Naveen Talawar, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Surveillance in Smart Cities: A Threat to Privacy or a Tool for Public Safety?

Naveen Talawar
LL.M. Candidate, Law and Technology
National Law School of India University (NLSIU), Bengaluru, India

Abstract - **The use of enhanced surveillance systems in the smart cities provides a great opportunity in enhancing the secure society, efficient urban planning, and development. However, it broadens some significant questions concerning the rights of individual privacy and the feasible manipulative use of data. While most proponents of smart cities claim that surveillance is one of the essential tools for keeping citizens safe, this paper will explore whether it is in fact the only means for protecting people in urban environments or just another invasive method to violate our rights to privacy.**

The research employs the doctrinal research method to analyse the existing legal provisions on surveillance in India and other jurisdictions. It discusses the importance of privacy as a human right and legal concerns arising from the rising adoption of AI, facial recognition technology, as well as data analysis in the management of cities. It also provides an analytical discussion of current privacy protections to ascertain their efficacy.

The selection of this theme is based on the fact that smart technologies are increasingly extending over cities, and therefore, the privacy concerns arising from these technologies need to be tackled. It is therefore important to fully grasp the meanings of surveillance within smart cities in order to come up with fair policies that would safeguard the privacy of the citizens and at the same time enhance security. The goal of the study is to outline a fair approach that the cities may follow when putting in place the surveillance technologies and still uphold the democratic governance as well as privacy of a person.

Finally, the paper concludes by presenting the guidelines for policymakers and urban planners to undertake surveillance ethically by providing recommendations that include the need to embrace transparency and accountability in the use of the technology.

Keywords - **Surveillance, Smart cities, Public safety, Privacy rights.**

I. INTRODUCTION

Technology has dramatically changed the way cities work and converted them into "*smart cities*" where data and automation help towards efficiency and safety.[1] While innovations in this direction mean a host of benefits, better services, safer streets, and wiser urban planning, such innovations raise serious privacy concerns.[2] A controversy arises when deciding whether it is actually beneficial or whether such surveillance technologies, which is one of the methods of protecting society, infringe on individual freedoms.

India is an embodiment of that challenge. Comparitech[3] ranked India third in countries failing to protect privacy or actually building a surveillance state in the 2019 survey.[4] Laws such as the Indian Telegraph Act, 1885, and the Information Technology Act, 2000, permit the government to conduct surveillance provided certain conditions are met, but these laws do not have adequate safeguards against abuse.[5] These were highlighted in the Pegasus spyware scandal, showing that without strong data protection laws, those laws are most likely to be abused.[6] While India's Supreme Court recognized privacy as a fundamental right[7]

back in 2017, the government allowing ten agencies to conduct surveillance in 2018 raised questions regarding the delicate balance between security and privacy of the individual. [8]

The present paper discusses whether surveillance in smart cities is an essential tool for ensuring public safety or an invasive threat to personal privacy. The research critically considers India's legal framework and compares it with international best practices, attempting to understand various perspectives, seeking a fair way of deploying smart technologies. It seeks to strike a delicate balance in which technology can provide security without jeopardising citizens' fundamental rights.

II. LITERATURE REVIEW

The idea of privacy has been debated along philosophical, legal, and social discourses for a long time, but in the digital era, it has radically changed and acquired many layers of meaning.[9] Bhairav Acharya argues that the essence of privacy in India remains complex and very different from the orthodox ideas of privacy as an arena of intimacy and secrecy. He regards privacy as a multilayered concept which involves issues about state surveillance coupled with the challenging advances in information technology. This perspective is very important to understand the growth of privacy jurisprudence in India.[10]

In parallel, Gautam Bhatia's work on the constitutional evolution of privacy in India deals with questions about state surveillance and its implications for the rights to privacy.[11] His argument thus aligns with Agnidipto Tarafder's comparative examination of privacy laws in India and the United States, emphasising how India has failed to develop a solid legal framework governing surveillance.[12] Both experts emphasise how important it is to have particular laws and judicial oversight to protect privacy in the face of growing surveillance.

A number of scholars warn about the results of complete surveillance. Amalia Berggren referred to the ideas of Michel Foucault, describing how even the feeling of being watched is sufficient to restrict freedom and lead to self-censorship.[13] In the same vein, James Boyle discusses how such technologies, while empowering in some ways, might lead to new shapes of invisible censorship and control.[14] This discussion becomes way more important in the case of smart cities. Large volumes of data are collected, giving consumers a false sense of security and decreasing their privacy.

The debate on privacy at the global level takes on a Foucauldian echo in the investigation that James Boyle makes with respect to "hardwired sensors" in cyberspace. According to Boyle, technology is less a neutral tool but more a method through which power structures can be embedded that interfere with and control information flows.[15] Mark Rathbone furthers this line of argument when, with respect to digital technologies, he carries through a panopticism in the light of how capitalism and the structures of surveillance associated with it construct "*digital personae*" either for purposes of profit or control.[16] He contrasts this with Adam Smith's idea of the "impartial spectator," whereby morality and self-regulation are adequate to resist oppressive surveillance.

This is further exacerbated with the advent of social media, as highlighted by Vrinda Bhandari. [17] She is against the immense collection of data by platforms like Facebook, most of the time with confusing policies that confuse the user. Her argument fits well into Sonali Srivastava's analysis of India's Digital Personal Data Protection Act, 2023 (DPDP Act), which, although a progressive step, still has gaps pertaining to the consolidation of data misuse.[18] Srivastava further compares the DPDP Act with the General Data Protection Regulation (GDPR) of the European Union and the Personal Information Protection Law (PIPL) of China, underlining how such a strong legal structure was required so as to balance security concerns and the rights of every individual to his or her privacy.

The question of the societal impacts of surveillance goes beyond what happens within the state and corporate domains to touch on most of the human experiences. Angela C. Henderson and co-authors

apply Foucault's concept of surveillance to modern motherhood in contemporary times when media scrutiny and social expectations create a "new state of surveillance" that compels mothers to adhere to ideal parenting standards.[19] This goes in tune with broader critiques of surveillance culture, including the way John W. Whitehead compares NSA surveillance to Orwell's Nineteen Eighty-Four and warns against unchecked government data collection and the erosion of civil liberties.[20]

Although state and corporate surveillance in general is nowadays the more dominating debate, implications for cities are in no way less crucial. In this connection, Liesbet van Zoonen and others focus on privacy practices in smart cities. According to them, people are prepared to give more data when they feel that "something" is being done for their security. [21] However, Guillem Cladon-Clavell critically looks at current smart city initiatives in Europe for having totally ignored the issues of privacy and asks for transparency, data minimization, and accountability in the implementation of smart cities. [22] The critique thus aligns with the argument proposed by Raddivari Revathi, who refers to a strong regulatory authority that would implement this protection and uphold respect for individual autonomy against rapid technological development. [23]

The tension between the right to privacy and the need for surveillance is arguably best framed within the context of George Orwell's dystopian narrative examined by Paul Babbitt [24] and Whitehead. [25] Orwell's work provides a frame through which the erosion of privacy and individual freedom can be viewed in a world increasingly dominated by technologies of surveillance. The literature indicates that, today, privacy is not about the *"right to be left alone";* [26] rather, it has turned into a battle to restore lost autonomy and safeguard human dignity in an age of pervasive surveillance.

This discussion shows that smart city surveillance has both benefits, such as improving safety and efficiency, and risks, such as invading privacy of an individual. The next section will therefore explore whether the use of surveillance is a threat to privacy or a necessary tool for security, using examples and theoretical frameworks.

III. RISE OF SMART CITIES AND PRIVACY CONCERNS

The emergence of smart cities is driven by big data and the Internet of Things (IoT) which has the potential to completely transform urban life by enhancing safety, sustainability, and efficiency.[27] However, there are costs associated with this advancement, including increased surveillance and possible privacy risks. This raises the question of whether the advantages of improved public safety exceed any possible violations of individual liberty? Smart city surveillance technologies exceed the use of simple CCTVs. Advanced sensors, face recognition systems, and AI-powered analytics create an intricate web collecting real-time data on everything from traffic flow and environmental conditions to individual movements in public open spaces. This can also be very useful for emergency response, crime prevention, and resource optimization. [28]

Many cities in order to predict the occurrence of criminal activity are investing money in predictive policing, crowd control and real time crime mapping.[29] However, many of the same technologies that give assurances of efficiency and safety also pose serious privacy issues which is one of the most serious concerns affecting smart cities. [30].

IV. IMPORTANCE OF PRIVACY IN THE DIGITAL AGE

The Right to privacy had been in consideration as one of the fundamental rights for long, protecting basic dignity and self-determination of every individual human being. [31] During the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[32] this was confirmed as the Supreme Court of India continued to bring it under the ambit of the Right to Life and Liberty under Article 21 of the Constitution of India. This underlines the value of privacy not merely as a legal right, but also as an essential component of human life. The thoughts of

George Orwell's warnings of privacy in Nineteen Eighty-Four, interpreted by Paul Babbitt, focus on how constant surveillance can dehumanize people. [33]

The concept of privacy has developed over time as a result of various advances in philosophy and law. In response to emerging technologies that threatened the dignity of people, Warren and Brandeis described it as a "*right to be let alone*" in the United States in their 1890 article. [34] Privacy in English common law was earlier associated with physical places, as captured by the expression "an Englishman's house is his castle." [35] It came to extend to cover private communications and relationships. The discussion was further enriched when John Stuart Mill linked privacy with individual liberty and contended that it acts as a counterbalance to the abuse of state power and popular opinion. [36]

In this respect, it is conceived that privacy in smart cities faces unparalleled threats due to the pervasive integration of biometric scans, location tracking, and real-time video surveillance.[37] These new developments indeed offer convenience and security unlike ever before, but they create a virtual-material ecology reminiscent of panoptic control as described by Michel Foucault. [38] In such cases, residents may have been compelled by persistent threats of surveillance to monitor themselves so that they can remain out of view. It reminds one of the concept of Big Brother in Orwell's depiction whereby omnipresence of gaze from the superior authority reduces man's freedom and individuality. [39]

The concerns connected with these technologies, including as profiling, data breaches, and unauthorised monitoring, mirror Rathbone's critique of digital panopticism, in which algorithms and data analytics discreetly influence and govern individual behaviour, frequently without individuals' knowledge or consent.[40] Such concerns underscore the critical need for a strong privacy framework, especially in India, where a lack of comprehensive legal protections exacerbates these issues. With the extension of smart cities and deeply embedded digital technologies in urban life, innovation should go hand in hand with strong protection of privacy. [41] Understanding privacy as a right that is both historical and modern underlines its importance for the protection of human dignity, autonomy, and freedom in the face of rapid technological change.

Surveillance as a tool for public safety?

The advocates of surveillance in smart cities indicate the crucial role of this concept in bringing safety and security. According to them, responsible use of all types of surveillance technologies pays more benefits than risks. Some of them are listed below;

- **Crime deterrence and reduction:** One of the most important advantages of surveillance is that it prevents crimes from occurring. The public appearance of surveillance cameras would prevent potential offenders from committing crime. [42] For example, in London, the more general use of CCTV cameras contributes to a reduction in property crime and helps to tackle criminals more effectively by the police forces. [43] According to studies, it has been recorded that neighborhoods which have visible installations of CCTV also show lower rates of crime. [44]

- **Intelligent Traffic Management:** Surveillance technologies play a very important role in enhancing urban mobility. For example, Singapore has a high-tech network of surveillance cameras and sensors to monitor traffic conditions in real-time. [45] It enables the authorities to institute necessary congestion controls, traffic flow discipline, and minimizes accidents to keep transportation systems running smoothly with increased commuter safety.

- **Public Space Protection:** The surveillance systems in high-density areas keep the citizens safe from the occurrence of stampedes and other suspicious activities. For example, during the FIFA World Cup held in Qatar, advanced technology was

employed to survey the stadiums and fan zones in a bid to check on any potentially dangerous situation as quickly as possible to avoid accidents within crowds. [46]

- **Monitoring Public Safety Threats:** Advanced video surveillance systems now make it possible for authorities to trace out a potential threat to any particular sensitive area. For instance, in New York, the Domain Awareness System [47] will draw data from thousands of cameras installed around key locations in Times Square, subways, and airports and will put all such information before police officials for appropriate action to be initiated and taken forthwith to protect people against any form of attack.

Concerns about surveillance as a threat to privacy

While smart city surveillance is very helpful in many ways, it also raises several ethical and legal concerns. Critics have warned that this may undermine the privacy of individuals and create a culture of perpetual monitoring. Some of them are as follows;

- **Erosion of Privacy:** Continuous surveillance in public areas demolishes the notion of private life. In China, the wide range of installation of surveillance cameras along with facial recognition technologies has raised serious concerns about the lack of privacy among its citizens. A behavior-monitoring system, the Social Credit System very well exemplifies how such surveillance would affect the daily life of the people and repress other freedoms such as speech and assembly. [48]

- **Data Collection and Misuse:** Collection of such large amounts of data from smart city infrastructures imposes rather huge privacy risks. In 2021, a data breach was detected in Singapore's health database and compromised the sensitive medical information of 1.5 million residents. [49] Events of this nature again show very well how data from surveillance stands vulnerable to being misused for profiling and theft of identity.

- **Perpetuating Societal Discrimination:** Prejudices within these systems often propagate into the larger society because of their flawed training data. For example, it was suggested in studies that face recognition systems being used in the United States were less accurate for minority groups, which thus resulted in targeting them disproportionately and arresting them mistakenly. [50]

Balancing surveillance and privacy is critical for establishing confidence and promoting responsible technology use. Smart cities can address privacy concerns and improve security by incorporating measures such as transparency, supervision, and public interaction.

V. AN OVERVIEW OF SURVEILLANCE LAWS IN INDIA

The legal framework for surveillance in India is based upon a mix of laws enacted during the colonial era, recent judicial pronouncements, and new technologies.[51] These laws do allow the government to take such actions for the purpose of surveillance and interception of data, but they are certainly not fully equipped to handle the implications of advanced technologies, including artificial intelligence and biometric systems.

Legal Framework in India

The Indian Telegraph Act, 1885, provides interception on the grounds of urgency or public safety. But it is essentially ill-equipped to handle such sophisticated technologies as AI and facial recognition, due to its colonial legacy.

Similarly, Section 69 of the **Information Technology Act, 2000** allows for the interception or monitoring or decryption of digital information in the interest of public safety and national security. But without

judicial control, and with phrases such as "security of state" vaguely defined, there is a wide possibility for abuse.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016, enacted to ensure effective delivery of welfare, was converted into a tool of surveillance.[52] The Supreme Court, in the Puttaswamy Judgment (2017), restricted the use of Aadhaar and said that it should be lawful, necessary, and proportionate. [53] Yet, there is a fear that without proper safeguards, Aadhaar might be misused for profiling and tracking.

The Digital Personal Data Protection Act, enacted in 2023, seeks to control data processing through private enterprises, but it does little to limit the government's surveillance actions. [54] Section 7(c) of the aforementioned legislation authorizes nonconsensual processing to protect the state's sovereignty, integrity, public order, and security. These broad justifications remain ambiguous, thereby leaving opportunities for abuse. [55]

Surveillance systems in India Among a range of advanced surveillance tools, the country has used the NATGRID, CMS, and NETRA system to deal with security challenges. [56]

- **NATGRID** (National Intelligence Grid) [57] provides the law-enforcing agencies with immediate access to any information related to banks, railways, and even tax departments. Though highly effective for the strengthening of national security, the NATGRID works without any form of parliamentary sanction; it operates by mere government notifications and thus evades all necessary legal checks on privacy rights.

- **The Central Monitoring System** was introduced after the attacks in Mumbai in 2008 for the direct monitoring of calls, text messages, and even social networking sites. While there is no strict transparency and protection over the data, fear for misuse and mass surveillance thus creates a barrier.

- **NETRA,** or Network Traffic Analysis,[58] monitors Internet traffic, including encrypted messages, for specific keywords. Like CMS, it is also bereft of oversight mechanisms and susceptible to abuse.

The Delhi High Court recently addressed the privacy concerns with regard to these systems by issuing a direction for the suspension of mass data collection through those systems. The direction was issued following a Public Interest Litigation filed by CPIL contending that the lack of any independent oversight mechanism over such systems is in violation of the right to privacy of citizens. The PIL demanded the establishment of a regulatory body that would ensure that such systems are used legally with accountability. [59]

While the government justifies these systems as indispensable to national security, questions of transparency, accountability, and conformity with rights to privacy remain open. In this regard, only an independent oversight approach, clear legal definitions, and robust privacy safeguards can let such challenges be overcome so that the fundamental rights of the citizens are protected.

Gaps in India's Surveillance Framework

Surveillance laws in India are especially suffering from serious lacunae, thereby rendering citizens most vulnerable on questions of privacy. The recent landmark judgment of Puttaswamy (2017) declared privacy to be a fundamental right under Article 21 of the Constitution. Justice D.Y. Chandrachud laid down the three-fold test for intrusions into privacy:

- **Legality** - There should be an existence of a law authorizing the action.
- **Necessity** – The action must be necessary to achieve a legitimate state purpose.
- **Proportionality** – There must be a rational connection between the action and its objective, ensuring the intrusion is not excessive. [60]

While this judgment laid a very strong foundation for the protection of privacy, its principles are applied very inconsistently to the surveillance laws of India. Most of the existing frameworks do not meet these standards and are thus vulnerable to overreach.

It was for this reason that the Supreme Court and expert committees like the **Justice B.N. Krishna Committee**[61] from time to time laid emphasis on having an independent oversight mechanism for surveillance carried out by governments. Despite recommendations, there is no place in the DPDP Act of 2023 for the existence of any such body regulating surveillance activities.

This lack of oversight lets government agencies collect and use data disproportionately, without checks and balances. As such, the citizens remain exposed to the potential misuses of the surveillance systems, and that urgently calls for reforms that ensure accountability and protection of fundamental rights.

Need for Policy Reform

With growing concerns over surveillance, India needs a comprehensive legal and policy framework that:

- Ensure accountability and oversight, through independent review and judicial oversight of activities related to surveillance, in order to prevent abuse.
- Balance security with respect for privacy through enforcing clear regulations that establish the necessity of proportionality inherent in the pursued goal.
- Safeguard citizen rights by making data collection transparent and giving full power to the individuals over their personal information.
- Implement best international practices in law, such as the GDPR, which would afford better legal protection and support the ethical and responsible practice of surveillance.

VI. CONCLUSION

The existing safeguards to privacy in India, like judicial oversight and limited provisions under the mentioned laws, are ineffective against the modern-day challenges created by advanced technologies of surveillance. Judicial pronouncements, most importantly the landmark Puttaswamy judgment, have emphatically captured the spirit of privacy as a fundamental right. However, the legislative frameworks have not kept pace with changes in technology, resulting in huge lacunas in the protection of individual freedoms.

While surveillance can be viewed as a means for public safety, the fact that it is being implemented without proper legal safeguards and oversight creates a serious threat to privacy. Therefore, updating the legal frameworks of India is of essence to ensure a proper balance between security and privacy, so that the rights of its citizens are protected against emerging surveillance technologies.

REFERENCES

1. 'Smart Cities Cannot Be Surveillance Cities' (Bridging Barriers, 30/11/24) https://bridgingbarriers.utexas.edu\
2. 'Smart City Technologies for Urban Safety' https://www.trigyn.com/
3. Bischoff P, 'Data Privacy Laws & Government Surveillance by Country' (Comparitech, 15 October 2019) https://www.comparitech.com
4. S S, 'India Ranked Third Worst For Data Privacy In Global Surveillance Index' (Inc42 Media, 17 October 2019) https://inc42.com/buzz/
5. 'What Are the Surveillance Laws in India?' (The Hindu, 30 November 2024) https://www.thehindu.com
6. Pavithran K, 'Right to Privacy - Pegasus Spyware' (2024) 5 International Journal of Research Publication and Reviews 5541. https://ijrpr.com/uploads
7. (2017) 10 SCC 1., also see 'Fundamental Right to Privacy' (Supreme Court Observer) https://www.scobserver
8. '10 Central Agencies Can Now Snoop on "Any" Computer They Want' The Economic Times (21 December 2018) https://economictimes.in

9. Roessler B and DeCew J, 'Privacy' in Edward N Zalta and Uri Nodelman (eds), The Stanford Encyclopedia of Philosophy (Winter 2023) https://plato.stanford.edu/
10. Acharya B, 'The Four Parts of Privacy in India' (2015) 50 Economic and Political Weekly 32 https://www.jstor.org/stable/24482489\
11. Bhatia G, 'State Surveillance and the Right to Privacy in India: A Constitutional Biography' (2014) 26 National Law School of India Review 127 https://www.jstor.org/stable/44283638
12. Tarafder A, 'Surveillance, Privacy and Technology: A Comparative Critique of the Laws of USA and India' (2015) 57 Journal of the Indian Law Institute 550 https://www.jstor.org/stable/44782800
13. Amalia Berggren, 'Surveillance in Nineteen Eighty-Four: The Dismantling of Privacy in Oceania' (BA Thesis, Karlstad University 2016).
14. Boyle J, 'Foucault In Cyberspace: Surveillance, Sovereignty, And Hardwired Censors' 66 University of Cincinnati Law Review 177.
15. Ibid
16. Rathbone M, 'Panopticism, Impartial Spectator and Digital Technology' (2022) 22 Indo-Pacific Journal of Phenomenology 1 http://www.scielo.org.za/
17. Bhandari V, 'Privacy Concerns in the Age of Social Media' (2018) 45 India International Centre Quarterly 66 https://www.jstor.org/stable/45129854
18. Srivastava S, 'India: Decrypting Critical Concepts under India's Digital Personal Data Protection Act, 2023 and Comparison with GDPR and PIPL' (IJLT, 20 March 2024) https://www.ijlt.in/post/
19. Angela C Henderson, Sandra M Harmon, and Jeffrey Houser, 'A New State of Surveillance? Applying Michel Foucault to Modern Motherhood' University of Northern Colorado
20. Whitehead JW, 'Orwell Revisited: Privacy in the Age of Surveillance' (Progressive.org, 24 June 2013) https://progressive.org/
21. Van Zoonen L and others, 'Privacy Behavior in Smart Cities': (2022) 3 International Journal of Urban Planning and Smart Cities 1 https://services.igi
22. Galdon-Clavell G, '(Not so) Smart Cities?: The Drivers, Impact and Risks of Surveillance-Enabled Smart Environments' (2013) 40 Science and Public Policy 717 https://academic.oup.com/
23. Raddivari Revathi, 'Evolution of Privacy Jurisprudence – A Critique' (2018) 60(2) Journal of the Indian Law Institute 189 https://www.jstor.org/stable/10.2307/26826635
24. Babbitt P, 'Orwell and the Value of Privacy' (Southern Arkansas University 2015)
25. Supra note 20
26. Sloot BVD, 'The Right to Be Let Alone by Oneself: Narrative and Identity in a Data-Driven Environment' (2021) 13 Law, Innovation and Technology 223 https://www.tandfonline.com/
27. Taaffe O, 'Are Smart Cities a Threat to Personal Privacy?' (Raconteur, 5 September 2022) https://www.raconteur.net/
28. Majid A, 'Security and Privacy Concerns over IoT Devices Attacks in Smart Cities (2022)' (2023) 11 Journal of Computer and Communications 26 https://www.scirp.org/journal/paperinformation?paperid=122582
29. 'Surveillance and Predictive Policing Through AI | Deloitte' https://www.deloitte.com
30. Johnson A, 'Balancing Privacy and Innovation in Smart Cities and Communities' (2023) https://itif.org/publication
31. Supra note 7
32. (2017) 10 SCC 1
33. Supra note 24
34. Warren and Brandeis, "The Right to Privacy" https://groups.csail.mit.
35. Is "An Englishman's Home Is His Castle" (Adam Smith Institute) https://www.adamsmith.org
36. Ebeling R, 'Private Property: The Missing Link in John Stuart Mill's Defense of Liberty | Online Library of Liberty' https://oll.libertyfund.org
37. Amos Z, 'Are Smart Cities a Threat to Data Privacy? | HackerNoon' https://hackernoon.com
38. Supra note 16
39. The Timeless Relevance of "1984": How George Orwell's Dystopia Mirrors Today's World' (Times Now, 22 April 2024) https://www.timesnownews.com/
40. Supra note 16

41. Booth D, 'The Challenges Smart Cities Face With Video Surveillance' (BCD, 19 December 2022) https://www.bcdvideo.com/
42. Jha R, 'Surveillance Cameras in Cities: A Threat to Privacy?' (Orfonline.org, 30 November 2024) https://www.orfonline.org/expert-speak/surveillance-cameras-in-cities-a-threat-to-privacy
43. Gerell M, 'CCTV in Deprived Neighbourhoods – a Short-Time Follow-up of Effects on Crime and Crime Clearance' (2021) 22 Nordic Journal of Criminology 221 doi/10.1080/2578983X.2020.1816023
44. East SS, 'Does Having CCTV Reduce Crime?' (Scutum South East, 18 November 2022) https://www.scutumsoutheast.co.uk/
45. Kumar S, 'Singapore Smart Traffic System Is Redefining Urban Mobility' (12 November 2024) https://www.intellistride.com
46. Disaster K, 'FIFA World Cup 2022: A Case Study of Traffic and Crowd Management in Qatar' (Knowdisaster, 24 June 2023) https://knowdisaster.com/
47. 'New York's Domain Awareness System: Every Citizen Under Surveillance, Coming to a City Near You' (North Carolina Journal of Law & Technology) https://journals.law.unc.edu/ncjolt
48. Codings, 'China's social credit system' https://orcasia.org/chinas-social-credit-system
49. 'Singapore Personal Data Hack Hits 1.5m, Health Authority Says' (20 July 2018) https://www.bbc.com/
50. Louter L, 'Racial Bias in Facial Recognition Algorithms' (Amnesty International Canada, 21 March 2023) https://www.amnesty.ca/
51. Supra note 5
52. Henne K, 'Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India' in Blayne Haggart, Kathryn Henne and Natasha Tusikov (eds), *Information, Technology and Control in a Changing World* (Springer 2019) https://doi.org/10.1007/978-3-030-14540-8_11
53. Supra note 7
54. Supra note 18
55. Ibid
56. 'Right to Privacy & Legitimate State Interest' (Drishti IAS) https://www.drishtiias.com/
57. Haritha D and Praneeth Ch, 'National Intelligence Grid — An Information Sharing Grid', 2017 ICAMMAET https://ieeexplore.ieee.org/document/8186674
58. 'Project NETRA - The Indian Internet Surveillance' (Cyber Defense Magazine, 8 January 2014) https://www.cyberdefensemagazine.com/
59. 'No Blanket Permission given for Surveillance under NETRA, NATGRID: Centre to HC' *The Economic Times* (5 February 2021) https://economictimes.in
60. AK A, 'Proportionality Test for Aadhaar: The Supreme Court's Two Approaches' (Bar and Bench, 26 September 2018) https://www.barandbench.com
61. 'Justice BN Srikrishna Committee Submits Data Protection Report' (Drishti IAS) https://www.drishtiias.com/