IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 4.819
Volume 1, Issue 3, January 2021

Encryption Policies of Social Media Applications and its Effect on User's Privacy

Prof. Karishma Tiwari and Narendranath B Gavande
Asst. Professor and Research Scholar
karishma179@gmail.com and narendragavande29@gmail.com
St. Rock's College of Commerce and Science, Borivali (W), Mumbai, India

Abstract: *The motive behind this research paper is to outline recently introduced social media encryption policies and the impact that they will have on user privacy. With close to no Data Protection Laws in the country, all social media platforms pose a threat to one's privacy. The various new privacy policies that have been put in place across different social media platforms, tend to take away the user's choice on whether they want their data shared with other social media apps or no. Seeing how WhatsApp, Facebook and Instagram are all Facebook owned, any data shared across one platform crosses over with the database of another, regardless of whether you have an account or not, completely taking away from the concept of consensual sharing of data. This paper will further discuss how the nature of encryption in India will significantly affect India's newly recognised fundamental right, the Right to Privacy. Various policy developments bring in various user violation concerns and that will be the focus of this research paper.*

Keywords: Encryption, Policies, Social, Media, Applications

I. INTRODUCTION

With the extensive use of social media in recent years, privacy has been an eminent topic of discussion. A person, knowingly or unknowingly, shares a lot about themselves on the internet, and with such extensive usage, comes the paramount concern of user privacy and data protection. To give an example, WhatsApp, Facebook, and Instagram are all Facebook owned, any data shared across one platform crosses over with the database of another, regardless of whether you have an account or not, completely taking away from the concept of consensual sharing of data . The internet, specifically social media, has a very open and/or public nature and any data shared can be distributed amongst a much larger audience than the user initially intended.

The layman cannot possibly protect itself from the wrath of the internet, their limited knowledge and experience with the tools of the internet do not help either and that is exactly why the need of the hour is to put data protection laws into place. This paper aims to provide an insight into the problems faced by users and what can be done to rectify them, how can the internet become a safer platform for people to share and experience and why exactly are there such privacy concerns in the first place.

Encryption used in social media

Encryption may sound like a new concept to a few, but it is not. It is what ensures secure communication over the internet and the transmission of data.

Without it, all private and confidential transactions would be impossible and high risk. Following the revelations, apps like Telegram were developed that offered end-to-end encryption, and already existing apps like WhatsApp followed suit, partly to maintain market share and partially to avoid having to comply with requests for data and information from law enforcement agencies. WhatsApp has been encrypting data for its communications since 2013, and it has finally achieved strong end-to-end encryption.

Privacy concerns in social media :- By using social media platforms, people open themselves to several privacy concerns and dangers. If information is not shared responsibly online, it can be misused in many ways and pose a threat to one's safety. Incidents of data breaches have highly alarmed many users and forced them to rethink their usage of the internet. It provokes the thought that they might have lost control over their own data and information, which in a lot of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 4.819
Volume 1, Issue 3, January 2021

cases, proves to be true. The many cases of exploitation of users' data have instilled a feeling of distrust and has deteriorated the various social media company's reputations.

Types of breach attacks online :-

Different types of Major Domain Attacks

- Attacks on the infrastructure of social networks
- Malware Infections
- Phishing attacks, third
- Evil twin assaults
- Attacks involving Identity Theft
- Cyber bullying
- Physical Attacks

II. REVIEW OF LITERATURE

2.1 Encryption and Privacy Protection:

Many studies highlight the role of encryption in safeguarding user data and communications. They underscore that robust encryption, particularly end-to- end encryption, is essential for protecting the privacy of users on social media platforms.

Security vs. Privacy Trade-offs:

Researchers often delve into the trade-offs between security and privacy in the context of encryption policies. While encryption enhances user privacy, it can also raise concerns related to security, as it may be exploited by malicious actors for illegal activities.

2.2 Objectives of the Research

To understand the concept of Encryption Policies.

III. RESEARCH METHODOLOGY

This study is based on Secondary data. Secondary data collected from various books, journal, internet, etc.

IV. FINDINGS

Privacy Concerns of Governments: Many governments have expressed concerns about the use of strong encryption on social media platforms, as it can hinder their ability to access user data for law enforcement and national security purposes. This has led to debates and discussions about striking a balance between privacy and security.

Global Variances in Encryption Policies: The research highlights that encryption policies vary around the world due to different regulatory environments and user expectations. Some countries promote strong encryption to protect user privacy, while others place restrictions on encryption to enable government access.

V. CONCLUSION

Social networking sites have few security concerns, and the number of users attempting to implement the necessary changes to their online media security is far smaller than for other types of security jobs. Additionally, many online media clients lack specialised updates, which results in low security concerns for their own content. Furthermore, many users are unable or unwilling to correct such inaccuracies. There is a lot of information that may be transmitted through the internet, yet virtually no user has any control over it. We will be able to secure the social networks from new vulnerabilities and ensure smarter and more responsible users if we enforce a set of clearly defined rules and policies for social media, including the use of strong passwords, awareness of the importance of changing your passwords frequently, awareness of information disclosure, and importance of antivirus or related software. In this paper, we have identified the shortcomings of the already existing policies and systems and have also talked about what can be done to improve those. On execution of it all, the internet will prove to be a safer space for all and a comfortable and secure

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 4.819
Volume 1, Issue 3, January 2021

environment for sharing and transmission of data. The huge acknowledgment of OSNs by the clients gives freedom to the assailants to make and cause new troubles and assaults each day. An extremely huge, circulated information base is utilized for OSNs, and this goes about as a benefit to make misuse ideal on the grounds that OSNs incorporate local areas of clients that offer similar interests in the structure of uses. These clients share similar applications with the assistance of stage receptiveness. This receptiveness brings about a client introducing the application which is vindictive and contaminated.

REFERENCES

[1]. T. Golshan, "Why it's now impossible for WhatsApp to help agencies like the FBI access messages," Vox Technology, 6 April 2016, available at

[2]. Data Security Council of India, "Encryption Policy".

[3]. K. Wagner, "Is Your Messaging App Encrypted?," Recode, 21 December 2015

[4]. J. E. Dunn, "WhatsApp's end-to-end encryption explained: What is it and does it matter?," TechWorld, 6 April 2016