शोध साहित्य SHODH SAHITYA
INTERNATIONAL PEER REVIEWED E-RESEARCH JOURNAL
(समसामयिक विषयों पर केंद्रित बहुविषयक मासिक ई-शोध पत्रिका)
E-ISSN 2584-2447
Impact Factor – SJIF 2024 = 3.621
Vol -2
Issue -1
November
2024

Role of Social Media and Privacy for Society

Riya Kumari
M.A Mass Communication

Dr. Asha Bala
Assistant Professor
Department of Mass Communication
Sri Guru Ram Rai University, Dehradun Uttarakhand

INTRODUCTION

Sharing private information through social media is commonplace in today's society and lifestyle. Individuals use numerous social networking sites such as Facebook and Instagram. These users share their private information, particularly upon registration to become a member of the sites. They also reveal their private information by making regular updates and posts that they put online. As a result, an individual can easily be traced and manipulated through the information offered on these websites making internet privacy a major concern. This sheds light on the importance of learning technological abilities to enable social media users deal with the issue of privacy on these websites.

Media has entered in almost every sphere of our lives, connecting us to both the local and global community. Most popular these days are social media platforms. These have become the most preferred pedestals of sharing information, most importantly on glaring social issues. They have become a vital source of information, especially for the younger generation. Hence, they create a glaring impact on young minds.

This is where the issue of the right to privacy creeps in. Right to privacy is a fundamental right of every citizen of India, interpreted by the Supreme court of India to derive from Article 21 of the Constitution of India. The issue at hand is that of competing claims between staunch advocates of social media platforms and people claiming breach of their right to privacy, at the behest of social media platforms, eulogized as the right to freedom of speech and expression.

Social media usage is constantly growing as people like to connect, share posts, videos, and photos, and engage with others. However, it's essential to be aware of the potential privacy risks and to know how to protect users' personal information. People are becoming more careful about their privacy, what they share on social media, and what social platforms do with their social media data. Even with tough privacy laws, sensitive user information could be at risk.Social media managers, content creators, and business owners need to manage data privacy across social media platforms. The first step towards solving

social media privacy issues is identifying them. Then, adequate steps for ensuring privacy on social media should be implemented. In this guide, we'll describe the most common social media privacy issues.

Why Is Social Media Privacy Important?

People often share personal and even sensitive information on social media platforms. Besides this, tracking cookies, cross-site tracking, tracking pixels, or other similar tracking technologiescould track a user's online activity such as webpage views, social media sharing, or purchase history. All this data is gathered and sorted by user segments, which then data owners sell for marketing purposes.

However, scammers and fraudsters can also get access to this information and use it for their malicious purposes. Reports about fraud originating on social media have soared over five years. In 2020, 46,000 reported in losses to fraud, while in 2021, more than 95,000 became victims of fraud on social media, according to the Federal Trade Commission.

What Types of Data do Social Media Platforms Collect?

Social media platforms often collect personally identifiable information, together with interests, purchases, internet browsing activities, lists of friends, geo-locations, and others. Often, when users sign up for an account, they agree to the terms and conditions, including access to social media platforms to collect users' personal data.

There are some examples of sensitive data:

1. medical or health records
2. biometric data (e.g. fingerprints or DNA);
3. education records
4. credit card data
5. financial records
6. personal identifiers, such as age, ethnicity, and race
7. photo of a face
8. personally owned property
9. employment information and applications
10. status updates at work, life, and relationship events
11. religious beliefs
12. location data
13. shared content on social media;
14. engagement on social media, such as likes, shares, or comments. Common Social Media Privacy Issues

Malware and viruses. Malware and viruses can spread through social media platforms. They can steal sensitive data, infect, or slow down users' computers. Cybercriminals can take over the social media account of a user and spread malware to the affected account of the user and all the user's friends.

Fake information. Social media can be used to spread false information or propaganda quickly. Trolls and bots often provoke social media users by manipulating emotions. They can also create a fake account or advocate for a person by posing as a person. It has also been used for harassment, or cyber bullying. Most social media platforms have content moderators or procedures for how other customers could report fake information, but it takes time for posts to be marked or deleted. You should always check information before resending it or making conclusions on social media.

Phishing Attack

Social networking sites are a popular target for cybercriminals who want to exploit users personal information for their gain. On social media, phishing attacks—where users are tricked into disclosing their login credentials or sensitive information—are common. To trick users and obtain unauthorized access to their accounts, cybercriminals may pose as reliable organizations, transmit harmful links, or develop fake login pages.

Harassment and cyber bullying. Defrauders can send threatening messages, perform harassment, or cause emotional trouble even without getting into users' social media accounts. Publicly visible inappropriate comments on social media accounts are one of the forms of harassment. Cyber bullying includes sharing negative or harmful content about persons on social media platforms.

Data mining. Scammers use data mining for identity theft. They do not need much data for that. Actually, publicly available information on social media can help them successfully target victims. Scammers can get email addresses, usernames, phone numbers, and physical addresses quite easily. With this data, they can send phishing scams or gather more information like leaked passwords or credit card numbers.

Even with your account set to private, advertisers and scammers can gain access to your sensitive data in the form of:

1. Profile information - such as your name, birth date, and contact information.
2. Status updates - including personal life events, work and relationship status, and religious beliefs.
3. Location data - such as your hometown information and geo check-ins.

4. Personal interests - including hobbies and buying history.
5. Shared content - such as personal images and videos.
6. Posts from friends and family - anything someone posts about you can be found and used by advertisers, hackers, and fraudsters.

Growth of Social Media and its Increasing Influence on Youth

From a thirteen-year-old child to a seventy-five-year-old senior citizen, from a daily wage worker to a software engineer, everybody is on social media. Social media sites like Facebook, Instagram, Twitter, Youtube, have made almost every mobile phone in their home. Among all these kinds of people, it is the youth who is most involved in social media. This involvement may have positive repercussions for some, these include easy accessibility to a wide variety of information, providing an encouraging platform to showcase their creativity, skills and also voicing their opinions on issues which may be social, political or economic. Therefore, it may serve as a source of empowerment for the youth.

With this flexibility, every person has access to a platform where he or she may share information or voice his or her opinions. However, it has to be kept in mind that this free flow of information is by no means an all empowering process for everyone. This may prove to be a bane for some innocent people who may fall prey to others mal intentions. Yes, flowing of false information, intentionally or unintentionally has become a commonplace on social media. We often hear news of fake allegations like that of sexual harassment, fraud etc particularly to defame someone. There are also many cases where someone's personal information is made available on the internet for public view. All this amounts to a breach of the fundamental right to privacy.

Social Media and Privacy Related Laws In India

Laws related to social media and privacy in India are clearly insufficient. The Indian judiciary and legislature have proved to be far behind expectations when it comes to the framing of laws in this arena. Some rules and legislations have been issued, those too are primarily related to defamation.

In the Kharak Singh v State of UP, often called the PUCL case, it was held that tapping of phones amounts to a breach of privacy. Extending this reasoning, it can be reasonably held that sharing of information by WhatsApp with Facebook, post its update, is an obvious breach of privacy of its users.

Now let's come to the Information and Technology Act, 2000. The concept of privacy in this act is comprehended in a very liberal and traditional sense. The act of knowingly

sending pictures of a person's private parts, without his permission, then Section 66E of this act is violated. Social media finds only a mention in Section 79 of this act. This section clarifies that if any person posts or uploads anything derogatory to some other, then the medium on which it is posted, that is Twitter, Facebook etc, is not to be held liable for the acts of such person. Beyond this, nothing is mentioned in the whole article with regard to social media. Let us understand this by a simple example- If X, a Facebook user posts something derogatory to Y, another Facebook user, then Facebook is not to be blamed for X's act.

This concept has however evolved with time, in the case of Shreya Singhal, it was held that it is Facebook's duty to remove any material posted by them which is objectionable. This has to be done by Facebook, applying its discretion, after complaints regarding the same are received.

One concept to be noted here is the growing popularity of meme culture. Memes of famous personalities carrying derogatory comments and comparisons can be safely termed as an invasion of the privacy of such individuals. To check such incidents is urgently required.

Next, let's learn about the recent Whatsapp- Facebook Privacy Case or Karmanya Singh v. Union of India. Constitutional rights were meant to deal primarily with the relationship between the state and individuals. However, this concept has seen a marked change due to the boom of privatisation in India. Private companies have taken up many functions which are traditionally associated with the state. Our Constitution makers, however, had framed laws according to the situation of the country which was prevailing at that time.

Due to these changed conditions, these private actors when performing state-like actions are subjected to the same Constitutional scrutiny. In the case at hand, the contract between two social networking sites, Whatsapp and Facebook was challenged, both private parties, invoking the above-mentioned ideology.

The facts of this case are – Whatsapp contends that now Facebook is its parent company, and hence data of its users can be sent to the latter. Examples of the data in question are- names, phone numbers, credentials, location, status etc. This vulnerable data may be used for a number of purposes of which the users would not even be made aware of. The most harmful one being the risk of uncalled for surveillance. It was also noted that this update of WhatsApp would affect a wide variety of users, most of whom would not even be aware of the damage that can be caused to them.

This case is presently pending before the Supreme court of India. The question of privacy as a fundamental right was then referred to a larger constitutional bench. This bench ruled that privacy has a tripartite structure namely, intimate, public and private zones of privacy. The intimate zone includes physical and sexual privacy, the private zone encompasses ATM number, PAN number etc. These two zones, held by the Supreme court of India are beyond the facts of the case at hand. The zone of public privacy, it was held, has to be dealt with on a case to case basis. The present case falls under this zone and is pending before the Supreme Court.

Social media companies are voicing significant concerns over the new Digital Personal Data Protection (DPDP) Act, particularly focusing on the challenges posed by restrictions on behavioural tracking of children and the need for verifiable parental consent (VPC), according to a report by The Economic Times.

As the Indian government prepares to release the rules for the DPDP Act, these platforms hope their issues will be addressed to balance privacy with safety.

What is the Digital Personal Data Protection Act?

The DPDP Act was notified in the Gazette in August last year. The Act has previously been criticised for allowing the government to access private and government agency data on grounds of sovereignty or public order, raising concerns about potential misuse of power and privacy infringement.

What does the Act say about data protection of minors?

As a protection measure, the Act requires verifiable consent from a legal guardian for processing data of children under 18. This necessitates age verification, potentially compromising digital anonymity and conflicting with India's obligations under the Convention on the Rights of the Child. It also includes stringent provisions in Section 9 that disallow behavioural tracking of children on digital platforms.

Tech giant concern with behavioural tracking

The inability to track behaviours of children has raised alarms among social media companies, as they argue that behavioural tracking is essential for ensuring the effectiveness of their safety features designed to protect young users.

Major players like Google, Meta, YouTube, and Snap, have expressed their worries about the implications of the DPDP Act. They assert that tracking user behaviour, including that of children, is crucial for detecting and preventing predatory behaviour and other online threats.

शोध साहित्य SHODH SAHITYA
INTERNATIONAL PEER REVIEWED E-RESEARCH JOURNAL
(समसामयिक विषयों पर केंद्रित बहुविषयक मासिक ई-शोध पत्रिका)
E-ISSN 2584-2447
Impact Factor – SJIF 2024 = 3.621
Vol -2
Issue -1
November
2024

Social Media Privacy Solutions

While the privacy concerns in the realm of social media can appear daunting, there are several practical solutions and strategies that individuals can employ to protect their personal information and online privacy. Here are some key steps you can take:

Review and Adjust Privacy Settings

1. Enhance Privacy Settings: Most social media platforms offer extensive privacy settings that allow you to control who can see your posts, access your personal information, and interact with you. Take the time to review and adjust these settings to align with your comfort level.
2. Limit Data Sharing: Opt to limit the data you share with these platforms. This can include restricting access to your location, contacts, and other sensitive information.

Use Virtual Private Networks (VPNs)

1. How VPNs Work: Virtual Private Networks, or VPNs, encrypt your internet connection, making it difficult for third parties to monitor your online activities. By using a VPN, you can significantly enhance your online privacy and security.
2. Protecting Personal Data: VPNs are particularly useful when accessing social media on public Wi-Fi networks, where your data is more vulnerable to interception.
3. What Do Companies Do With This Data?

Platforms for social media employ data to analyze the market, display targeted adverts, customize services, and suggest postings. Likes and dislikes can both influence how an individual is portrayed on social media.

Businesses use this data to learn more about the preferences of their clients. If the advertising is appropriate for their channels, they might inquire. These few questions can aid in tailoring advertisements to a person's interests.

Your interests are also questioned in social media polls. These replies are logged, and businesses that are interested in user interests, as well as those in comparable interest categories, such as pet owners, vehicle enthusiasts, or video gamers, can buy the data. Companies can tag people in their social media postings to keep them interested using the data gathered from these polls.

A platform is compensated for promoting a brand. Users who have access to information about the advertising brand may see these posts as sponsored content.

Companies make payments to show up in consumers' social media feeds who are interested in their products. Tracking cookies or shared information is used to collect this specific data. Companies may utilize users' provided email addresses or phone numbers to contact them with information about their goods and services.

THE LATEST SOCIAL MEDIA CONTROVERSY: BANNING OF TIKTOK

In April 2019 the Madras High Court passed an order to direct the state government to prohibit the use of the TikTok App, and they called it dangerous. The Indian government banned the TikTok app on 29 June 2020 and called it detrimental to the integrity of India and the sovereignty, public order, and security of the state. The act was banned under section 69(a) of the Information and Technology Act r/w with the provisions of Information Technology (Procedure and Safeguards for Blocking of Access to Information by Public) Rules 2009.

The Ministry of Electronics and IT has received various complaints from their sources that the data of the users is stolen in an unauthorized manner and sent outside India. The Indian Cyber Crime Coordination Centre gave recommendations for blocking these apps.

INTERNATIONAL LAWS RELATING TO SOCIAL MEDIA

In Germany, there is a law called NetzDG in which they set up the procedure so that they can review the content, and if any illegal material is found then it has to be removed within 24 hours, and also give updates about what's happening by them and if they did not remove it then they have to pay the fine.

In the European Union, they only emphasize terror videos if the content is not removed within one hour, then they have to pay a huge fine. In Australia, the Online Safety Act Act 2015 was created so that social media companies would not harass others and remove abusive posts otherwise they have to pay huge fines.

In Russia and China, some apps such as Google, Twitter, and WhatsApp are banned so that their information cannot be shared beyond their territories and they have lessened their cyber-attacks by banning these apps.

SUGGESTIONS TO PROTECT INFORMATION

Be cautious while opening a new social media account because each site has a bigger danger. Make sure the platform is safe and reliable before using it. If you're leaving a

platform, delete your account first. The following are some other strategies for protecting information:

1. Create secure passwords. Never use the same password for many apps or websites. Use a password manager to securely store information to aid in remembering sign-on credentials.
2. Don't overshare. Don't go into more detail than is necessary. On all sites, users shouldn't be required to disclose their addresses or dates of birth.
3. Don't click on suspicious links. Avoid clicking on links unless they come from a reliable source, even if they look to be from a friend.
4. Avoid public devices. When done utilizing a shared device, make sure you log out.
5. Disable geolocation data. In the privacy and security settings on the phone, disable sharing location data with apps.
6. Use two-factor authentication. The app's security is increased by implementing two-factor authentication, which may include a passcode and biometric identification.

CONCLUSION

In the age of digital interconnectedness, social media has brought about transformative changes in the way we communicate, connect, and share our lives. However, this remarkable digital revolution has also cast a shadow - a dark side that encompasses privacy concerns and potential risks to our personal information. As we conclude our exploration of "The Dark Side of Social Media: Privacy Concerns and Solutions," it is imperative to reflect on the key takeaways and the path forward.

1. Awareness is Key: Understanding the privacy concerns associated with social media is the first step toward safeguarding your personal information. Being aware of how data is collected, tracked, and used by social media platforms empowers you to make informed decisions.
2. Individual Responsibility: Users must take individual responsibility for their online privacy. Reviewing and adjusting privacy settings, employing VPNs, and practicing digital literacy are actions that users can take to protect themselves.
3. Government Regulations: Privacy regulations like GDPR and CCPA provide a legal framework to hold social media companies accountable for their data handling practices. These regulations set global standards and encourage more responsible data management.
4. User Advocacy: User advocacy groups play a crucial role in advocating for privacy rights, raising awareness, and lobbying for stronger privacy laws. These organizations empower individuals to assert their digital rights.

5. Ongoing Vigilance: The digital landscape is constantly evolving, and so are privacy concerns. Staying informed, adapting to new tools and technologies, and advocating for stronger privacy protections will be ongoing endeavors.
6. Balancing Act: Achieving a balance between the convenience and benefits of social media and safeguarding personal privacy is a continuous challenge. As users, we must strike this balance to enjoy the benefits without compromising our security and personal information.

As we navigate the dynamic world of social media, let us remember that while technology has given us incredible opportunities for connection and expression, it also places upon us the responsibility to protect what is most valuable — our privacy and personal data. By remaining informed, advocating for change when necessary, and adopting privacy-conscious practices, we can enjoy the best of both worlds — the digital connectivity of social media and the assurance that our personal information is kept safe from prying eyes.

In this ever-evolving digital age, we must stand together as informed users, advocates, and responsible digital citizens to ensure that the future of social media is one where privacy is respected and protected.

REFERENCES

1. https://assets.pewresearch.org/wpcontent/uploads/sites/14/2013/05/PIP_TeensSocial MediaandPri vacy_PDF.pdf
2. https://cdn.manesht.ir/11890Big%20data%20privacy%20issues%20in%20public%20social%20media.pdf
3. https://dataprivacymanager.net/how-to-protect-your-privacy-on-social-media/
4. https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020
5. https://nordvpn.com/blog/social-media-privacy-issues/