THE REMOVAL OF END-TO-END ENCRYPTION IN INSTAGRAM BY META AND ITS LEGALITY AS PER INDIAN LAWS

Nirupama Narayan, BBA LLB (Hons.), Sastra Deemed University

Revathy Sunderesan, BBA LLB (Hons.), Sastra Deemed University

ABSTRACT

As Meta decides to roll back the End to End Encryption option from Instagram over alleged low user rates and pressure from multiple governments and activist bodies across the world, this paper tries to discuss what the effects of the change would mean on the Indian user population and the extended impacts of what this decision may result in various other tech sectors. By first understanding and decrypting what exactly end to end encryption is, its architecture and its evolution with Meta, their stance on its other messaging services and the future predictions around the same, this paper tries to build on what this change could mean for Instagram users. Moreover it looks at the overlap of where privacy concerns for the Indian population stand and the history of surveillance tactics and data breaches caused by Meta in various parts of the world and what effect this may have on users being targeted with more and more concerningly personalised advertisements. With billions of daily users on its platforms, Meta is an undisputed hub of personal information which ranges from user activity, their contacts, their friends contacts, their device information, their location, their online and private interactions, information for third parties etc. giving them more responsibility to track and uncover illegal activities would be very efficient but in reality, whether this is truly meant to combat the spread of illicit material online or is a symbolic representation of individual privacy taking a backseat allowing surveillance in the name of national security is unclear. With where the objective of being a preventive measure for heinous crimes ends and being a tool of governmental supervision begins being blurry, this paper also covers the legality of such a change with relation to the current frameworks in India mainly the Digital Personal Data Protection Act, 2023 and the Indian Constitution to review the current position and what may have to change in the near future.

Keywords: End to End Encryption, Privacy, Digital Surveillance, Digital Personal Data Protection Act, Article 21

Introduction

In 2019, Meta pledged to introduce end to end encryption technology across messaging services on Facebook and Instagram, saying "the future is private" but as of May 8th 2026, Meta officially announced that it was removing their previously lauded feature on one of those services - Instagram[1]. This means that from here on network providers and institutions will be able to access messages, photos, videos and voice notes. The announcement was met with much controversy and discourse around its anticipated impact on user privacy and extended issues. The decision was prompted by international pressure on Meta to allow government bodies to access messages and online communication to scan for safety threats and to expose child predator networks and the spread of child sexual abuse material(CSAM).[2] Various safety groups have welcomed this change as a positive measure but it does give rise to pressing concerns regarding the extent of the overlap between scanning for preventive and protective reasons and the infiltration of user privacy. Other services like WhatsApp which introduced end to end encryption (E2EEe) in 2016 remain untouched as yet but considering the global trend of crackdowns on E2EEe it may not be long for shifts there as well.

India with a wide history of suffering through various degrees of data breaches and security risks sits at a precarious position as this decision would affect upwards of 390 million Indian users.[3] As of October 2025 India has the single largest population on the app, over double the amount of users from the United States, the second largest user population. Now, not only the new messages be open to scrutiny but also previous communications will be up for grabs, Meta is suggesting users to download their chat history if they want to not be subject to this but this was to be done before May 8th to fall out of the purview of impacts after the crackdown on E2EEe. For a population as vast and expansive as India this would result in the privacy of all the users who had not promptly followed the guidelines be laid bare. As of now the fallout of this has yet to be observed but any discerning individual aware of the history of mass data breaches India has faced this decade would be right to be apprehensive.

[1] Instagram, "End-to-end encryption on Instagram", *Instagram Help Center*, 8th may 2026, available at <https://help.Instagram.com/491565145294150/?helpref=uf_share> (last visited on 20th May, 2026)
[2] Joe Tidy, "Instagram privacy tech is turned off today - what does this mean for your DMs?", *British public service broadcaster, may 8th 2026, available at <https://www.bbc.com/news/articles/clypzxl3lvqo>* (last visited on 21st May 2026)
[3] Market Biz "Instagram Users Statistics and Facts (2026)" available on <https://market.biz/Instagram-users-statistics/> (last visited on 20th May, 2026)

This change also comes after pressure from foreign governments to allow the scanning of chats to search and detect material which may be proliferating child sexual assault material. These include the UK's Online Safety Act 2023[4] which gives power to Ofcom to scan for the same and the Take It Down Act[5] signed last year from the United States which requires platforms to detect and remove non-consensual intimate imagery within 48 hours. In India Acts such as Digital Personal Data Protection Act, 2023 (DPDP Act) and the Information Technology Act, 2000[6] (IT Act) govern the collection and usage of user data by corporations and how to balance privacy to broader sociological concerns, but the changes brought forth by Meta and the recent trend of privacy taking a backseat bring to question the efficacy of such balances. Moreover, the Digital Personal Data Protection Rules, 2025 make it clear that Meta is data fiduciary as per section 2(i)[7] and as such is to release any information to the state under section 7(c) in the interest of sovereignty, integrity and security of India. This is a very vague scope and its language is similar to what is mentioned in section 152 BNS[8], an already very controversial section accused of being the rebrand of sedition. Therefore, many users are concerned and doubtful about what the State's next steps will be and what will ultimately be the fall out of such changes.

Research problem

What does Meta discontinuing end to end encryption in Instagram mean for its users and how does this decision align with India's current legal framework emphasising the Digital Personal Data Protection Act, 2023 and the Indian Constitution.

Literature review

The research report Politics of Digital Surveillance, National Security and Privacy published by H. Akın Ünver in 2018[9] discusses the dilemmas around digital surveillance and the duty of governments to balance 'secrecy, transparency and surveillance' and how because of political, strategic necessities along with the divided reaction of the public they have to 'come up with

[4] Online Safety Act 2023 (OSA) (c. 50)
[5] S.146 - 119th Congress (2025-2026): TAKE IT DOWN Act
[6] The Information Technology Act, 2000 (Act 21 of 2000) notified on 17 October 2000
[7] The Digital Personal Data Protection Rules, 2025, s.2(i) and s.7(c)
[8] THE BHARATIYA NYAYA SANHITA, 2023 (Act 45 of 2023) s.152
[9] Ünver, H. Akın, Centre for Economics and Foreign Policy Studies "*Politics of Digital Surveillance, National Security and Privacy*". 2018. Available at < http://www.jstor.org/stable/resrep17009 > last visited on 14th May 2026

the surveillance-privacy balance that conforms to the country's political culture, but also to the universal human rights'. It also discusses the concept of a 'surveillance industrial complex' which is in essence almost a business model where governments and corporations cooperate to gather and process user data and the dangers of such an alliance as it would create a quasi public-private surveillance nexus which traps citizens and they lose access to their own personal data for commercial and national interests. Further, the report argues that by increasing surveillance in a way which undermines user privacy, it only forces those users to innovate and create more complex and varied methods to bypass such surveillance. The core problem the report puts out is that 'Digital surveillance oversight has to balance between an impetuous executive that seeks to engage in power-maximizing behavior, and an inquisitive public, which is interested in preventing corruption, mismanagement and abuse.' Essentially the tussle between the authoritative efforts of the government and that of the public to stay free in their actions.

From the report, readers can easily see that the delicate balance between privacy and surveillance is the core concern for most users of the internet. Ultimately it comes back to the extent of trust the impacted user population and the government in question have between each other. When it comes to India, at a time where critique towards government entities is at an all time high and with prolific cases of data breaches like the Aadhar database leak in 2018 which affected over 130 million citizens and the ICMR(Indian Council of Medical Research) data breach where the personal information of over 815 million citizens was sold on the dark web just in 2023, regardless of the intentions of the government, the citizens are always left in a vulnerable position.

Moreover, as of 2026 India has fallen to the 157th position out of 180 countries in the world press freedom index[10]. Such a shift has heightened public tensions and made the public more doubtful of the real effects of changes to the digital infrastructure like what this article tries to discuss, the discontinuation of end to end encryption. No matter the reason why Meta brought in that change, it opens up possibilities of the state using this to not just scan communications for illegal, actionable material like child pornography, which should be done rightfully so, but also to further monitor and sit into user's actions. Again, with Indians making up the majority of Instagram users, the affected sample size would be colossal. Furthermore, there is the possibility that instead of targeting the actual perpetrators of such content, its overflowing

[10] Reporters Without Borders "ASIA-PACIFIC - INDIA" available on <https://rsf.org/en/country/india>

effects mainly end up on the average user. The report mentioned that citizens would be pushed to break the purview of surveillance if it is enforced too tightly and that surveillance methods would never reach a point of equilibrium because it'll always have to adapt and overcome the new methods of escape being created. As such, said perpetrators would simply switch to other safer routes leaving the average, unaware user to expose his private life to his government.

Technical Background and Encryption Architecture

End-to-end encryption is a secure communication process wherein the data is encrypted to prevent unauthorized access from service providers that facilitate the transaction and other 3rd party servers[11]. This process involves the travelling of data only between 2 parties- the sender and the recipient. This encryption is considered to be far better than the rest since it provides data security during transmission by ensuring the plain text is converted to cipher text while also ensuring that only the 2 concerned parties are able to decrypt the message by using a specialised version of encryption known as asymmetric encryption.

Meta uses a standard transport layer security encryption[12] (TLS) which is a complete security protocol used to establish a secure connection between the application and Meta's servers. This authenticates the website and ensures no third party attacks take place. Meta ensures that anytime a person opens any of their apps, the electronic gadget connects to Meta's server and establishes a secure network space.[13] This security system ensures that even during transmission phase, the message remains unintercepted by external forces or by Meta itself.[14] A simple example to understand the same: An ornament sent through the post is tightly sealed and cannot be modified during transportation.

Asymmetric Encryption is a form of encryption colloquially known as 'Public Key Encryption' which consists of 2 keys- public key and private key to encrypt and decrypt data.[15] The

[11] Patil, B & Kharade, Kabir & Kharade, Shraddha & Kamat, Rajanish. (2021). "Significant Study of Data Encryption and Steganography." DOI:10.9734/bpi/ramrcs/v1/6978D. (last visited on 20th May 2026)
[12] Manu Bretelle, "DNS over TLS: Encrypting DNS end-to-end " (2018) available on <https://engineering.fb.com/2018/12/21/security/dns-over-tls/> (last visited on 18th May 2026)
[13] Geeksforgeeks, "Transport Layer Security (TLS)" (last updated: 10th, April, 2026) available on <https://www.geeksforgeeks.org/computer-networks/transport-layer-security-tls/> (last visited on 19th May 2026)
[14] Amit Tidke, "Understanding TLS(SSL) Encryption: Symmetric vs. Asymmetric" available on <https://medium.com/@amittidke/understanding-tls-ssl-encryption-symmetric-vs-asymmetric-f4eef15270d4 > (last visited on 19th May 2026)
[15] Geeksforgeeks, "Asymmetric Encryption" (Last Updated : 21 Nov, 2025), available on <https://www.geeksforgeeks.org/computer-networks/what-is-asymmetric-encryption/> (last visited on 19th May 2026)

generation of the 2 keys is such that the public key can be shared openly to anyone while the private key pertains to a certain individual and is kept a secret. The process of this encryption is such that the sender uses the public key of the recipient to encrypt the message and upon receipt the recipient uses their private key to decrypt the message. This encryption ensures that even during transmission, if the message is intercepted it remains unreadable. To briefly explain this with an example, suppose an ornament is sent to a person in a locked box with a key with the sender and a spare with the receiver. No party involved in the transmission has any means of opening it.

Meta platforms introduced end-to-end encryption by default to chats and calls on WhatsApp, Facebook and Messenger. [16]A technology that was only available to the elite and tech savvy, was suddenly provided to the masses in the modern world by including it in social media apps to prevent data breach and respect the right to privacy of every Indian citizen by ensuring unauthorized access is denied. The platform publicly announced that it was going to bring encryption to Instagram to prove the 'future is private' by giving users the option to opt in for this choice back in 2022. However, unlike WhatsApp, which provided for encryption on default, Instagram left the choice to its users to manually enable 'secret conversations'. [17]

Instagram's encryption architecture also includes device authentication and secure session management to improve communication security. Features like device verification, disappearing messages, and encrypted chat backups are part of the system to boost privacy protection. Furthermore, modern encryption systems use forward secrecy. Temporary session keys are created for each communication session so that the compromise of one key does not expose previous conversations.

Despite the protection of message content, some Metadata may still be accessible to the platform. Metadata can include details like the identities of users, timestamps, device information, IP addresses, and how often users communicate. Because of this, even though message content is encrypted, communication patterns may still be visible for operational or

[16] Aman Gupta, "Meta quietly removes end-to-end encryption from Instagram: What does it mean for your private DMs?", available on <https://www.livemint.com/technology/tech-news/Meta-quietly-removes-end-to-end-encryption-from-Instagram-what-does-it-mean-for-your-private-dms-11778379795263.html> (last visited on 19th May 2026)

[17] Annie Badman, Matthew Kosinski, "What is asymmetric encryption?", available on <https://www.ibm.com/think/topics/asymmetric-encryption> (last visited on 19th May 2026)

regulatory reasons.

The encryption system used by Meta Platforms shows an effort to find a balance between user privacy and the needs of platform governance and cybersecurity. However, the introduction of end-to-end encryption (E2EEE) has sparked important legal and regulatory discussions. These debates focus on traceability, criminal investigations, child safety, and government access to digital communications. In 2026, Meta announced it would remove E2EE for Instagram direct messages due to regulatory pressures and safety concerns. This move further fueled global conversations about the balance between digital privacy and lawful surveillance.

Illusion of Privacy

Not all encryption is developed equally. The encryption that is marketed to protect its users from unnecessary usage differs from the encryption that protects the makers, businessmen, middlemen who swear to never peek into the files of citizens. This is a major showcase of how the encryption protection to its users is a security measure developed to protect when the data is idle. But it isn't built to necessarily protect the data from the people who run the system itself. When users log on to social media apps, they voluntarily agree to the platform policies and terms of service, but this consent is often given through the standard-form digital contracts in which the bargaining power is highly imbalanced. This raises similar issues as under the Indian Contract Act, 1872, of free consent, informed agreement and validity of obligations arising from contractual relationships of unequal status.[18]

The infamous Cambridge Analytica Scandal[19] back in the 2010's where the data of millions of Facebook users was collected by a British Consulting firm without the user consent for political advertising which was used to analytically assist the 2016 Presidential campaigns of Donald Trump and Ted Cruz. In response to this, Zuckerberg apologised for the breach of trust and pledged to make changes in the policies to prevent further breaches. The public reacted to this by initiating hashtag trends such as "#DeleteFacebook" and "#OwnYourData" to show their frustration to an issue as big as breaching their trust to which Facebook did not provide a proper response or compensation.

[18] THE INDIAN CONTRACT ACT, 1872, s.14, s.16, s.19
[19] Ikhlaq ur Rehman, Library Philosophy and Practice (e-journal), "Facebook-Cambridge Analytica data harvesting: What you need to know" (2019)

The concept of managed encryption in itself is purely a puppet string mechanism. A euphemism that quite literally hands control of user data to the developers, even if the same is not acquired directly by manipulating the statistics and getting a hand on the plain text, it may be done based on the digital footprint based on what they like, what group they involve themselves in, etc. From this myriad of data points, the wealth of information that is gained makes it very easy for the developers of the encryption to get their hands on the final communication text.

In Rutledge v. Facebook, Inc.[20] The plaintiffs claimed that Facebook used social plugins and web cookies up until 2011 to track users while logged out, going as far as to gather information related to the user's browsing history. Facebook's response to this was to deny all claims and when the case was further pushed into a full trial, Zuckerberg agreed to settle it for a couple million dollars.

In 2016, under the Campbell v. Facebook, Inc case[21], the plaintiff filed a lawsuit against Facebook for allegedly scanning messages that were deemed to be private for marketing purposes which were outright violating the federal privacy laws. Facebook's response to this was that multiple messages were scanned at once and the URL data was anonymous and only used in combined form.

E2EE is regarded as critical for protecting freedom of speech as it is 'under unprecedented strain' and it was reported that an approximate crowd of users were from countries where people had been imprisoned for posting online content on grievous matters. In 2018, the UN special rapporteur on freedom of expression suggested that companies should provide E2EE, either by default or through an opt-in function, to fulfil their 'responsibility to safeguard freedom of expression'. [22]This is particularly important in the context of protecting vulnerable and marginalised groups, journalists and the free press from censorship by illiberal and authoritarian regimes. In such regimes, the right to privacy for journalists, activists and opposition politicians protects their life.

Meta evolution

While Meta is familiar amongst people in the modern day due to its growth with TikTok,

[20] Rutledge *v.* Facebook, Inc. (5:12-cv-00669)
[21] MATTHEW CAMPBELL v. Facebook INC. (13-cv-05996-PJH (MEJ))
[22] Office of the High Commissioner for Human Rights, Report on encryption, anonymity, and the human rights framework, A/HRC/29/32, May 22 2015

Instagram and WhatsApp, it started off primarily with Facebook back in 2004 by Mark Zuckerberg along with Eduardo Saverin, Andrew McCollum, Dustin Moskovitz, and Chris Hughes.[23] The website was initially something that was only exclusively available to Harvard students before being extended to other universities and finally to the general public.

As Facebook expanded globally, the company introduced features such as the 'Like' button, photo sharing systems, algorithm based suggestion structure, etc. These developments significantly increased the number of users that were involved in social networking. Simultaneously, the company entered the business market by providing targeted advertisements, user interaction modules, behavioral analytics, and so on.

Through various external investments, Zuckerberg acquired Instagram in 2012 for approximately one billion dollars and WhatsApp in 2014 which was particularly popularised for its inbuilt encryption technology.[24] Along the course of his business decisions, he further acquired various other networking systems.

In 2021, he officially made a shift from Facebook to Meta to signify 'Metaverse' meaning the company was going to reach limits above and beyond by taking it further from a social media corporation. The rebranding of Meta also came along with stricter privacy measures, where Zuckerberg encouraged people to sign up for end to end encryption to protect data from breach.

Today, Meta operates as one of the biggest corporations that manages the world's largest networking platforms taking it from a mere university level networking system to a wide scale industry.

Legal Perspective

- **Article 21**

Article 21 of the Indian Constitution provides that- "No person shall be deprived of his life or personal liberty except according to procedure established by law."[25] This huge bracket also

[23]Big 3 Media, "A Brief History of Meta and The Evolution of Facebook", available on < https://www.big3.sg/blog/a-brief-history-of-Meta-and-the-evolution-of-Facebook>
[24]Engineering at Meta, "Meta's Infrastructure Evolution and the Advent of AI ", available on <https://engineering.fb.com/2025/09/29/data-infrastructure/Metas-infrastructure-evolution-and-the-advent-of-ai/>
[25] The Constitution of India, art. 21

included the 'Right to Privacy' as according to the K.S. Puttuswamy v. Union of India[26] judgment from 2017. End-to-end encryption extends beyond cybersecurity concerns by entering into a broader domain of personal liberty. In the digital era, every individual expects their message to be protected from unauthorized intrusion by wanting their private communication to be encrypted. For a platform like Instagram, users expect to have private conversations that are protected by high security and not leaked anywhere. At the same time, the traceability measures taken by the State to ensure that there is no national security issue pertaining to private chats while also respecting the private digital spaces and not intruding is a major exception to Article 21.

This technology also reshapes the entire dynamic between citizens and digital intermediaries since encryption was traditionally used by the State and with the growing economy, private intermediaries were able to get their hands on the technology. Privately held companies like Instagram and WhatsApp, which are free social networking apps, serve as important infrastructures for democratic, public and interpersonal expressions and communications. When private companies themselves refuse encryption access to their platforms, it becomes hard for the State to exercise its investigative and surveillance powers since it becomes unable to access user communication.

However, solely because these restrictions limit the government from being unable to access information does not automatically make it a violation to democracy.

- **Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025**

As previously mentioned, the DPDP Act says that a data fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data. Moreover they have the duty to 'protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.'[27] After taking an objective look at Meta and its functioning, it is highly likely that rather than just being a data fiduciary it should be classified as a significant data fiduciary. The current qualifications for such a title include: (a) the volume and sensitivity of personal data processed; (b) risk to

[26] Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018, (2017) 10 SCC 1
[27] The Digital Personal Data Protection Rules (2025), Rule 6

the rights of Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; and (f) public order.[28] Though the official notification said that the list of such entities will be released 18 months later[29] (possibly 2027), the current impact of Instagram can be said to qualify all of these factors.

As such Meta would have to be held to a much higher standard for how they use user data and the protections they give to such users. In their official privacy policy and their policy on 'How Meta uses information for generative AI models and features'[30], they explicitly said Meta cannot read the private communications of users and as such they would not use that to train their AI models. However, once E2EEe is discontinued, there is no specific policy declaration that continues with their earlier position along with the technology being perfectly apt for it. Moreover, earlier, user information like location, content preferences, public interactions etc and from 2025 any communications with the Meta AI chatbot were used to target advertisements according to personal preferences, now there is no guarantee that private communications won't be another basis for personalising marketing tactics.

In 2023, Meta services Facebook and Instagram were together met with a €390 million fine after Ireland's data protection commission concluded that Meta's terms of service requiring users to accept personalized ads when signing up to the social media services violated EU rules.[31] In 2024, the Competition Commission of India (CCI) imposed a fine of INR 213.14 crore ($25 million) on them for unfair business practices with the WhatsApp Privacy Policy update implemented in January 2021 which had notified its users of the updated privacy policy which included an expanded scope of data collection and mandatory data sharing with all Meta Companies and Meta Company Products on a take-it-or-leave-it basis, removing the earlier opt-out option, similar to the complete takedown of E2EEe we see now.[32] The current law does not specify the limits of where information can be sourced from for personalised advertising and how far it can be taken. This leaves a regulatory gap between Meta's collection of personal communications, private details and to what extent that information can be used.

[28] The Digital Personal Data Protection Act, 2023, s. 10
[29] Press Information Bureau, Government of India, "DPDPD Rules, 2025 notified", available on <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf>
[30] Meta, Privacy Center, "How Meta uses information for generative AI models and features" (last visited on 23rd May 2026)
[31] Chris Vallance, BBC, "Meta fined €390m over use of data for targeted ads", 5 January 2023 (last visited on 22nd May 2026)
[32] Swathi Singh, IJLT Blog, "India's $25 Million Fine on Meta: Lessons in Competition and Privacy, 2025"

As per the DPDP rules 2025 section 3, the data fiduciary must provide the data principle with a proper account of details so that they can give their informed consent on how their data will be processed and so must receive (i) an itemised description of such personal data; and (ii) the specified purpose or purposes of, and specific description of the goods or services to be provided or users to be enabled by, such processing but this requirement does not come into effect until May 2027 further widening the regulatory gap within which Meta will be functioning.

Conclusion

When the regulatory mechanisms to protect against misuse of personal data are not yet fully in force, and a large quantum of the Indian population is left vulnerable to such offenses, a move such as removing end to end encryption by Meta can go largely unsupervised. Despite the pressing issue of combating the spread of illicit sexual abuse and online harassment material which may be addressed through this move, with the company and the government being able to access and scan the communications of millions of users, a Pandoras box will be opened. Movement of population can now be surveilled under the guise of checking for CSAM, terrorist activities etc. The next few years will reveal how the access to such information changes the way the government and third party groups respond to user content, whether it helps protect vulnerable children in the online spaces or it'll only fine tune the personalisation of commercial advertisements converting the only non commercial aspect of the internet, that is personal conversations, into another corporate marketing strategy. With the laws supposed to be controlling these actions still not in full effect, it is highly likely that more cases of data misuse will take place. As of now the only available safety mechanism is for users to refrain from putting all of their confidential information through such unsecure streams and exercise more digital prudence.