

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.



Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS
ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

EXPLORING THE IMPACT OF TECHNOLOGY ON PRIVACY RIGHTS: BALANCING INNOVATION AND MEDIA LAWS

AUTHORED BY - NAINA JATAV

INTRODUCTION

The right to privacy and freedom of expression have become increasingly intertwined with the advent of the digital age. This is exemplified, for instance, by the chilling effect *that privacy violations can have on media freedom. Developments such as hacking, data retention and big data, artificial intelligence-powered territorial surveillance, monitoring of online activity, and hacking all simultaneously threaten our privacy and the freedom to practice journalism. Free and independent journalism is in threat due to the increasing sophistication and undetectability of malware and spyware as well as the growing use of these tools against human rights¹ advocates and journalists by both state and non-state actors. A fundamental requirement for media freedom internationally acknowledged and codified in UN Resolutions, source protection is violated by surveillance since it can reveal material that journalists have obtained, including information from whistleblowers. For journalists to do their jobs and to guarantee that we have access to accurate and trustworthy information, privacy is needed. It is essential if they want to be able to speak openly with sources, obtain private information, look into corruption, and ensure both their own and their sources' safety.*

The lack of robust legal protections for these technologies makes them more accessible because most surveillance laws have not kept up with advancements in technology. Journalists and other law-abiding individuals are targeted on the pretext of security, and national control over security activities and *security legislation is insufficient*. Additionally, this jeopardizes our group's right to privacy and information access.

¹ Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue', 'Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue' (International journal of law and information technology 7 February 2016).

Furthermore, the COVID-19 epidemic has highlighted the extent of the internet economy's influence. The social, political, and economic spheres have all migrated substantially online, and internet corporations now play a major role in many facets of society. A growing number of people are questioning how an ecosystem, on which we all depend, is held democratically responsible as the public and societal significance of internet corporations increases.

KEYWORDS- *Media, Rights, Privacy, Transparency, Regulation, Digital Age, Innovation.*

ISSUES AND PROBLEM ARISING

The digital age has had a significant impact on many elements of human existence, including privacy rights. The fast rise of the internet, social media, and digital communication platforms has altered how people communicate, share information, and protect their personal privacy. This transition presents important problems and opportunities, particularly in the context of media laws, which seek to balance the right to privacy with the values of free expression and public interest.

Current media regulations frequently *struggle to keep up with technology* advancements, leaving a regulatory gap that can either hinder technological growth or inadequately *safeguard human privacy*. This quandary needs a thorough assessment of how media laws might evolve to meet the conflicting goals of supporting technology innovation and protecting privacy rights. The challenge is to establish and execute legislative frameworks and rules that strike an appropriate balance, ensuring that technological benefits do not outweigh personal privacy concerns.

FEW INSTANCES

The analysis contains case studies of important intersections between technology and media legislation. These case studies provide practical insights into how media regulations are applied and the results of their implementation in real-world circumstances. This section explores the problems and opportunities for striking a balance between innovation and privacy rights. It takes into account the opinions of different stakeholders, such as individuals, corporations, governments, and advocacy groups.

In recent years, the convergence of privacy rights, media practices, and social media surveillance has become a source of contention. Surveillance technology advancements have

given media and government agencies unprecedented access to personal data, frequently resulting in severe privacy abuses. This blog digs at a recent high-profile case of privacy abuses involving media surveillance of social media, as well as few additional examples that highlight the broader implications and ethical concerns surrounding this topic.

U.S. Federal Agencies and Social Media Surveillance

The most recent and prominent case involves the extensive surveillance conducted by U.S. federal agencies, including the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the State Department. These agencies have been monitoring social media platforms for various purposes such as criminal investigations, threat detection, and immigration screening. This widespread surveillance raises significant concerns about civil rights and privacy, particularly for marginalized communities who are disproportionately targeted.²

Cambridge Analytica and Facebook

The Cambridge Analytica scandal is one of the most well-known examples of privacy abuses committed by social media surveillance. In 2018, it was found that Cambridge Analytica, a political consulting firm, had acquired the personal information of millions of Facebook users without their knowledge. This information was used to generate detailed voter profiles, which influenced the 2016 US presidential election and the Brexit referendum. The intent was to create voter profiles to influence political results. Moreover, outcomes in raised awareness regarding data privacy, leading to increased monitoring of social media sites.³

Clearview AI and Facial Recognition Technology

Clearview AI, a facial recognition company, has been criticized for scraping billions of images from social media platforms like Facebook, Twitter, and YouTube to build a massive facial

² Statement of Civil Rights Concerns About Monitoring of Social Media by Law Enforcement | Brennan Center for Justice](<https://www.brennancenter.org/our-work/research-reports/statement-civil-rights-concerns-about-monitoring-social-media-law>) [oai_citation:2, Social Media Surveillance by the U.S. Government | Brennan Center for Justice](<https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government>) [oai_citation:3, Federal Government Social Media Surveillance, Explained | Brennan Center for Justice](<https://www.brennancenter.org/our-work/research-reports/federal-government-social-media-surveillance-explained>).

³ Statement of Civil Rights Concerns About Monitoring of Social Media by Law Enforcement | Brennan Center for Justice (<https://www.brennancenter.org/our-work/research-reports/statement-civil-rights-concerns-about-monitoring-social-media-law>) [oai_citation:5, Social Media Surveillance by the U.S. Government | Brennan Center for Justice] (<https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government>).

recognition database. Law enforcement agencies across the globe have used this database, often without the knowledge or consent of the individuals whose images were collected⁴. Which lead to significant privacy concerns and legal challenges over unauthorized data collection and usage.

Pegasus Spyware Scandal

The Pegasus spyware incident is India's most recent and important case of media spying violating privacy rights. In July 2021, it was revealed that the Israeli spyware Pegasus, produced by the NSO Group, was used to monitor more than 300 Indian phone numbers. The targets included journalists, activists, opposition politicians, and government officials. The spyware used smartphone vulnerabilities to access messages, emails, and calls without the user's knowledge. This has targeted journalists, activists, opposition politicians, and government officials by exploiting smartphone vulnerabilities for monitoring. Impact in Concerns have been raised over privacy rights, press freedom, and political exploitation of monitoring techniques.

Aadhaar Data Breach

Aadhaar, India's biometric identification system, has been the source of various privacy concerns. In 2018, it was revealed that the personal information of over 1.1 billion Aadhaar cards was available online owing to a security breach. This includes sensitive information including names, addresses, phone numbers, and email addresses, raising severe questions about data security and privacy. It highlighted the weaknesses in India's biometric data infrastructure.

Social Media Monitoring During Anti-CAA Protests

During the 2020 anti-Citizenship Amendment Act (CAA) protests, the Indian government came under fire for using social media monitoring extensively to track dissent. Authorities allegedly exploited social media platforms to identify and jail demonstrators, raising worries about the repression of free expression and the right to demonstrate. Concerns Suppression of free expression and the right to protest. Result in a loss of trust in the government's adherence

⁴ Statement of Civil Rights Concerns About Monitoring of Social Media by Law Enforcement | Brennan Center for Justice (<https://www.brennancenter.org/our-work/research-reports/statement-civil-rights-concerns-about-monitoring-social-media-law>) [oai_citation:7, Social Media Surveillance by the U.S. Government | Brennan Center for Justice] (<https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government>).

to democratic norms.

SUGGESTIONS

Many international human rights documents, including the 1948 Universal Declaration of Human Rights (Article 12), the 1966 International Covenant on Civil and Political Rights (Article 17), the European Convention on Human Rights (Article 8), the African Charter on Human and Peoples' Rights, and the Arab Charter on Human Rights (arts. 16, 8), among others, recognize the right to private life. It is common to conflate the ideas of private life and privacy.

The proportionality principle is the primary legal technique used to balance the various human rights when they conflict with the right to privacy. Then, based on the proportionality principle, a balancing test must be performed. The proportionality test is specifically used in the context of the American regional human rights system (IACHR), the African regional legal framework (ACHPR), the East African Court of Justice (EACJ), and the European legal systems (ECJ and ECHR). It has also been making an appearance in a number of Human Rights Committee (HRC) decisions.

Three steps make up the proportionality test: necessity (also known as the "less restrictive alternative" or "minimal impairment"; if the action taken is the least restrictive alternative), suitability (i.e., whether the interference is actually appropriate to achieve the purported aim), and proportionality in the strict sense (i.e., whether the benefits achieved are outweighed by the limitations caused). Additionally, two additional tests of legality—whether the interference is founded on national law—and justifiable aim are typically conducted before it.

To determine whether the privacy rights guaranteed by the applicable Conventions have been violated, the Regional Human Rights Courts employ a three-part test. These are predicated on the ideas of necessity, legitimacy, and lawfulness in a democratic society.

LAWFULNESS

The term "lawfulness" refers to the presence of a prior, obtainable law that was passed by a legitimate procedure and that permits the specific person or authority to operate. Stated differently, the basis for the interference must be observable and predictable domestic legislation.

LEGITIMACY

It refers to the action's goals if they further one of the following legal purposes as defined by the Conventions: national security, public safety, the nation's economic prosperity, the avoidance of chaos or criminal activity, the preservation of morality or health, or the defense of others' rights and liberties.

NECESSITY

Necessity is marked by the lack of a less restrictive option. In this instance, it also resonates with stringent proportionality features since it weighs the potential benefits of the action against the potential impact it may have on rights.

CONCLUSION

At the national and international levels, robust legal and regulatory frameworks are required for the peaceful coexistence of innovation and privacy. Governments, academic institutions, civic society, and AI developers must work together to shape a future that is focused on people. Also, Public awareness and education are essential components of this project. Encouraging a society that is aware of the possibilities presented by artificial intelligence and how it affects human rights enables people to actively engage in the decision-making processes that will shape our shared digital future.

Ultimately, the responsibility lies with us, as stewards of technology, to steer it in a direction that reflects our shared values and aspirations. By embracing the principles of transparency, fairness, and accountability, we can strike the delicate balance between innovation and safeguarding the fundamental rights of humanity in the digital age.

Further, each instance emphasises the importance of strong data protection regulations, increased openness, and accountability to guarantee that individual privacy rights are not jeopardised in the name of security or public interest.

As social media and digital technology evolve, protecting privacy remains critical. The authorities must develop and enforce strict privacy legislation, assure monitoring of surveillance activities, and strike a delicate balance between security concerns and individual liberties. Addressing these concerns will preserve citizens' privacy while also promoting democratic values and trust in governance.

It highlights the nuanced and frequently contentious interplay between privacy rights, media practices, and social media surveillance. While technological advancements have brought tremendous tools for data collecting and analysis, they have also raised serious concerns about privacy and ethical issues. As social media continues to play an important role in modern life, it is critical to address privacy concerns through strong legislation and increased transparency about how data is gathered and utilised. The balance between security and privacy remains a complex and continuing topic, demanding close monitoring and civil liberty. Examining these examples reveals that the convergence of media, technology, and privacy rights necessitates careful consideration in order to protect individual liberties while also addressing valid security concerns.

