[6] Cristina Criddle, BBC News Facebook sued over Cambridge Analytica data scandal (28 October 2020). Available at <https://www.bbc.com/news/technology-54722362>.

[7] CyberNews Team, Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof (06 April 2021, Updated on 07/04). Available at <https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/>.

[8] LinkedIn Pressroom, An update on report of scraped data (Jun 29, 2021). Available at <https://news.linkedin.com/2021/june/an-update-from-linkedin>.

[9] Lee Rainie, Pew Research Center, Americans' complicated feelings about social media in an era of privacy concerns (March 27, 2018). Available at <https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/>.

---

your friends and relatives will still disclose your personal information, such as your pictures, locations, and more on social media even if you take measures to safeguard your privacy on social media, including deleting your social media accounts. In another word, “Tell me who your friends are, and I will tell you who you are.” works on social media, too. In 2008 testimony, EPIC’s Executive Director Marc Rotenberg stated that “on Facebook ... third-party applications do not only access the information about a given user that has added the application. Applications by default get access to much of the information about that user’s friends.”[10] This makes it clear that we are not alone in controlling our privacy on social media.

To have a balance of privacy for all of us and organizations in this digital age is only possible through the toughest laws on privacy such as the General Data Protection Regulation (GDPR)[11], as well as increased inspections of companies responsible for protecting personal information under greater scrutiny. For example, the EU recognized the necessity for updated security as technology advanced, the Internet was developed and the European Data Protection Directive was adopted. Then in 2006 Facebook opened to the public and in 2011 the company was sued by a Google user for scanning her emails, Europe’s data protection authority declared the EU needed “a comprehensive approach on personal data protection”. Following the GDPR was adopted by the EU as the successor of the EU 1995 Directives as the result of the conceptual debates and issues regarding personal data. If privacy issues on social media are taken lightly, then digital privacy issues will invite more and more cyber attacks thereby leading

companies to lose their reputation, theft of sensitive records of users, and no trust of social media users. When it comes to digital data nothing can be completely private such as photos, conversations, health information, or financial information. If there is currently not a way to 100 percent obscure your online profile, then that could open the door to future strict regulatory action. “When it comes to making these decisions about privacy and vulnerabilities, without any clear law or anything, it all becomes a matter of opinion,” said Jeremiah Grossman, Chief of Security Strategy and Founder of WhiteHat Security.

Even today, many countries do not recognize the right to privacy as a specific constitutional right. Some countries have enacted general comprehensive data protection laws, and sectoral legislation dealing with privacy rights, yet privacy law has primarily evolved through judicial interventions in which the courts have read a right to privacy into existing rules. Considering that Internet, social media do not have a border, privacy needs international action. Although in many countries, international agreements such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights recognize privacy rights have been adopted into law, however, the law on privacy and its regulation mechanism needs to keep pace with technological development.

In conclusion, data privacy must not be ignored even if you think that you have nothing to hide. What we should be doing now is actively participating in the fight against the challenges that are causing the unintended death of data privacy in this era of digitization.

---

[10] Testimony and Statement for the Record of Marc Rotenberg Executive Director, EPIC, Hearing on “Impact and Policy Implications of Spyware on Consumers and Businesses” Before the United States Senate Committee on Commerce, Science and Transportation (June 11, 2008). Available at [https://epic.org/wp-content/uploads/privacy/dv/Spyware\\_Test061108.pdf](https://epic.org/wp-content/uploads/privacy/dv/Spyware_Test061108.pdf).

[11] What is GDPR, the EU’s new data protection law? Available at <https://gdpr.eu/what-is-gdpr/>.

---

## References

1. Piller C. "Privacy in peril". Macworld 10.7, Jul.1993.
2. Thomas McIntyre Cooley. Treatise of the Law of Torts. 2nd ed. Callaghan, 1888.
3. Kirsty Hughes, The social value of privacy, the value of privacy to society and human rights discourse, Published online by Cambridge University Press: 05 July 2015.
4. Moreno Mancosu and Federico Vegetti, What You Can Scrape and What Is Right to Scrape: A Proposal for a Tool to Collect Public Facebook Data, SAGE journals, First Published July 31, 2020.
5. Granville, K. The New York Times. Facebook and Cambridge Analytica: What you need to know as fallout widens, 2018, March 19. <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>.
6. Cristina Criddle, BBC News Facebook sued over Cambridge Analytica data scandal, 28 October 2020. <https://www.bbc.com/news/technology-54722362>.
7. CyberNews Team, Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof, 06 April 2021, Updated on 07/04. <https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/>.
8. LinkedIn Pressroom, An update on report of scraped data, Jun 29, 2021. <https://news.linkedin.com/2021/june/an-update-from-linkedin>.
9. Lee Rainie, Pew Research Center, Americans' complicated feelings about social media in an era of privacy concerns, March 27, 2018. <https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/>.
10. Testimony and Statement for the Record of Marc Rotenberg Executive Director, EPIC, Hearing on "Impact and Policy Implications of Spyware on Consumers and Businesses" Before the United States Senate Committee on Commerce, Science and Transportation, June 11, 2008. [https://epic.org/wp-content/uploads/privacy/dv/Spyware\\_Test061108.pdf](https://epic.org/wp-content/uploads/privacy/dv/Spyware_Test061108.pdf).
11. What is GDPR, the EU's new data protection law? <https://gdpr.eu/what-is-gdpr/>.