



The Right to Privacy and Digital Surveillance in the Age of Technological Advancements

Prof. (Dr.) S.P.S.Shekhawat¹, Mr.AbhishekBishnoi², Ms.Bhawana³

¹Head & Dean, Faculty of law, JaganNath University, Jaipur, drspsshekhawat@gmail.com ²Assistant Professor, Faculty of law, JaganNath University, Jaipur, abhi29bishnoi@gmail.com ³Research Scholar, Faculty of law, JaganNath University, Jaipur, bhawanasattawat@gmail.com

Abstract: The primary objective of this research is to shed light on the multifaceted dynamics between privacy rights and digital surveillance in the current technological landscape. By tracing the historical development of privacy rights, the article establishes a foundation for comprehending the significance and evolution of privacy in the digital age. It critically evaluates the far-reaching consequences of digital surveillance on individuals' privacy, such as the erosion of personal autonomy, the commodification of personal data, and the potential for discrimination and misuse of power.

This research article delves into the complex legal framework governing privacy protection in the context of digital surveillance. It thoroughly examines relevant laws, regulations, and judicial decisions that delineate the boundaries of privacy rights and the permissible extent of surveillance activities. Special attention is given to emerging technologies like facial recognition, biometric data collection, and mass surveillance programs, highlighting the legal challenges they pose. The article aims to provide a comprehensive and nuanced perspective on the interplay between digital surveillance and privacy protections, equipping policymakers, legal practitioners, and the public with vital insights to navigate the complexities of privacy protection in an increasingly digitized society.

Ethical considerations play a vital role in the discourse on digital surveillance, and this article explores the ethical implications and dilemmas associated with the practice. It examines questions of consent, transparency, accountability, and the appropriate balance between privacy and security. The article emphasizes the need for ethical guidelines and frameworks to govern the responsible and ethical use of surveillance technologies.

By synthesizing insights from various sources, this research article contributes to the existing knowledge on privacy rights and digital surveillance. The findings will inform policymakers, legal practitioners, and individuals, fostering a deeper understanding of the complex dynamics at play and facilitating informed discussions on how to strike a balance between privacy concerns and the benefits offered by technological advancements.

Keywords: Privacy rights, Digital surveillance, Technological advancements, Implications, Legal framework.

Copyright © JURJ http://jagannathuniversity.org/jurj





Volume No.-IV, Issue No.-II, November, 2023, ISSN: 2582-6263

1. INTRODUCTION

The right to privacy, a fundamental human right acknowledged by international conventions and national constitutions, entails the individual's control over their personal information and activities, safeguarding them from unwanted intrusion or surveillance. Nevertheless, the rapid of digital technologies advancement dramatically altered the privacy landscape, presenting unprecedented challenges.

The pervasive growth of technology has significantly expanded surveillance capabilities, posing new threats to individuals' privacy.

The rapid development and widespread adoption of digital technologies have revolutionized various aspects of modern life. These technologies, such as smartphones, social media platforms, and Internet of Things (IoT) devices, have become an integral daily routines, enabling communication, convenient services, and access to a vast amount of information. However, this increasing interconnectedness has also exposed individuals to heightened surveillance risks.

Governments, corporations, and other entities have embraced digital surveillance as a means to monitor, track, and collect data on individuals. Surveillance practices include the interception of communication, monitoring of online activities, use of biometric technologies, and the proliferation of closed-circuit television (CCTV) cameras. While these surveillance measures are often justified on grounds of national security, crime prevention, or improving service delivery, they raise significant concerns regarding privacy infringement, civil liberties, and the potential for abuse.

2. EVOLUTION OF PRIVACY RIGHTS

2.1. Historical Development

The historical lineage of privacy in Indian society can be traced back to its cultural, religious, and philosophical traditions. In ancient India, the concept of "Antahkaran" encompassed notions of personal autonomy and the inner self, valuing privacy as a crucial aspect of individual dignity and personal space.

With the establishment of modern legal frameworks, the recognition of privacy as a legal right in India became more pronounced. The Indian Constitution, promulgated in 1950, guarantees

certain fundamental rights, including the right to privacy. Although the term "privacy" is not explicitly mentioned in the Constitution, the Supreme Court of India has acknowledged privacy as an integral part of various fundamental rights, such as the right to life and personal liberty enshrined under Article 21.4

Over time, the judicial interpretation of the right to privacy in India has evolved, adapting to societal changes and emerging challenges. Notably, in the landmark case of Kharak Singh v. State of Uttar Pradesh (1963)³, the Supreme Court acknowledged the right to privacy as an inherent aspect of the right to personal liberty. Subsequently, in the landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)⁶, the Supreme Court of India has firmly established the fundamental right to privacy as constitutionally protected, recognizing its significance in upholding human dignity and personal autonomy.

2.2. The Digital Age

In the digital age, privacy in India encounters new dimensions and complexities. The pervasive use of digital technologies, such as smartphones, social media platforms, and e-commerce, has resulted in the generation and collection of extensive volumes of personal data. Indian citizens actively participate in digital services, willingly sharing personal information and relying on technology for various facets of their lives. As a consequence, the protection of privacy becomes a critical concern, necessitating robust measures to safeguard individuals' personal data in the digital realm.

Digital surveillance practices in India raise concerns about the erosion of privacy. Government surveillance programs, such as the Central Monitoring System (CMS)⁷ and the National (NATGRID)⁸, Grid Intelligence have established to enhance national security and prevent criminal activities. However, the scope and extent of these surveillance programs have prompted debates about the proportionality and necessity of

Copyright © JURJ

⁴Indian Constitution, 1950.

⁵Kharak Singh v. State of Uttar Pradesh, 1963 AIR 1295.

⁶Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

⁷Central Monitoring System (CMS), Ministry of Home Affairs, Government of India.

⁸National Intelligence Grid (NATGRID), Ministry of Home Affairs, Government of India. 6



such measures, especially in relation to privacy rights.

Furthermore, private companies and technology platforms engage in the collection and processing of personal data for various purposes, such as targeted advertising and user profiling. The occurrence of data breaches and unauthorized sharing of personal information has highlighted the pressing need for robust data protection measures and legal safeguards to ensure individuals' privacy is adequately preserved.

In India, the legal framework for privacy Information encompasses the Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These rules govern the collection, storage, and transfer of sensitive personal data by organizations. Additionally, the Personal Data Protection Bill, 2019, is currently under consideration and seeks to provide comprehensive data protection and privacy rights to individuals. This bill aims to establish guidelines for the processing of personal data, address concerns related to data breaches, and establish a data protection authority to oversee and enforce data protection regulations.

The evolution of India's legal framework reflects the country's recognition of the importance of safeguarding privacy rights in the digital age. As technology continues to advance, ensuring robust data protection measures and implementing effective privacy regulations are essential for preserving individuals' privacy and fostering trust in the digital ecosystem.

3. DIGITAL SURVEILLANCE TECHNOLOGIES

Digital surveillance technologies have emerged as powerful tools for monitoring, collecting, and analyzing vast amounts of data in the digital age. These technologies have revolutionized the way governments, corporations, and other entities conduct surveillance activities, raising important legal, ethical, and societal concerns.

- Closed-Circuit Television (CCTV) Cameras
- Facial Recognition Systems
- Data Mining and Profiling
- Location Tracking
- Internet Monitoring and Communication Surveillance

The implementation of digital surveillance technologies gives rise to critical legal and ethical considerations concerning privacy, human rights, and broader societal implications.



Volume No.-IV, Issue No.-II, November, 2023, ISSN: 2582-6263

4. IMPLICATIONS OF DIGITAL SURVEILLANCE ON PRIVACY

Digital surveillance technologies have significant implications for privacy, as they introduce new challenges and risks to individuals' personal information and autonomy. The widespread use of these technologies by governments, corporations, and other entities raises concerns regarding the erosion of privacy rights and the potential for abuse.

4.1. Invasion of Privacy

Digital surveillance can lead to the invasion of individuals' privacy in both public and private spaces. Surveillance technologies, such as CCTV cameras and location tracking systems, enable the monitoring and recording of individuals' activities and movements without their knowledge or consent.

4.2. Data Collection and Retention

Digital surveillance involves the collection and storage of vast amounts of personal data. Surveillance technologies capture various types of data, including video footage, biometric information, online activities, and communication metadata. The collection and retention of such data raise concerns about the potential misuse, unauthorized access, and security breaches that can lead to identity theft, surveillance abuses, and threats to individuals' personal safety.

4.3. Profiling and Discrimination

The data collected through digital surveillance technologies can be used for profiling individuals based on their characteristics, behaviors, or preferences. Profiling can lead to discriminatory practices, where individuals are treated differently or targeted based on their perceived characteristics.

4.4. Threats to Freedom of Expression and Association

Digital surveillance can have a chilling effect on individuals' freedom of expression and association. The knowledge that one's online activities, communications, and social media interactions are being monitored can lead to self-censorship and the suppression of dissenting opinions.



4.5. Government Surveillance and Mass Monitoring

Digital surveillance technologies enable governments to engage in mass monitoring and surveillance of their citizens. This raises concerns about the potential abuse of power, infringement on civil liberties, and the erosion of trust between governments and their citizens.

4.6. PSYCHOLOGICAL AND SOCIETAL IMPACT:

The pervasive presence of digital surveillance technologies can have psychological and societal impacts. The constant awareness of being under surveillance can create feelings of anxiety, self-consciousness, and mistrust.

5. LEGAL FRAMEWORK FOR PRIVACY PROTECTION

Privacy protection is crucial in the digital age, where individuals' personal information is vulnerable to surveillance and misuse. To address these concerns, various legal frameworks have been established to safeguard individuals' privacy rights.

5.1. International Level

5.1.1. Universal Declaration of Human Rights (UDHR)

The UDHR, adopted by the United Nations General Assembly in 1948⁹, stands as a pivotal document recognizing the right to privacy as a fundamental human right. Article 12 of the UDHR firmly asserts that "no one shall be subjected to arbitrary interference with his privacy." This declaration provides a foundational principle for safeguarding privacy on a global scale.

5.1.2. International Covenant on Civil and Political Rights (ICCPR)

The ICCPR, adopted by the United Nations in 1966¹⁰, further elaborates on the right to privacy. Article 17 of the ICCPR emphasizes that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence." It underscores the significance of privacy in protecting individuals' personal and familial spheres.

⁹United Nations. (1948). Universal Declaration of Human Rights

¹⁰United Nations. (1966). International Covenant on Civil and Political Rights.

Copyright © JURJ http://jagannathuniversity.org/jurj

Political Rights.

Copyright © JURJ



Volume No.-IV, Issue No.-II, November, 2023, ISSN: 2582-6263

5.1.3. European Convention on Human Rights (ECHR)

The ÉCHR, established by the Council of Europe in 1950¹¹, guarantees the right to privacy under Article 8. This provision safeguards individuals' private and family life, home, and correspondence. The European Court of Human Rights plays a vital role in interpreting and upholding privacy rights under the ECHR.

5.1.4. General Data Protection Regulation (GDPR)

The GDPR, implemented by the European Union in 2018¹², sets comprehensive rules for the protection of personal data. It applies to organizations processing the personal data of individuals within the EU, regardless of the organization's location. The GDPR reinforces individuals' rights, including the right to be informed, the right to access personal data, and the right to erasure.

5.2. National Level:

5.2.1. Constitutional Provisions

Article 21 of the Indian Constitution guarantees the right to life and personal liberty, a right that the Indian judiciary has interpreted to include the right to privacy. In the seminal judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India*¹³, the Indian Supreme Court affirmed the fundamental right to privacy as an intrinsic part of the right to life and personal liberty protected under Article 21.

5.2.2. Statutory Framework

The Information Technology Act, 2000: The Information Technology Act (IT Act) serves as the primary legislation governing various aspects of electronic transactions and digital communication in India. It contains provisions concerning data protection, privacy, and cybersecurity. Section 43A of the IT Act, along with the associated Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, imposes obligations on entities handling sensitive personal data to implement reasonable security measures and ensure the protection of personal information.

¹¹Council of Europe. (1950). European Convention on Human Rights.

¹²European Union. (2016). General Data Protection Regulation.

¹³Justice K.S. Puttaswamy (Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012, Supreme Court of India (2017).



5.2.3. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016¹⁴:

The Aadhaar Act was enacted to provide a unique identity number, known as Aadhaar, to residents of India. It contains provisions pertaining to the collection, storage, and use of biometric and demographic information. The Act also includes provisions for the protection of individuals' privacy and places restrictions on the sharing of Aadhaar-related information.

5.2.4. Judicial Interpretations

Justice K.S. Puttaswamy (Retd.) v. Union of India: As mentioned earlier, the landmark judgment of the Indian Supreme Court in the Justice K.S. Puttaswamy case recognized the fundamental right to privacy as an integral part of the right to life and personal liberty under Article 21 of the Constitution. This judgment laid a robust foundation for privacy protection in India and underscored the need for a comprehensive data protection regime.

5.2.5. Privacy Judgments subsequent to Puttaswamy

Following the Puttaswamy judgment, the Indian judiciary has continued to play a pivotal role in interpreting and safeguarding privacy rights. Several judgments, such as the *Shreya Singhal v. Union of India* case¹⁵, which struck down Section 66A of the Information Technology Act, and the *Justice K.S. Puttaswamy (Retd.) v. Union of India II case*¹⁶, which upheld the constitutionality of the Aadhaar Act with certain limitations, have contributed significantly to the development of privacy jurisprudence in India.

6. CASE STUDIES AND EXAMPLES

6.1. Prism Surveillance Program

The PRISM surveillance program, disclosed by Edward Snowden in 2013, is a notable case study that has implications for privacy in the Indian context as well. PRISM involved the mass surveillance of personal data by the National Security Agency (NSA) in the United States,

¹⁴The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, India.

¹⁵Shreya Singhal v. Union of India, Writ Petition (Criminal) No. 167 of 2012, Supreme Court of India (2015).

¹⁶Justice K.S. Puttaswamy (Retd.) v. Union of India II, Writ Petition (Civil) No. 494 of 2012, Supreme Court of India (2018).

Copyright © JURJ http://jagannathuniversity.org/jurj



Volume No.-IV, Issue No.-II, November, 2023, ISSN: 2582-6263

including data collected from major Indian tech companies. This case highlights the need for robust legal safeguards and transparency surrounding surveillance programs, especially when it involves the data of Indian citizens.¹⁷

6.2. Aadhaar Biometric Data Collection:

India's unique identification system, Aadhaar, has been a subject of privacy concerns due to its collection and storage of biometric data, such as fingerprints and iris scans. The case of Aadhaar has sparked intense debates about the potential misuse of personal data, the risk of surveillance, and the necessity for robust data protection measures.

In response to these concerns, the Supreme Court of India has played a pivotal role in addressing and scrutinizing the Aadhaar system. The court has issued landmark judgments that underscore the importance of privacy rights and individual autonomy within the Aadhaar framework. These judgments have emphasized the need to strike a delicate balance between the goals of providing efficient public services and safeguarding citizens' privacy and data security.

As a result of the Supreme Court's intervention, several significant changes have been made to the Aadhaar system, including the introduction of robust data protection measures and limiting the scope of data collection and usage. The court has also emphasized the need for clear and explicit informed consent from individuals regarding the sharing and usage of their personal data.

Overall, the Aadhaar case has prompted critical discussions about privacy rights and data protection in India. It has set essential precedents for ensuring that technological advancements and data-driven initiatives do not come at the cost of compromising citizens' fundamental right to privacy. The Supreme Court's involvement has been instrumental in shaping the Aadhaar system to be more privacy-centric and safeguarding citizens' personal data in the digital age.

6.3. Social Media and Personal Data Protection

The Cambridge Analytica scandal, although primarily focused on the United States, has implications for privacy in the Indian context as

¹⁷Greenwald, G., &MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. The Guardian.



well. The misuse of personal data harvested from Facebook users has raised concerns about the privacy practices of social media platforms and the potential impact on Indian users. The case underscores the need for stringent data protection regulations, transparency in data practices, and informed consent for the use of personal data. 18

6.4. Surveillance and Aadhaar-linked Systems

The increasing integration of Aadhaar in various government services and programs, such as financial transactions, healthcare, and social welfare schemes, has raised concerns about the potential for widespread surveillance. The use of Aadhaar-linked systems has the potential to create comprehensive profiles of individuals, which could be misused or lead to privacy breaches. This case highlights the need for robust safeguards, transparency, and accountability in the use of Aadhaar data to protect citizens' privacy.

7. FUTURE TRENDS AND CHALLENGES

As technology continues to advance at a rapid pace, the landscape of digital surveillance and privacy protection is expected to undergo significant changes. This section explores some future trends and challenges that are likely to shape the intersection of privacy and digital surveillance in the years to come.

7.1. Big Data and Artificial Intelligence

The rapid growth of big data and artificial intelligence (ĂI) technologies presents a dual impact on privacy. On the positive side, the analysis of extensive datasets holds immense potential for valuable insights and innovation. However, the collection and processing of vast amounts of personal data also raise significant concerns about individual privacy.

algorithms ΑI become increasingly sophisticated, there is a pressing need to find a delicate balance between data-driven advancements and privacy protection. The challenge lies in potential harnessing the of ΑI compromising the privacy rights of individuals. To address this, emerging privacy-preserving AI techniques, such as federated learning and differential privacy, are gaining prominence. These techniques aim to strike a harmonious equilibrium

Copyright © JURJ http://jagannathuniversity.org/jurj



Volume No.-IV, Issue No.-II, November, 2023, ISSN: 2582-6263

by enabling AI systems to learn from distributed data sources while preserving the privacy of individual contributors. By leveraging these privacy-enhancing approaches, society can navigate the exciting possibilities offered by big data and AI while upholding the critical importance of individual privacy.¹⁹

7.2. Internet of Things (IoT)

The rapid growth of the IoT, with interconnected devices and sensors, creates a web of surveillance potential. IoT devices collect vast amounts of personal data, ranging from biometric information to behavioral patterns. Ensuring privacy in an IoT ecosystem requires robust security measures, transparent data handling practices, and user-centric privacy controls. The challenge lies in developing privacy frameworks that address the unique characteristics environments.²⁰ and vulnerabilities of

7.3. Biometric Surveillance

Advancements in biometric technologies, such as facial recognition and fingerprint scanning, present new challenges to privacy. Biometric data is highly personal and unique to individuals, raising concerns about its collection, storage, and potential misuse. deployment widespread of biometric surveillance systems by governments and private entities necessitates the establishment of clear regulations and safeguards to protect individual privacy rights.²¹

7.4. Privacy in Online Social Networks

Online social networks have become integral to modern communication and social interactions. However, the extensive collection of personal data by social media platforms raises privacy concerns. Future trends in privacy protection for online social networks involve empowering users with granular privacy controls, enhancing transparency regarding

¹⁸Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian.

¹⁹Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308-318.

²⁰Perera, C., Zaslavsky, A., Christen, P., &Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by Internet of Things. Transactions on Emerging Telecommunications Technologies, 25(1), 81-93.

²¹Pagallo, U. (2018). The legal challenges of facial recognition. Computer Law & Security Review, 34(1), 23-30.



data practices, and enabling individuals to have greater ownership and control over their personal information.²²

8. CONCLUSION AND SUGGESTIONS

In conclusion, India's right to privacy faces significant challenges in the digital age due to the rapid growth of digital technologies, leading to increased surveillance and data protection concerns. The article examined various aspects, including privacy rights evolution, implications of digital surveillance, legal frameworks, ethical considerations, case studies, privacy-enhancing technologies, and future trends specific to India.

Digital surveillance has profound implications for privacy, necessitating a balance between legitimate objectives like national security and protecting individual privacy rights. Collaborative efforts are needed from policymakers, technology developers, civil society, and citizens to establish robust data protection regulations, adopt privacy-enhancing technologies, and promote digital literacy. By prioritizing privacy as a fundamental right, India can responsibly navigate the digital landscape and safeguard its citizens' rights in the digital age.

To address these challenges and safeguard the right to privacy in India's digital landscape, the following measures can be taken into consideration:

- Strengthen Legal Frameworks
- Promote Transparency and Accountability
- Privacy by Design
- User Education and Empowerment
- International Cooperation

By embracing these suggestions and continuously adapting to technological advancements, India can foster an environment where privacy is respected, and individuals' rights are upheld in the face of digital surveillance. It is a collective responsibility of the government, organizations, and individuals to ensure that privacy rights are safeguarded, enabling Indian citizens to navigate the digital landscape with confidence and trust.

REFERENCES

- [1]. Ackerman, S., & Sánchez Abril, P. (2017). The digital fourth amendment and the global future of privacy. Emory Law Journal, 67(2), 219-291.
- [2]. Barocas, S., &Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In Privacy, Big Data, and the Public Good: Frameworks for Engagement (pp. 44-75). Cambridge University Press.

Jagannath University

Volume No.-IV, Issue No.-II, November, 2023, ISSN: 2582-6263

- [3]. Floridi, L. (2017). Is information the key to understanding the universe? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 375(2094), 20160335.
- [4]. Mayer-Schönberger, V., &Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.
- [5]. Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57, 1701-1777.
- [6]. Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477-564.
- [7]. Stahl, B. C., Timmermans, J., Mittelstadt, B., & Van den Hoven, J. (2016). Ethical issues of profiling and big data. In The Cambridge Handbook of Information and Computer Ethics (pp. 248-272). Cambridge University Press.
- [8]. Swire, P. P. (2017). A model for when disclosure helps security: What is different about computer and network security?. Journal of Policy and Complex Systems, 3(1), 19-40.
- [9]. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193-220.
- [10]. Westin, A. F. (1967). Privacy and freedom. The American Book Company.
- [11].Justice K.S. Puttaswamy (Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012
- [12]. The Personal Data Protection Bill, 2019
- [13]. Internet Freedom Foundation (IFF)
- [14]. Shreya Singhal v. Union of India, Writ Petition (Criminal) No. 167 of 2012
- [15]. Telecom Regulatory Authority of India (TRAI)



First Author: Prof. S.P.S. Shekhawat, is a knowledge thinktank in the field of academics. He was formerly appointed as Dean, Faculty of Law at University of Rajasthan.He secured a toppers position at University during his LL.M. program. At present, he is appointed as Head & Dean,

Faculty of Law at Jagannath University, Jaipur. Hissupervisory role as guide for more than twenty Ph.D. candidates proved fruitful in suggesting legislative policies to Parliament. His dynamic personality is built upon renowned positionsheld such as; Journal Editor of Journal of Legal Studies Editorial Board; Chairman at National seminars; Expert Member of Academic Board at Indian Law Institute, New Delhi; Expert Member of selection board at R.P.S.C., Ajmer. He enlightened various judges, academicians and young scholars by publishing almost aroundfortyresearch papers in prestigious Journals on emerging legal issues including; uniform civil code, sustainable development, Human Rights, Constitutional laws, Judicial Activism, Mohammadan laws, Domestic Violence, Legal Aid, DNA profiling, Right to Information, Evidence Act, Rights of under trial prisoners.

²²Mislove, A., Viswanath, B., Gummadi, K. P., &Druschel, P. (2010). You are who you know: inferring user profiles in online social networks. Proceedings of the Third ACM International Conference on Web Search and Data Mining, 251-260.





Second Author:Abhishek is currently pursuing his Ph.D. at Vivekananda Global University, Jaipur, showcasing his commitment to advancing legal research. Abhishek holds an LL.M. in Criminology from Jagannath University, Jaipur, where he graduated with distinction, demonstrating his academic prowess.

In addition to his academic pursuits, Abhishek is an Assistant Professor at the Faculty of Law, Jagan Nath University, where he imparts his knowledge and expertise to aspiring legal minds. His dedication to academia is further underscored by his previous role as an Assistant Professor at the Department of Law, Vivekananda Global University.

His notable contributions extend beyond the courtroom and lecture halls. Abhishek has authored and presented research papers on diverse legal topics, including "The Impact of Social Media on Adolescent Behavior," "ADR Mechanism and Arbitration Law in India," and "Unveiling Online Digital Piracy in the Indian Film Industry."

Third Author: Monica Singh is a Research Scholar currently



pursuing PhD in Faculty of Law, Jagan Nath University, Jaipur. The topic of her Research is "Abuse of Laws by Women in India: A socio legal Study". She has attended various conferences and seminars related to her topic of

research and has a good experience in law field. With her research work she very positively wants a change In the current laws which are only in favour of women in our society.

Volume No.-IV, Issue No.-II, November, 2023, ISSN: 2582-6263

Copyright © JURJ http://jagannathuniversity.org/jurj