IMPACT OF PRIVACY VIOLATIONS ON SOCIAL MEDIA USERS

- Dr. Preeti Singh[*] & Dr. Avnish Singh[**]

Abstract

Privacy infractions on social media can be extremely damaging to the people they affect. The issue of privacy breaches has gained attention as a result of a recent change to WhatsApp's privacy policy that permits the sharing of users' personal data and information with Facebook. Due to this, many users are seeking out other messaging services in order to safeguard their privacy. Social media platform privacy breaches can result in a variety of negative outcomes for the victims, including identity theft, financial fraud, and even cyberbullying. In the case of WhatsApp, many users have voiced worries about the sharing of their personal information with Facebook, a company with a track record of privacy violations and improper use of user data for commercial gain.

This demonstrates the requirement for more stringent privacy safeguards on social media sites and more user education regarding the risks and perils of exposing personal information online. Ultimately, people who experience privacy violations on social media sites lose faith in both the network and their own capacity to safeguard their personal information. Social media sites must prioritise user privacy and have effective security measures in place to stop data breaches to reduce these dangers.

Keywords: *Social Media, Privacy, Breach, Victim, WhatsApp etc.*

[*] Assistant Professor of Law @ Bennett University (The Times Group), Email: singh.preeti1092@gmail.com

[**] Assistant Professor of Law @ Bennett University (The Times Group), Email: singh.avnish94@gmail.com

INTRODUCTION

The recent privacy hack involving users of WhatsApp emphasises the need for improved user privacy protection on social media platforms. A variety of detrimental effects, such as loss of trust, financial injury, and emotional pain, may befall privacy breach victims[1]. Users of WhatsApp, for instance, may have had their personal information, including phone numbers and chat messages, accessible by unauthorised third parties, raising the possibility of identity theft, cyberstalking, and other types of online harassment. Financial impact from this breach could also occur, such as loss of money from hacked bank accounts or fraudulent charges.

Furthermore, it is impossible to disregard the psychological effects of such violations. When their personal information is revealed to others, victims of privacy breaches may feel violated, out of control, and anxious. This might make people reluctant to interact on social media sites in the future or cause them to lose faith in the technology sector as a whole. Social media platforms must prioritise the safety of users' personal data by implementing robust security measures, clear privacy policies, and early notification of any security breaches in order to address these challenges. Additionally, they should give consumers the resources and tools required to keep an eye on and manage their personal information, such as the capacity to decline data sharing and the capacity to erase their data from the platform. Further improving users' privacy and security on social media platforms may be the development of privacy-enhancing technology like end-to-end encryption.

[1] Megha Mandavia, *WhatsApp tweaks privacy policy to share more user data with Facebook*, ETtimes, Jan 12, 2021; *available at:* https://economictimes.indiatimes.com/tech/technology/whatsapp-tweaks-privacy-policy-to-share-more-user-data-with-facebook/articleshow/80144280.cms?from=mdr

In order to develop clear principles and standards for data protection and to hold businesses accountable for privacy violations, governments and regulatory organisations must collaborate.

LAWS AND RULES RELATING TO PRIVACY

To protect data security and privacy, India has put in place a number of laws and regulations. Among the most significant ones are:

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[2], lay forth standards for businesses that gather, store, process, or manage sensitive personal data or information concerning Indian citizens. Companies must get people's consent before collecting personal data, make ensuring the data is accurate and current, and implement the necessary security measures to guard the data from unauthorised access or disclosure.

The Personal Data Protection Bill, 2019[3] is a measure that has not yet been passed but aims to give Indian citizens complete data protection. It establishes the Data Protection Authority of India to monitor adherence to the law and lays out criteria for the collection, storage, processing, and handling of personal data.

The Right to Information Act, 2005[4] under certain limitations and exemptions, enables citizens in India to have access to information maintained by public

[2] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (April 17, 2023), *available at:* https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

[3] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, (April,17,2023), *available at:* http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[4] *See,* The Right to Information Act, 2005, No. 22, Acts of Parliament, 2005 (India).

bodies.

The Aadhaar Act, 2016[5] is a piece of legislation that creates the Aadhaar unique identity system for Indian citizens and lays out rules for its collection, storage, and use.

The Information Technology Act, 2000[6] establishes sanctions for cybercrimes such hacking, identity theft, and phishing and offers a legal foundation for electronic transactions.

The Indian Contract Act, 1872[7] governs all contracts made in India, especially those that concern the security and privacy of personal data. It outlines the conditions that must be met for a contract to be valid, such as that both parties must offer their free and informed consent.

In general, these laws and rules seek to establish a framework for data protection in India and to guarantee that people have control over their personal data. Some experts, however, contend that the existing regulations are insufficient to solve the current problems with data breaches.

RISKS AND EFFECTS OF PRIVACY VIOLATIONS

For both people and organisations, data privacy violations in India can have serious risks and repercussions. Among these dangers and effects are the following:

Identity theft: Personal information, including name, address, phone number,

[5] *See,* The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).

[6] *See,* The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

[7] *See,* The Indian Contract Act, 1872, No. 09, Acts of Parliament, 1872 (India).

email address, and social security number, may be stolen as a result of a data privacy breach and used to commit identity fraud. Financial losses and damage to credit scores may result from this.[8]

Financial losses: Both individuals and organisations may suffer financial losses as a result of data breaches. Companies may experience legal costs, regulatory fines, and reputational damage in addition to direct cash losses, all of which can have a major negative impact on their bottom line.

Reputational harm: Both individuals and businesses may suffer from data breaches. Data loss can be considered as irresponsibility or incompetence in today's society, as data is increasingly valued as an asset, damaging relationships with stakeholders and customers.

Legal repercussions: Data privacy violations may have legal repercussions. For instance, businesses must guarantee the security and confidentiality of personal data under the Indian Information Technology Act, 2000[9]. Legal action and substantial fines may follow failure to do so.

Regulatory penalties: The Personal Data Protection Bill[10], which India just introduced, will impose harsher rules and restrictions on organisations that handle personal data once it is passed. Businesses who disregard these requirements risk severe fines and penalties.

Psychological effects: Individuals may have psychological effects as a result of

[8] Jennifer Bellemare, What are your odds of getting your identity stolen? IDENTITY FORCE (Apr.17, 2023), *available at:* https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics#:~:text=By%20the%20Numbers&text=In%202017%2C%206.64%20percent%20of,than%20twice%20the%20global%20average

[9] *Supra note 3.*

[10] *Supra note 6.*

data privacy violations. Anxiety, stress, and feelings of vulnerability brought on by the loss of personal information can have a long-lasting impact on people's mental health.[11]

Overall, there are serious risks and repercussions associated with data privacy breaches in India, so it is crucial for people and organisations to take precautions to safeguard personal information and avoid data breaches.

USER AWARENESS AND EDUCATION

In India, user education and awareness about data protection are essential because they can help people realise how important it is to secure their personal information and stop data breaches. Here are some suggestions for raising user awareness and education in India:

Government actions: The Indian Government may take actions to raise public awareness of data protection. To raise awareness about the value of data protection, they might hold awareness campaigns, seminars, and workshops.[12]

Education in schools and colleges: Schools and colleges can include data protection in their curricula to teach students the importance of privacy and data protection. This can increase awareness at a young age and help teach students appropriate behaviour.

[11] Harrell, E., 2019. Victims of identity theft, 2016. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. 1-29/NCJ 251147.(April, 17, 2023), *available at:* https://bjs.ojp.gov/content/pub/pdf/vit16.pdf

[12] Akash Dutta, *Data Privacy Day is an occasion to raise awareness among people on the issue: Prof. SK Shukla*, HTtech, August 21, 2022; *available at:* https://tech.hindustantimes.com/tech/news/data-privacy-day-is-an-occasion-to-raise-awareness-among-people-on-the-issue-prof-sk-shukla-71643340226542.html

Online resources: People can use a range of internet tools to learn more about data privacy. Government agencies may promote these resources and link to them from their websites.

Social media awareness: Data protection can be made more widely known by using social media platforms. To inform people about data privacy, businesses and individuals can post articles, blogs, and videos on social media.

Company training initiatives: Businesses might hold training initiatives to inform staff about data protection. Employees will be better able to appreciate the value of data security and help the company avoid data breaches.

Public-private partnerships: To raise awareness about data privacy, the government might work with commercial organisations. This can aid in expanding the audience reached and significantly increase user awareness and education.[13]

In order to prevent data breaches and safeguard personal data, it is vital to raise user awareness about and educate users about the importance of data protection in India.

CORPORATE RESPONSIBILITY AND ACCOUNTABILITY

WhatsApp and other social media platforms have a big obligation to safeguard the privacy and data security of their users. Some of the

[13] National Cyber Security Policy, 2013, Ministry of Electronic and Information Technology, (April, 17, 2023), *available at:* https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

explanations are as follows:

User trust: Since, the social media users trust these sites with their personal data, it is up to these platforms to make sure the data is kept secure. Users anticipate that social media sites will protect their privacy and data security by being open and honest about how their data is utilised.

Legal obligations: Social media platforms must abide by the rules and legislation governing data protection in the nations in which they do business. For instance, the Personal Data Protection Bill in India mandates that businesses take steps to protect personal data.

Business reputation: Social media networks have a reputation to protect, and data breaches or privacy violations can harm their brand image and make users lose faith in the platform. As a result, the platform may lose users and income.

Cybersecurity threats: Social media companies must take appropriate security measures to safeguard the data of its users because they are susceptible to cyberattacks. Data encryption, routine security upgrades, and threat detection are all part of this.

Ethical considerations: Social media platforms have an ethical obligation to safeguard the privacy and data security of its users. It is crucial to think about how data breaches or privacy violations may affect users' life and to take precautions to avoid such occurrences.

In general, social media platforms like WhatsApp are responsible for safeguarding the privacy and data security of their users, so it is imperative that they take the necessary precautions to protect that data.

TECHNOLOGY BASED SOLUTIONS

To stop data breaches in WhatsApp and other allied social media platforms, a number of technological options are available. Several of these options include:

End-to-end encryption: Only the sender and the recipient of a message can view the message's content thanks to this security safeguard. With the aid of this functionality, hackers will find it more difficult to intercept messages and steal personal data.

Two-factor authentication: By requiring two separate forms of identity, two-factor authentication is a security feature that stops unauthorised individuals from accessing accounts. As a result, there may be less chance of data breaches and user accounts being accessed without authorization.

Biometric authentication: A security measure known as biometric authentication verifies user identity by employing distinguishing physical characteristics like fingerprints or facial recognition. By doing so, the possibility of data breaches can be reduced, and unauthorised access to user accounts can be stopped.

Anti-phishing tools: Users can avoid falling for phishing attempts, which are frequently used by hackers to obtain personal information, by using anti-phishing tools. By identifying phishing messages, these tools can warn users of the danger.

Data backup and recovery: Tools for data backup and recovery can be used to guarantee that user data is backed up and is retrievable in the event of a data breach or system failure. This can lessen the effects of a data breach and prevent the loss of data for good.

FUTURE TRENDS AND CHALLENGES

In terms of data protection, there are a number of emerging trends and difficulties that we anticipate in the upcoming years.[14] Here are a few examples:

Increasing data volumes: People, organisations, and devices are all producing more and more data. In such a vast and complicated data landscape, it will become more and more difficult to protect personal data as a result of this development.

Rapid technological development: New data protection concerns are being brought about by the Internet of Things (IoT) and artificial intelligence (AI), among other technologies. For instance, the growing use of IoT devices introduces new security threats and vulnerabilities for personal data.

Stricter regulations: The General Data Protection Regulation (GDPR) in the European Union and the Personal Data Protection Bill in India are two examples of the tighter restrictions that governments around the world are putting into place to protect personal data. For businesses that operate internationally, compliance with these standards will be a substantial problem.

Cybersecurity dangers: Cybersecurity dangers including phishing, ransomware, and data breaches are become increasingly complex and difficult to spot and stop. To protect customer data, businesses must invest in strong

[14] Gavin Mills, Identity Theft: Everything You Need to Know to Protect Yourself, Summersdale Publishers (7 May 2006)

cybersecurity measures.[15]

Data ethics: Businesses will need to give data ethics top priority in their operations as the ethical use of personal data becomes more and more crucial. This entails being open and honest about how personal data is used, respecting people's right to privacy, and taking precautions to stop data misuse.

CONCLUSION

Overall, data protection will continue to be an important issue in the years to come, and it will be critical for people, businesses, and governments to collaborate in order to address the issues and safeguard personal data.

Finally, the current privacy incident affecting WhatsApp users emphasises the need for improved user data protection on social media networks. Social media platforms may aid in preventing privacy breaches and safeguarding the personal information of their users by putting in place robust security measures, open privacy policies, and privacy-enhancing technologies, as well as by creating precise norms and standards for data protection.

[15] Allison, S.F.H., A.M. Schuck, and K.M. Lersch, Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. Journal of Criminal Justice, 33 (1): 19-29, (2017).