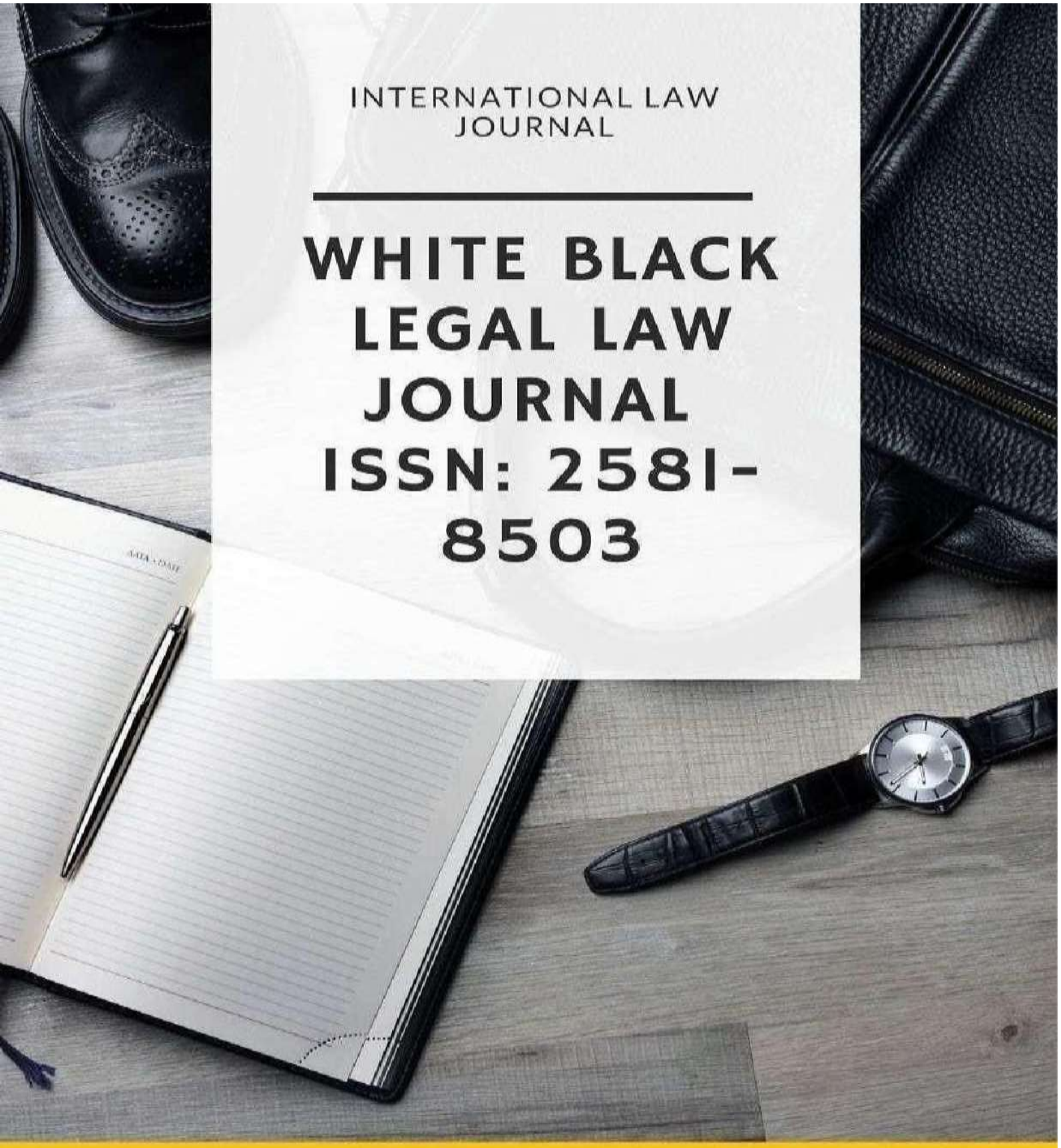

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | April 2025 ISSN: 2581-8503

PROTECTING PRIVACY IN THE AGE OF SOCIAL MEDIA: A LEGAL ANALYSIS OF USER RIGHTS AND CORPORATE RESPONSIBILITY

AUTHORED BY - PARI MISHRA & DR. AVANTIKA MADHESIYA

"The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."

— Supreme Court of India, Puttaswamy v. Union of India (2017)[1]

Abstract

The emergence of social media has profoundly altered communication and information exchange. Although the platforms provide many advantages, they also pose significant challenges to the protection of user privacy. Social media firms harvest, process, and profit from enormous amounts of personal data, frequently without users being fully aware of how their data is being utilized. Data breaches, unapproved data sharing, and coercive consent mechanisms have caused worldwide concern regarding privacy rights and corporate responsibility.

This research paper offers an in-depth legal examination of protection of privacy with respect to social media. It assesses current legal frameworks for regulating online privacy, company adherence to such rules, and the efficacy of consumer remedies in instances of privacy invasion. Through consideration of landmark legislation like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and India's Digital Personal Data Protection Act, this research evaluates how various jurisdictions are regulating social media privacy.

Overall, this study adds to the current debate on digital privacy by highlighting stronger legal protection, more business transparency, and user empowerment in handling personal data. The results reinforce the imperative for governments, corporations, and civil society organizations to work together in resolving privacy issues in the changing digital environment.

[1] https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time

Introduction

Social media platforms, especially Instagram, are an integral part of life in the modern world. People can share their experiences, interact with one another, and exhibit their creativity. However, such platforms require a lot of personal information which becomes a matter of concern regarding privacy breaches. Instagram poses serious privacy challenges through its immense data harvesting activities such as storing personal pictures, locations and user activities. Indian users are subjected to data misuse, stalking, and targeted profiling advertisements that invade their privacy.

Instagram came to master social media paradigms thus making it influential information for the youth. Thereby moulding teenagers and younger adults. With this comes the issue of privacy. Article 27 of the Indian Constitution fundamentally factors in the context of the right to privacy, and thereon lies the prerogative of every Indian citizen stated by the Supreme Court of India. On one side we have vocal advocates of social media platforms and on the other, defenders arguing that undue breach of privacy is forced in the name of the free speech and expression.

Regardless of configurational privacy settings employed, Instagram's multi-faceted policies and meticulous user monitoring seem to eliminate any user concern over the possible extent of information collected and disseminated. This research paper explains how Instagram's data practices violate users right to privacy concerning data collection, sharing and system profiling. This Instagram privacy case study attempts to analyse the unilateral approaches that Instagram has taken towards user privacy and the applicable regulation gaps in India which surround the collection and amalgamation of data, poses threats to user privacy and outline suggestions to strengthen user safeguards in the flux of social media.

The Role of Social Media:

As noted, social media has now integrated into the lifestyle of each and everyone in this modern era, which clearly affects us. Its influence is both positive and negative but one of the most appreciated positive impact is the information being readily available at no cost. Information van be deprived from any part of the world in seconds. Furthermore, we are also able interact with our friends and family who may be living far from any part of the world in seconds. Furthermore, we are also able to interact with our friends and family who may be living far

away from us. Moving on to the negative aspects, there's more than one. The most dangerous one is perhaps violation of the right to privacy, especially in regard to social media. Another one is cell phone addiction, increased stress levels. Nd poor mental health. Change in sleeping patterns, several sleep-related issues, and numerous psychological issues are all highly probable outcomes. Platforms such as Instagram greatly influence the creation of social privacy norms because of their inclination to soften between the public and private spheres. While these social media give people the means to connect and express themselves, the primary focus of these platforms is to advertise and capitalise on the user information which results in significant privacy threats. Features such as algorithmic personalization, geotagging of location, and live sharing encourage oversharing, tend to encourage posting sensitive information not knowing what cost they incur leaving users vulnerable to monitoring, profiling and abuse of data. But social media also has the potential to engender privacy awareness by virtue of transparency mechanisms. Balance requires robust legal frameworks, ethical platform design and high user empowerment to ensure that benefits of social media does not have any cost in terms of privacy rights.[2]

Right to Privacy

Recently, there was significant doubt regarding the limits of right to privacy under the Indian constitution. In India 2017 the nine-judge bench judgement of the Supreme Court in Justice K.S Puttaswamy v. Union of India held the privacy is the fundamental right and it is part of the right to life and personal liberty under Article 21. It cannot be absolute, and it may be restricted by the state provided it is consistent with "legality, need and proportionality of the protection this fundamental right". One needs to understand that privacy has to be safeguarded in the public space as well as in cyberspace. Smart electronic gadgets reduced price of internet access and connectivity across national, made the internet and social media sights immensely popular in India. Whereas social networking websites offer a gratis platform that has the potential to reach a huge number of people in very short time for self-expression, they also make one vulnerable to information of a personal kind. In certain cases, one is aware of the information that social media networking websites are gathering.

[2] **Legal Service India**. (n.d.). *The Right to Privacy in the Age of Social Media*. Retrieved from https://www.legalserviceindia.com/legal/article-18994-the-right-to-privacy-in-the-age-of-social-media.html

What is The Impact of Social Media on Privacy?

Privacy has been greatly affected by the rise of social media. Social media platforms like Facebook, Instagram, and Twitter encourage users to divulge personal details and information about themselves and their lives. As users share more personal information on social media, there is a greater increase in transparency and visibility, making it harder to separate private and public settings. Most users do not realize the full impact of privacy risks that come with sharing seemingly harmless information on social media platforms. User data is collected, analysed, and monetized by social media platforms. Increased privacy issues about how personal data may be weaponized or land in the wrong hands also exist. Additionally, greater internet connectivity on social media also opens users up to different cybersecurity threats. And with emerging technologies, the privacy discussion becomes more complex due to features like facial recognition and location tracking, especially within social media applications.

The concept of privacy has changed due to the rise of social media. While social media platforms allow for self-disclosure and connectivity with others online, they also present dangers associated with profiling, micro-targeted advertising, and surveillance via social media applications. Also, social media users need additional education to empower them to make better-informed decisions about privacy on social media. Social media sites also have a duty to be transparent and give users more agency over their data in social media. Finding the right balance between transparency and privacy is important as social media becomes further integrated into everyday life.

The Right to Privacy in the Digital Age:

The right to privacy is one of the principle human rights recognized in the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17). However, in this age of information, social media platforms joyfully disregard the individual right to privacy. A case in point is Instagram, operated by Meta (formerly Facebook), which collects vast amounts of personal information about users for targeted advertising and to improve user experience. Information Collection on Social Media Social media sharing platforms utilize multiple techniques to collect information such as build large-scale profiles on individuals. Understanding how information is collected on social networking sites such as Facebook and Instagram are necessary to evaluate the implications of privacy. It can be said that at the heart of the social media platform, they merely collect

personal user data at the time of registering accounts. In this data collection, the platforms request some of the following information: full name, email address, phone number, location, date of birth, and more. Most platforms will also ask the user to verify email or phone number before completing the account settings. [3]

In addition to self-reported information, a great deal of information is collected indirectly from users engaged in their online behaviours. Web tracking technologies such as cookies, pixels, and APIs track user actions, such as whose posts are liked, what content is shared or engaged with, pages viewed, and search history patterns. These behaviours can help identify user interests, beliefs, identity markers, and daily habits. Social media applications also exploit the sensor capabilities of smartphones, as well as the calendar, contacts list, and metadata, to gain insight into patterns of usage. In addition, complex social graphs can be built from the connections and actions between users. A user's activity within their network adds even more points of data to profiling. Comments, tags, or messages can provide an unintentional view of and insight into relationships, preferences, and offline connection to others. In addition, facial recognition algorithms operating within photos and videos supplement data collection. Some of the data is volunteered to users, even though users may not perceive these as volitional. For example, when users voluntarily upload contacts to search for friends; share location; answer questions about personality; log-in third-party applications with a social media login; or grant access to other linked devices or applications, the data collection tends to go beyond user imagination.

Even though the data practices on various platforms differ substantially, the amount of user data being harvested is vast and increasing. There are not comprehensive laws governing the harvesting of social media data by corporate platforms. Self-regulation and consent systems have proven to be ineffective from a privacy perspective. Critics have argued that excessive and unclear data mining on social media violates user privacy and leads to overreach. In contrast, the companies maintain that data powers personalized experiences and makes their platforms safe. Users need to be more aware of the various ways social networking platforms collect their personal information. Privacy controls provide some control over sharing options, but behind-the-scenes observation is ubiquitous. Stricter regulation of user data, improved consent flows, and "privacy by design" models have been proposed to re-establish the power

[3] **IEEE Digital Privacy**. (n.d.). *Privacy Risks and Social Media*. Retrieved from https://digitalprivacy.ieee.org/publications/topics/privacy-risks-and-social-media

balance between users and the platforms providing social media services. There will need to be sound risk-benefit analyses about data collection by social media services in the future.

How Instagram Violates Privacy:

Methods of Data Collection - Instagram collects all types of information from its users, namely location and browsing data, personal data and, through filters, even biometric data. Some of which is required to provide certain functionality. But Instagram's practices, taken broadly, far exceed this for its services. Users unknowingly agree to those dense legalese terms and conditions. Targeted Advertising - The main source of income from Instagram is advertisements generated by data analytics. Complex algorithms that the site applies create interactive, in-depth profiles derived from the user behaviours, preferences and interactions on the web, making Instagram's profile intrusive to the user's privacy whilst enabling targeted advertising and surveillance exercises. Insufficient data protection systems - Instagram has had substantial security, but it has also been hacked multiple times. Most prominently in 2019 when there was a significant leak of millions of users' personal data which brings into question Instagram's ability to protect its users.

Third-Party Data Access - Users also are quite concerned that data used by Instagram is not stored by third parties to the same level of protection as Instagram offers. This once again exploits the user's data. Privacy and privacy policies have been a big issue lately in social media. The main privacy issues on sites like Facebook and Twitter are data mining, ad targeting, user tracking, and data breaches. When using social media, users are asked to provide personal information, such as name, email address, date of birth, interests, location, and more. The information is stored and later used for various purposes. Companies build and enhance user profiles based on online actions and activity. Every action taken and post made on social media are examined with a goal of understanding what users are interested in and what they are doing.

Social media companies often utilize these types of personal information for targeted marketing purposes. Knowing someone's preferences, location, and identity is a way to get remarkably personalized advertisements in front of them. Users often agree to this in very lengthy terms of service documents without fully understanding how that information is going to be used. In addition to the marketing use of user information, it can also be passed along from marketers to the government without the social media user's knowledge or consent. These practices create

obvious risks to the user's right to privacy. Any data collection of personal information contains a risk of the personal data being disclosed without consent, or more severely, having it hacked. Data breaches of social media or their platform could disclose information to cybercriminals and potentially lead to identity theft, fraud, or other unlawful gains. Users are also subject to mass surveillance, monitoring of sensitive data, profiling, and discrimination.

For many years, privacy advocates have protested against the open data collection and monitoring practices of social media giants. Public awareness of social media privacy and distrust of such services have grown dramatically. Nowadays, individuals worry about their data being breached or mismanaged without their knowledge. Many people even want more transparency about data processing, and more control over their own privacy. However, social media applications have not made sufficient progress to reduce the threat to privacy and give users more rights.

User Actions and Privacy:

Instagram policies are mainly responsible for privacy breaches, but user actions are also a prime ingredient. Many users exercise autonomy over their identity, and provide sensitive information, such as real-time locations or happy moments, without regard to privacy. A purely operational culture that encourages users to share, and the user's own desire to share, mar and threaten privacy even more.

Legal and Ethical Implications:

Legal principles of privacy hold par with the advancement of technology. Some countries have modified rules of privacy for advancement in user privacy, such as the European Union with GDPR; other aspects of privacy within other nations are not well developed or detailed in their laws. Thus, Instagram may operate comparatively unreasonable in a nation with less than sound privacy rules. Ethically, from the angle of corporate responsibility, Instagram's actions provide ethical questions. Investing the individual's right to privacy is a move; and profit over that right dilutes trust down the line and promotes a surveillance culture. Current Laws in India regarding Privacy and their Shortcomings:

Although the privacy law has developed in India, the legal system still struggles to keep up with the increasingly complex reality of the electronic age. The Information Technology Act, 2002, informs and directs India's approach toward electronic commerce. Section 43A

establishes liability for corporations where it is alleged that their services are not used to[4]

safeguard sensitive personal data; Section 72A establishes liability for unauthorized disposition of information. These provisions are generally restricted in their scope and application, and it appears that they pertain only to corporate negligence. There seems to always be space in this statute to modify the law to prevent any current malfeasance, such as algorithmic profiling or mass surveillance, for instance, to name some. The act hardly even governs the behaviours of social networking sites like Instagram, where the gathering or commodification of personal data occurs with no oversight.

A significant shift occurred with the trailblazing acknowledgment of the right to privacy under Article 21 of India's constitution. The Supreme Court's ruling in 2017 from Justice K.S. Puttaswamy v. Union of India underlined that the right to privacy is integral to human dignity and autonomy. Although the decision was a strong antecedent to privacy as a constitutional right, it was not readily invoked in the legal ecosystem as an enforceable right. Even though some of the problems dealing with privacy can be brought about by social media operators, most of these issues remain in a state of legal ambiguity, and clash with the digital landscape, thereby creating no express statutory directive for the persons who are ostensibly being exploited under the "privacy" provision. The Bhartiya Nyaya Sanhita, 2023, repeals the IPC, and brings together new provisions to address offences related to privacy and troll-counting related offences from July 1, 2024. The areas which specifically relate to social media misconduct are:

Section 354D - addresses the issue of stalking, including cyber stalking by penalizing the act of routinely sweeping or contacting a person without their consent, hence acknowledging online abuse.

Sections 499 and 500 pertain to defamation. These sections provide legal protection arising from the act of publishing a defamatory statement or the act of falsely stating something defamatory about someone that harms their reputation. Sections 509, the above sections dealt with conduct intended to outrage the modesty of a woman, which includes online harassment or abuse, or obscene gestures or remarks via any social media application. The Provisions in

[4] **ResearchGate**. (n.d.). *Privacy Laws in the Age of Social Media: A Communication Analysis*. Retrieved from https://www.researchgate.net/publication/389513030_Privacy_Laws_in_the_Age_of_Social_Media_A_Communication_Analysis

BNS, 2023, relate to strengthening the legal mechanisms against cyber abuse and accountability in online engagement. In response, India of passed its first meaningful and comprehensive data protection law, in the form of the Digital Personal Data Protection Act, 2023 (DPDPA). The law mandates explicit consent for the processing of personal data, a right of access, rectification, and erasure, and imposes liability for data breaches. It also includes penalties for violations. Yet the act has several drawbacks, in that it provides broad exemptions to government agencies under the guise of national security or public order, introducing uncertainties around surveillance without regulation. In addition, it contains ambiguous laws around cross border data transfer and an ineffective enforcement mechanism, which significantly undermine the legislation's effectiveness regarding privacy protection.

The deficiencies of the existing law must be addressed and the privacy rights of citizens should be protected through clear reforms. The entire data protection regime in India must attain the reformative level as per the DPDPA. Data protection law must offer stronger rights for the user, e.g., the portability rights and forget-me-not rights. These laws would enable greater control for the users over their data, especially on Instagram, which collects data on a large scale. In addition, government exemptions under the guise of national security must be reduced with adequate checks and balances to eliminate any misuse. Another important step for privacy is the regulation of social networking sites. Sites like Instagram should be made to explain how their algorithms use and process users' data, as well as the algorithm they apply to rank users' data. Transparency of how the data is shared with third parties, especially advertisers, must be made obligatory so no misuse or unauthorized handling of the individual's personal data exists. Legislation can be another means to hold accountable and punish heavily all those who deviate.

Children and other vulnerable populations would receive the same protection as a compellingly privacy-focused legal framework. Therefore, the rules should contain requirements that make it illegal for a company to collect personally identifiable information about minors without prior consent from a parent or guardian. All personally identifiable information about children must be collected, stored, processed, and shared at the most robust security levels. The vulnerable communities that are subjected to profiling and discrimination must receive worthy specialized protections from abuses of their personally identifiable information. The reform must also address the systemic nature of digital platforms. When privacy-aware design principles are integrated, users' data is better safeguarded during the life-cycle of a product. Features like transparent privacy settings, user-friendly data anonymization, and collect only

the minimal data by default can greatly enhance user privacy. These practices must be required of social media firms and industry practices.

Social Engineering and Privacy

Social engineering is a different social media privacy and social engineering risk. The method plays into the human tendency to reduce defences and share decisions that may then be intentionally misused. Being cautious is the best defines against social engineering. Social engineering exploits personality traits such as curiosity, a sense of obligation to help others, desire for reward, and worry about violating social norms. Social media contexts exacerbate those vulnerabilities because users are introducing an informal participation with large groups of people. Some of the social engineering tactics you should be aware of are phishing, impersonation, grooming, catfishing, spreading disinformation, multi-step attacks, and others. The goal is to elicit information, money, access, or compliance from unsuspecting users. For example, the most common scheme is a spoof account pretending to be some authority figure or friend to get the person to share their login information or to send someone money. Baiting curiosity uses status updates that are clickbait, thus encouraging someone to click on malware links. Spreading rumours and lying socially engineer thought and behaviour.

Multi-faceted tactics incorporate strategies like first befriending a targeted "victim" through a made-up persona, then creating an emergency to call upon urgent aid for exploitation. Online personal data assists these tactics in gathering plausible background information and identifying victims. Direct connection and peer-to-peer sharing on social media provides an acquired trust perspective. However, the limited cues available during online interaction allow impersonation and ploy to take place more readily than in person. Users must therefore utilize a more conscious determination of credibility. Education about to be on the lookout for common tricks such as impersonating an authority channel, creating urgency, or garnering interest through curiosity/greed serves to reduce user susceptibility. Source fact-checking information offerings and link prior to sharing content acts to counteract misinformation/evidence. Controlling the privacy settings of posts/messages takes thoughtfully collected, private information off the data collecting table for others. Critical [5]thinking and verification processes also support validation of the credibility of requests when strange

[5] **The Digital Speaker**. (n.d.). *Privacy in the Age of AI: Risks, Challenges and Solutions*. Retrieved from https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/

activity is needed to exchange finances, or hiring use of data. Verifying from a questionable source through another channel of contact is always wise. Although individual accountability must take place, social media sites must also develop the means to actively seek out and disable fake accounts. Developing an internal identity verification examination process and deploying AI notification's to documented suspicious activity with a data collection purpose could also be possible.

Social engineering leverages the natural proclivities of human beings towards deceit and avarice. As social media continues to permeate vast corners of life, both individuals and organizations need improved levels of literacy to mitigate risks associated with smart manipulation. Requires vigilance and critical analysis. Overview of Privacy Legislation An extensive collection of privacy-related data protection laws has been enacted around the world that impact a myriad of social media activities. This paper presents an overview of the prominent laws and their focus, then draws attention to distinction in country-based laws and finally concludes by discussing the issue (and corresponding gaps) of enforcing legislation - through compliance-based and often consent-driven measures. The European Union General Data Protection Regulation was enacted in May 2018, followed shortly by the USA California Consumer Privacy Act in January 2020, complicating access to and provision of digital services for European and USA consumers. Organizations providing services to EU citizens, regardless of their base of operation, have been expected to conform to the GDPR's expansive data protection strategy, raising the profile of the EU and Ireland as locations for privacy activism, as well as a site for regulation. There are important disparities among data protection statutes worldwide in terms of scope, substantive and procedural rights. For example, major differences between the GDPR and CCPA pertain to access, correction, erasure, portability and restrictions, opt-out directions and duration, and fines. As global data-sharing practices exist, there are calls worldwide for interoperability among privacy regimes in all jurisdictions and dynamic and changing legal changes. Yet this is an often balanced against lobbying by industry and pushback from influencers. The European Data Act, however, is considerate of current calls. Many scholars claim that users that consent to data-sharing, collection, and use are neither informed, free, nor power-balanced, which constrains user agency and also reinforces the case for corporate social responsibility.

Implications and Challenges

What do the privacy laws imply for social media, particularly based on user expectations and the medium itself? Communications unrestricted and unregulated in a global medium are still constrained and shaped by nation-state interests and values. But the proposal of regulation involves a number of challenges, including formulating and enforcing rules regarding the behaviour of platforms, intermediaries, providers, regulators, and industry members on one side and audience members on the other. At first glance, the absence of those kinds of regulations could be attributed to a lack of international cooperation and a counter-force that regulation inevitably faces from faster-than-regulation technology. In addition, with the institutions that are supposed to be regulating the system, a cluster of issues around the enforcement of laws and the degree of compliance and trust in the law has only recently come to be better understood. Privacy legislation also looks likely to produce a higher degree of distrust and a lower level of use, as users bring about a behaviour change that defends and protects themselves from the regulations.

Privacy Issues in the Era of AI

The advanced technology behind AI creates a threat to individual and organisational privacy. In fact, increasingly sophisticated algorithms in AI systems can make decisions based on subtle data patterns that we find difficult to detect ourselves. This means that an individual may not even realise that their private data is being used to inform a decision about them.

The Risk of Erosion of Privacy

While AI technologies possess a lot of potential advantages, they also carry several significant risks. A primary risk to individuals is the potential for AI to be used to infringe on privacy. AI systems require massive amounts of (personal) data, and if that data is contained in the hands of anyone with malicious intent, it could be used for purposes such as identity theft or cyberbullying.

The Problem of Bias and Discrimination

Another problem that AI technology raises has to do with the possibility of bias and discrimination. AI systems are only as bias-free as the data on which they are trained, so if the data used to train a system has a bias, the AI system will too. This can lead to discriminatory outcomes for people based on attributes like race, ethnicity, gender, and socioeconomic status.

It is very important for people to assess whether AI systems are trained on data that reflects diversity, and to regularly monitor AI systems for bias after they have been deployed. At first glance, bias and discrimination in AI systems may not seem to have a direct link to privacy. And for good reason, because generally privacy is seen as a tangential consideration to the protection of personal data, and the idea of an individual's right to be left alone. However, in fact, the two issues are intimately related, and here is why.

First off, it should be noted that routine AI systems derive their decisions from data, which could come from anywhere, including online behaviour, social media, or public records. Even if the data appears innocuous initially, it can reveal an extensive amount of insight about an individual, such as their political views, religion, gender, and race. So, when an AI system tends to be biased or discriminatory, it can use this knowledge to further bias itself and create unjust or damaging outcomes for individuals. As an example, envision an AI system that is being used by a hiring organization to screen applications for open job positions. If that AI system is biased against women, or against people of colour, it can use a candidate's gender or race to invalidate their consideration, unfairly. This not only harms the particular applicant but also strengthens structural inequalities in the workforce.

Inherent Privacy Concerns in the Era of AI

Privacy in the age of AI is a complex problem. All the data collected and analysed by businesses and governments has put individuals' private data at risk like never before. Examples of these problems include invasive surveillance which undermines personal autonomy and oversensitive balances in power, and unconsented collection of data which can put people in cyber danger when their sensitive personal data is disclosed. Big tech lends to these issues as they have huge amounts of data at their disposal and they are professional at collecting, researching, and evolving their use of that data.[6]

Use and Collection of Data by AI Technologies

One of the major effects of technology involving AI is the way that data is collected and used. AI systems are designed to learn and improve by processing massive amounts of data. Therefore, the amount of personal data that AI systems collect is growing, and issues related

[6] IBM. (2024). *Exploring privacy issues in the age of AI*. Retrieved from https://www.ibm.com/think/insights/ai-privacy

to privacy and data protection are being raised. We only need to think of the variety of generative AI tools, from ChatGPT to Stable Diffusion and other tools in development, to see how our information (articles, images, videos, etc.) is being used, often without consent. Most importantly, the use of personal data by AI systems is not transparent. Ai system algorithms can be complex, and individuals may have difficulty recognizing how their data is used to inform decisions that affect them. Non-transparency may create mistrust for AI systems and uneasiness.

To mitigate these issues, it is imperative that organisations and businesses applying AI technology take proactive action to help assure people's privacy. This is likely to include establishing strong data security protocols, ensuring that data is used for the reasons it was collected and developing AI technologies that are ethical. Furthermore, there must be transparency in AI systems "use" of personal data. Individuals must be able to see how companies use their data and have the ability to control whether their data is being used. This constitutes the right to opt-in or opt-out of data being collected and a right to request their data to be deleted. By following this approach, we can achieve a future where AI technologies are able to enrich society while providing protections for individuals related to privacy and data security.

AI Privacy Issues: Practical Examples

In the era of AI, personal information is garnering increasing value for businesses and organizations, being applied in ways that may have been previously unthinkable. From facial recognition, to predictive algorithms, AI is used to collect, process, and analyse our personal data, often without our awareness or consent. For instance, the growth of generative AI such as text/image generation software has become increasingly common over the last few years. Generative AI allows users to create content that imitates media created by humans. However, the use of generative AI raises important privacy considerations because the companies that make these products may collect and analyse the information users input to generate media.

CASE 1. Google's Location Tracking

In recent years, Google has faced criticism over its location-tracking policies due to privacy concerns. Google keeps a record of its users' locations, even when users have not explicitly consented to provide their locations, and this issue bubbled up to the surface in 2018 when the

Associated Press reported that Google services continued to store location data even when users expressly turned off location tracking. This raised serious concerns about user privacy and trust and Google quickly became the target of criticism from users and privacy advocates alike. Since 2018, Google has changed its location-tracking policies and increased transparency regarding how it collects and uses location data. However, lingering questions remain regarding the scope of the data collected, how the data is used, and who has access to it. Google's activities, as one of the major tech companies in the world, are consequential for individuals and society at large.

CASE 2. AI-Powered Recommendations: My Personal Experience with Google's Suggestion Engine

One example of privacy issues in the AI age is the invasive action of Big Tech companies. Not too long ago, I posted about a personal experience I had when I watched a show on Amazon Prime on my Apple TV. Two days after finishing the show, I received news suggestions about the show on a Google app on an iPhone, and I never watched the show on my iPhone. Alarming behaviour that makes one ask: does Google have full access to everything we do on our apps and what we do? I have worked with large data for over a decade, so I know that it is technically possible, but I'm concerned it is allowed! For the recommendation to be this personalized, Google would have to access data regarding applications running on the iPad (despite the privacy setting I have enabled to avoid this) or [7]listen in to my conversation by accessing the microphone on my iPhone or iPad and transmitting that information to my Google account. Both are violations, and both raise a flag that giants in instance storage are violating privacy.

CASE 3. The Use of AI in Law Enforcement

One instance of AI utilization in law enforcement is through the employment of predictive policing software. The software uses data analysis and machine learning algorithms to predict where crime might occur and who might commit it. While the concept seems promising, the technology has been criticized for exacerbating biases and sustaining prejudices. For example, some predictive policing systems have identified and pinpointed categories of minority populations, subsequently triggering allegations of racial profiling and discrimination. Facial recognition technology represents another application of AI in policing. Facial recognition

[7] Stanford University Institute for Human-Centered Artificial Intelligence. (2024). *Privacy in an AI Era: How Do We Protect Our Personal Information?*. Retrieved from https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information

technology uses algorithms to match photographs of faces to a database of previously identified individuals, and to enable law enforcement to track and identify individuals in real time. While facial recognition can be beneficial in assisting law enforcement in solving crimes, it raises the need to consider privacy and civil liberties. Facial recognition systems have misidentified individuals, resulting in wrongful arrests and erroneous accusations, in certain circumstances. With the implementation of artificial intelligence in law enforcement, there is a risk that these tools may contribute to and possibly deepen existing social biases and injustices. In addition, these artificial intelligence approaches in law enforcement raise the concern of transparency and accountability. It is difficult to understand how these systems work and make decisions, so it remains necessary to establish regulations and oversight to ensure their implementation is transparent, ethical, and protects human rights and freedoms.

Solutions to Overcome These Challenges

As we continue to embrace AI in various facets of our lives, it is clear that privacy and ethics are issues that are being recognized with increasing urgency. The opportunities for AI are great, but so are the concerns surrounding its use. As humankind, we must proactively respond to these concerns for the sake of individual privacy and to ensure AI's use is ethical and responsible. Organizations and businesses who use AI need to prioritize privacy and ethical consideration in their AI systems' builds and deployments. This means being transparent about what data is being collected and how it is being used, safeguarding data, continuously auditing for bias and discrimination, and constructing AI systems that are inspired by ethical principles. When businesses do this, they are more likely to build trust among customers, avoid reputational harm, and grow quality stakeholder relationships. As AI continues to evolve and disrupt the world, it is critical not to lose sight of the value of privacy and ethics. By emphasizing privacy and shooting for better information and data-protecting practices, we can use and evolve AI technology more responsibly with respect to privacy and other ethics issues with data.

Privacy is a critical human right, and as artificial intelligence technologies advance, it is imperative that we acknowledge the importance of privacy and protection of individual rights associated with privacy. This will require a multi-faceted effort involving all levels of government, organizations, and individual members of society. Governments must pass legislation to ensure AI is built and deployed with respect for individual privacy and other

ethical concerns. Organizations must value privacy as a core value and develop strong personal data protection strategies that show respect for individual privacy. Finally, individuals must be protected to have transparency and choice as it relates to ownership and access to their data. By valuing privacy and applying a strong regulation for the protection of data, we can foster AI's development and implementation in a way that effectively respects personal privacy. In this way, we will hopefully arrive at a world where individuals can realize the benefits of AI's endless capabilities without losing their inherent and natural human right to privacy.

CONCLUSION

In the age of social media, privacy is a complex issue, especially for sites like Instagram which invite contributions from users and personal data inputs. While India's emerging legislative framework, including the Digital Personal Data Protection Act (2023) and the Bhartiya Nyaya Sanhita (2023), suggests attention to privacy and privacy protection, it is important to navigate the complexities of the digital ecosystem in a balanced approach. Importantly, current frameworks struggle to keep pace with rapid technological advances, and legislative lag is prevalent. Even though the judiciary has embraced privacy as a fundamental right, the implementation mechanisms cannot keep up with the issues around cross-border data flows, algorithmic bias, and the extent of personal sensitivity to monetizing data.

Moreover, there exists the possibility of redressal solutions, such as the intermediary guidelines, good motives notwithstanding, with the potential to overstep their boundaries and trample upon freedoms, such as expression and dissent. On the other hand, while social media services have committed to privacy-protecting measures, as evidenced by continuous data breaches and obfuscation of their algorithms, they remain profit-driven. This clearly shows the limitations of legal protections alone, without systemic reform in corporate accountability.

The alternative way forward would acknowledge and attempt to balance the individual's rights with technological progress. This means the introduction of tougher laws, educating the public on their digital rights, and pushing for international agreement on the regulation of cross-border platforms. Otherwise, privacy will continue to be a feature that remains an aspiration, outdone by the commercial considerations of the digital economy. The protection of privacy in the artificial intelligence era represents a matter that affects the individual and society as a whole. We need an integrated response to this issue with both technical and regulatory approaches.

Decentralised AI technologies represent a promising route forward by providing secure, accessible, and transparent AI services and algorithms. By adopting such platforms, we will mitigate the risks of centralisation, but also promote greater democratisation and access to AI solutions.