

ISSN: 2582-6433



# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary  
Peer Reviewed 6th Edition

VOLUME 2 ISSUE 7

[www.ijlra.com](http://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 2 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

IJLRA

## EDITORIAL TEAM

### EDITORS

#### **Megha Middha**



*Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar*

*Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society*

#### **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.

# **PRIVACY AND SURVEILLANCE: HOW MONITORING AFFECTS OUR LIVES**

AUTHORED BY - SHAGUFA PARVEEN

Privacy and surveillance are two ideas that are connected but frequently at odds with one another. On the one hand, surveillance has the potential to be a useful instrument for enhancing public safety, deterring crime, and safeguarding national security. The employment of surveillance technologies, however, can also result in invasions of personal privacy, a loss of civil liberties, and abuses of power by those in positions of control. The subject of privacy and surveillance is intricate and varied, covering social, legal, ethical, and historical considerations. We will give a general review of the subject in this post, outlining its history, advantages and disadvantages, legal and regulatory environment, and ethical considerations.

## **I. Introduction**

In order to obtain information, maintain control, or identify and prevent crime, surveillance is described as the act of monitoring, observing, or keeping a record of individuals, things, or occurrences. From physical surveillance, like video cameras, to digital surveillance, such tracking software and social media monitoring, there are many different types of surveillance. Contrarily, the right to privacy is the ability to govern one's personal information, to be free from unauthorised access, and to lead an unhindered existence. The Universal Declaration of Human Rights, the European Convention on Human Rights, and the Fourth Amendment of the United States all recognise privacy as a fundamental human right. Privacy is also protected by numerous other international and state legal systems. Constitution. The conflict between surveillance and privacy stems from the possibility of invasion of personal private via surveillance. Even though surveillance

---

Moore, A. D. (2000, July). Employee Monitoring and Computer Technology: Evaluative Surveillance V. Privacy. *Business Ethics Quarterly*, 10(3), 697–709. <https://doi.org/10.2307/3857899>

Hermida, A., & Hernández-Santaolalla, V. (2020, January 7). Horizontal surveillance, mobile communication and social networking sites. The lack of privacy in young people's daily lives. *Communication & Society*, 33(1), 139–152. <https://doi.org/10.15581/003.33.36450>

has the potential to be an effective instrument for enhancing general safety and security, it can also result in abuses of authority, discrimination, and social control. It is crucial to have a thorough awareness of the evolution, advantages and disadvantages, legal and regulatory framework, and ethical issues of surveillance and privacy in order to strike a balance between the benefits of monitoring and the protection of individual privacy rights.

## II. The Development of Monitoring

The practise of surveillance dates back to ancient times, when emperors and rulers employed spies and informants to gather data and keep their citizens under control. However, the industrial revolution and the emergence of contemporary nation-states are to blame for the development of current monitoring systems. Governments started to develop new monitoring techniques to uphold social order and deter crime as cities grew in size, population grew, and commerce grew.

Modern surveillance methods came into being as a result of new technology like photography, telegraphy, and the telephone. Surveillance photographs were made possible by the development of photography in the middle of the 19th century, and they were utilised by law enforcement organisations to identify suspects and gather evidence. Telegraphy and the telephone's quick information transfer over great distances made it simpler for governments to monitor and regulate their territories.

The 20th century saw a revolution in monitoring thanks to the emergence of new technologies like radio, television, and computers. Governments were able to sway public opinion and uphold social control through the employment of radio and television for propaganda and mass communication.<sup>3</sup> Governments and businesses have been able to gather and analyse enormous amounts of data on individuals because to the advent of computers and the internet, raising worries about privacy and civil liberties. There are many different sorts of surveillance, including social, digital, and physical monitoring.

---

<sup>3</sup> Diffie, W., & Landau, S. (2009, September). Communications Surveillance: Privacy and Security at Risk. *Queue*, 7(8), 10–15. <https://doi.org/10.1145/1613128.1613130>

Froomkin, A. M. (2014). Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2400736>

Using cameras, sensors, and other tangible equipment, physical surveillance keeps an eye on individuals, things, or events. If or not the subjects are aware that they are being watched will determine if physical surveillance is overt or covert. Cameras are an example of physical surveillance.

### **III. The Benefits and Drawbacks of Monitoring**

Surveillance has advantages and disadvantages. We will examine the advantages and disadvantages of monitoring in this part, as well as how it affects society.

#### **A. The Advantages of Monitoring**

**Enhanced Security:** Enhanced security is one of the key advantages of monitoring. Theft, vandalism, and assault are just a few of the crimes that surveillance systems can aid in stopping and catching. CCTV cameras put in public areas can serve as a deterrent to criminal activity as well as a tool for law enforcement to identify individuals and acquire evidence. Surveillance can also increase safety in public settings like schools, offices, and other gathering places. In factories, for instance, surveillance systems can help monitor employees and spot potential hazards, while in schools, monitoring can help stop bullying and guarantee the safety of students.

**Public health:** Monitoring and tracking the spread of diseases like COVID-19 can also be done through surveillance. Using monitoring data, public health professionals may spot outbreaks, track the efficacy of immunisations, and take the appropriate precautions to stop the disease's spread.

#### **B. The Negative Effects of Surveillance**

**Privacy Issues:** Privacy issues are one of the key problems of monitoring. When surveillance devices are used, people may worry that their privacy is being violated because they may believe that everything they do is being watched and recorded. **False Sense of Security:** The false sense of security that surveillance may induce is another disadvantage. While surveillance systems may deter some criminals, they can also give people who think they are constantly being watched a false sense of security. **Abuse of Power:** Those in positions of authority may misuse surveillance technologies. Government authorities might, for instance, monitor and intimidate members of particular social groups or political opponents using surveillance technology. Similar to this, employers might spy on their workers without getting their permission or knowledge.

### C. The Social Effects of Surveillance

Society is significantly impacted by surveillance in both positive and negative ways. On the plus side, surveillance can boost public health, increase safety, and raise security. On the downside, monitoring can lead to privacy issues, a false sense of security, and abuse by those in positions of authority. It's critical to weigh the advantages and disadvantages of surveillance. In order to protect people's privacy and civil liberties, surveillance must be utilised properly and ethically, even though it can be a useful tool for enhancing security and safety. Privacy rules and regulations can aid in ensuring both the proper use of surveillance technologies and the observance of people's rights.<sup>4</sup>

As we saw in the last section, there are advantages and disadvantages to monitoring, and it's critical to establish a balance between the two. Privacy rules and regulations are one approach to guarantee that monitoring is utilised morally and responsibly.

#### A. Privacy Laws and Regulations Overview

The purpose of privacy laws and regulations is to safeguard people's civil liberties and privacy. They lay forth regulations and standards for the gathering, use, and dissemination of personal data, including data gleaned from surveillance. The principles of fair information practises, which include the following, are the foundation of privacy laws and regulations in many nations. Individuals must be made aware of how their personal information is collected, used, and disclosed. Individuals must give their consent before their personal information is collected, used, or disclosed. Individuals are entitled to access their personal information and, if necessary, ask that it be updated.

**Security:** It is important to guard against unauthorised access, usage, and disclosure of personal data.

**Accountability:** Businesses that gather, use, and divulge personal data must take responsibility for their actions.

---

<sup>4</sup> Page, A., Kocabas, O., Soyata, T., Aktas, M., & Couderc, J. P. (2014, December 16). Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance. *Annals of Noninvasive Electrocardiology*, 20(4), 328–337. <https://doi.org/10.1111/anec.12204>

## **B. Comparison of International Laws and Regulations**

The laws and rules governing privacy are different in every nation. While some nations have comprehensive privacy laws that offer stern protections for people's privacy, others have fewer safeguards. For instance, the General Data Protection Regulation (GDPR), which is regarded as one of the most comprehensive privacy rules in the world, was enacted by the European Union. The GDPR creates stringent guidelines for the gathering, use, and disclosure of personal information and gives people powerful rights, including the right to have their personal information erased and the right to object to its processing. The privacy laws in the United States are more dispersed, with several laws and regulations governing various sectors and industries. For instance, the Children's Online Privacy Protection Act (COPPA) protects children's personal information online while the Health Insurance Portability and Accountability Act (HIPAA) offers privacy protections for health information.

## **C. Analysis of Current Laws and Regulations' Effectiveness**

Despite the existence of privacy laws and regulations, questions remain concerning how well these laws actually safeguard people's private. Some critics contend that privacy rules are insufficiently strong and do not adequately secure people's personal information. For instance, certain privacy rules might not apply to government surveillance or might have exceptions for purposes of law enforcement or national security. Additionally, some businesses might not fully adhere to privacy laws or might discover ways to do so. Some supporters have demanded stricter privacy laws and rules, as well as more accountability, transparency, and enforcement measures, to address these worries. In conclusion, privacy rules and regulations are crucial for preserving people's civil liberties and privacy in the face of surveillance. The principles of fair information practises give a framework for ensuring that<sup>5</sup> surveillance is utilised responsibly and ethically, despite the fact that laws and regulations vary from nation to nation. To make sure that they continue to be effective in defending people's privacy in the face of new surveillance technologies and practises, privacy laws and regulations must be continually evaluated and improved.

---

<sup>5</sup> Agwi, U. C., Irhebhude, M. E., & Ogwueleka, F. N. (2020, December 22). Video surveillance in examination monitoring. *Security and Privacy*, 4(2). <https://doi.org/10.1002/spy2.144>

#### **IV. Technology and Surveillance**

In order to build and implement surveillance systems, technology is essential. Technology advancements have made it possible to use surveillance techniques that are more effective and efficient, but they have also generated questions about privacy and civil liberties. The function of technology in surveillance and its effects on society will be discussed in this section.

##### **A. Technology's involvement in surveillance**

The evolution of surveillance has been significantly influenced by technology. Technology is heavily used in modern surveillance techniques to capture and process data. For instance, modern security cameras come with facial recognition software and high-resolution lenses that can follow and identify people in real-time. The ability to follow suspects and keep tabs on their whereabouts has also been facilitated by GPS tracking technology for law enforcement organisations.

##### **B. drones being used for surveillance**

In particular, police enforcement organisations are using drones more and more for monitoring. High-resolution cameras and thermal imaging equipment can be added to drones to enable information gathering from a distance. This technology can be helpful for keeping an eye on large crowds or finding criminals in distant locations. However, privacy issues have been brought up by the use of drones, particularly when they are used to monitor people without their knowledge or consent.

##### **C. Social media's effect on surveillance**

For surveillance organisations, social media sites are now a rich source of data. Social media is used by many people to publish personal information and details about their everyday life, which can be used to create a profile of a person's interests, routines, and whereabouts. It is possible to follow someone and keep an eye on their activities using this information. However, privacy issues and the protection of personal data have been brought up by the usage of social media for monitoring reasons.

##### **D. Ethics-related matters**

A number of ethical questions are raised by the use of technology in surveillance. The possibility for misuse of surveillance technologies is one issue. Law enforcement authorities have, for instance, employed facial recognition technology to identify protesters or people taking part in peaceful protests in some situations. The potential for prejudice is another issue. Darker skinned individuals

are more difficult to recognise using facial recognition technology, which could result in racial profiling. The potential for technology to destroy privacy is another issue. Without their knowledge or consent, surveillance cameras and other technologies have the ability to gather enormous amounts of data about people. This information can be used to track their whereabouts and activities, resulting in a surveillance state where people have little freedom of movement or privacy. To ensure that<sup>6</sup> surveillance technology is utilised responsibly and ethically, there is a need for strong privacy laws and regulations.

Overall, there are both advantages and disadvantages to using technology for surveillance. Technology can make surveillance more effective, but it also creates issues with privacy, civil liberties, and the potential for abuse. As a result, it is essential to carefully analyse the moral implications of surveillance technology and to create strict laws that safeguard people's rights and liberties.

## **V. Security at Home and Monitoring**

Governments and law enforcement organisations use surveillance as a crucial instrument to preserve national security. It is employed to stop terrorist acts, track down and capture criminals, and safeguard the security of citizens. However, there are serious questions regarding how to strike a balance between privacy and security raised by the use of monitoring in national security.

### **A. surveillance and national security: a link**

With the use of surveillance, governments can keep an eye out for prospective threats and avert attacks before they happen, which is essential for maintaining national security. For instance, intelligence agencies can utilise surveillance to monitor the actions of terrorist groups and spot people who could be a danger to the country's security.

### **B. How surveillance may be used to stop terrorists**

In several nations around the world, surveillance has been crucial in stopping terrorist strikes. For instance, monitoring in the US helped foil a number of terrorist plans, including the attempt to bomb the New York City subway system in 2009 and the Times Square vehicle bombing attempt in 2010.

---

<sup>6</sup> Shilton, K. (2009, August). Four Billion Little Brothers? Privacy, mobile phones, and ubiquitous data collection. *Queue*, 7(7), 40–47. <https://doi.org/10.1145/1594204.1597790>

### **C. Keeping privacy and security in balance**

The balance between security and privacy is seriously questioned by the use of monitoring for national security purposes. Although monitoring might deter terrorist acts and other crimes, it can also violate people's right to privacy. There has been much discussion about the conflict between these two goals in many nations, especially those that place a high importance on individual privacy rights. Individual rights might be violated and opposition can be repressed, according to privacy activists. For instance, the Patriot Act, a U.S. law passed in the wake of the 9/11 terrorist attacks, increased government monitoring authority and caused alarm over potential infringement of private rights. The law permitted the government to gather information about American people without a court order and perform warrantless wiretapping. Privacy advocates viewed this as an infringement on people's rights and an invasion of their privacy. Governments contend, however, that surveillance is necessary to safeguard populations and preserve national security. According to them, monitoring is only employed when a clear threat to national security exists and is vital to stop terrorist attacks.

### **D. Monitoring and the COVID-19 Epidemic**

The COVID-19 pandemic has led to a rise in the usage of surveillance technology to track and limit the virus's spread. Governments all throughout the world have employed surveillance to enact quarantine directives, monitor the travel of contaminated people, and guarantee mask compliance. For instance, the Chinese government has employed facial recognition technology to keep tabs on citizens and enact quarantine regulations. The Singaporean government uses Bluetooth technology to follow people who have tested positive for COVID-19 wherever they go.

Although these efforts have been successful in stopping the virus's spread, they have also caused some people to worry that their privacy rights may have been violated. Critics contend that the deployment of surveillance technology to track people's activities during the pandemic could create a risky precedent and result in future overreaching government surveillance.

### **VI. Education and Monitoring**

The monitoring of pupils' behaviour and activities inside of schools is referred to as surveillance. To maintain student safety and deter crime, schools employ a variety of surveillance techniques, including video cameras, metal detectors, and drug testing. While surveillance at schools can help reduce crime and increase safety, it also raises issues with student privacy and civil liberties.

State and federal laws and regulations govern how surveillance is used in schools. The Family

Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA) in the United States safeguard student privacy and control how student data is used. According to these laws, schools must acquire parental permission before collecting any personal information from them and give them access to their children's records. The use of school surveillance has a number of advantages and disadvantages. On the one hand, surveillance in schools can aid in deterring violence like bullying and harassment. Additionally, it can aid in locating and assisting students who are battling drug use, mental health issues, or other issues. Additionally, school surveillance can contribute to ensuring students' safety and security while on school grounds. On the other hand, student privacy and civil liberties may be violated by school surveillance. It can result in a climate of distrust and constant observation, where pupils believe they are being watched and evaluated based on their actions. Furthermore, discrimination against students based on their race, ethnicity, or other characteristics may be practised in schools through the use of surveillance.

## **VII. Surveillance and Human Rights**

Since surveillance can be used to track and restrict the actions of people, groups, and society, it has a substantial impact on human rights. Concerns about privacy violations, civil liberties violations, and violations of human rights have been raised by the use of surveillance technology by governments and other organisations. In this chapter, we'll look at how surveillance affects human rights, the moral ramifications of violating those rights when conducting surveillance, and the significance of upholding those rights.

The use of surveillance technology may significantly affect how communities and people exercise their human rights. International human rights legislation protects the rights to privacy, freedom of expression, and freedom of association, yet surveillance can erode these rights. For instance, governments' use of surveillance to keep tabs on the activities of journalists, human rights advocates, and political dissenters may stifle free expression and association. The use of surveillance to harass and intimidate those who disagree with the government or who identify as members of minority groups is another possibility. Privacy rights are also threatened by the gathering and storage of personal data by for-profit businesses and governmental organisations. Data gathered in large quantities may be used to create profiles that could be used to discriminate against people based on their race, religion, political views, or other traits. Misuse of personal information can also result in financial fraud, identity theft, and other types of cybercrime.