Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Global Surveillance and Privacy Rights

Article History:

Name of Author:
Felicia Adkins[1] and Jessica Baker[2] and Roberta Harvey[3]

Affiliation: [1]Associate Professor, Faculty of Business Studies, Università di Nova, Kenya
[2]Associate Professor, Faculty of Accounting and Finance, Nairobi Metropolitan University, Kenya
[3]Dean of Commerce, Department of Marketing, Oceanic Research University, Kenya
Corresponding Author: Felicia Adkins

How to cite this article: Felicia Adkins, *et, al*. Global Surveillance and Privacy Rights. *J Community Med* 2021;2(1);49-51.

Abstract: As digital surveillance technologies evolve at an unprecedented pace, nations and corporations are deploying increasingly advanced systems to monitor, analyze, and predict human behavior. In 2025, this rapid expansion presents profound challenges to privacy, civil liberties, and democratic governance. This article critically examines the intersection of global surveillance practices and privacy rights, tracing their evolution through international human rights law, emerging technologies, and national regulatory responses. It explores key developments such as the rise of AI-powered analytics, biometric tracking, cloud-based monitoring, and smart city integration, alongside the expansion of surveillance markets, notably in Asia-Pacific and North America. Through comparative analysis of privacy legislation—such as the EU's GDPR, India's Digital Personal Data Protection Act, and U.S. state laws—the article highlights principles of consent, data minimization, breach notification, and the right to erasure. It also discusses contemporary controversies, including surveillance capitalism, algorithmic bias, and the disproportionate impact of monitoring on vulnerable populations. The article concludes by offering a framework for harmonizing privacy and security through international cooperation, privacy-enhancing technologies, and robust legal oversight to ensure accountability and preserve fundamental freedoms in a data-driven world.

Keywords: Global surveillance, digital privacy, right to privacy, surveillance technology, GDPR, DPDPA India, AI surveillance, facial recognition, predictive policing, data protection laws, human rights,

INTRODUCTION

Surveillance practices have expanded globally in tandem with technological innovation and the push for digitization. From public safety to national security, governments and corporations have adopted increasingly sophisticated surveillance tools, often tipping the balance between collective safety and individual privacy. This research article analyzes the evolution, scale, regulatory frameworks, and ongoing debates regarding global surveillance and privacy rights in 2025.

1. INTERNATIONAL PRIVACY RIGHTS: LEGAL AND NORMATIVE FRAMEWORKS

- **Universal Recognition**: The right to privacy is embedded in foundational human rights instruments, including the Universal Declaration of Human Rights (UDHR, Article 12) and the International Covenant on Civil and Political Rights (ICCPR, Article 17), which state that no one shall be subject to arbitrary or unlawful interference with their privacy, and everyone deserves legal protection against such intrusions[1].
- **Regional Enforcement**: Rights are reinforced by regional conventions, such as the European Convention on Human Rights (Article 8) and the American Convention on Human Rights (Article 11).
- **Digital Age Evolution**: UN resolutions since 2013 recognize that digital surveillance presents new threats to privacy, urging states and companies to uphold legality, necessity, and proportionality in data collection and monitoring[1][2].

2. Contemporary Surveillance: Global Expansion and New Technologies

2.1 Growth of Surveillance Markets

- The global video surveillance market reached $57.96billion in 2025, driven by urban expansion, smart city initiatives, and security concerns, with Asia Pacific leading market growth[3].
- Governments and enterprises have invested heavily in IP (internet protocol) surveillance, advanced edge computing, and cloud-based monitoring—enabling real-time, remote access and analysis of vast datasets[4][3].
- The market is projected to reach $88.71billion by 2030, reflecting a CAGR of 8.5% from 2025 to 2030[3].

2.2 Technological Innovations

- **Artificial Intelligence (AI)**: Automated threat detection, facial recognition, behavioral analytics, predictive policing, and anomaly detection have become mainstream in surveillance systems[5][4].
- **Internet of Things (IoT)**: Integration of cameras, sensors, and access control systems supports widespread, interconnected monitoring.
- **Edge Computing & Analytics**: Localized AI processing on devices reduces latency, enabling faster detection and privacy challenges[4].
- **Hybrid & Cloud Storage**: Enhanced scalability and security for data retention and analysis[4].
- **Mobile Surveillance Units**: Portable monitoring solutions are becoming common for temporary events and remote sites[6].

[image:1]

Figure 1: Key Technology Trends in Global Surveillance, 2025

3. THE SCOPE AND IMPACT OF MODERN SURVEILLANCE

3.1 Global Scale and Penetration

- Massive deployments: China leads with hundreds of millions of surveillance cameras and ambitious facial recognition programs; the U.S., U.K., and India have rapidly increased urban surveillance coverage[3].
- **Expansion into private sector**: Retail, finance, health, and transport increasingly rely on real-time monitoring for security and operational efficiency[7][3].
- **Smart Cities**: Surveillance is foundational in smart city infrastructure, but raises profound questions about privacy vs. safety[3].

3.2 Impact on Human Rights

- Digital surveillance poses significant risks to autonomy and expression. Intrusive practices—such as unauthorized mobile tracking, biometric analysis, and digital ID monitoring—have led to chilling effects on free speech, association, and personal freedom[7][8][2].
- Notable abuses: Spyware tools like Pegasus have enabled states to monitor dissidents, activists, and journalists, violating privacy and sometimes endangering lives[7][2].

4. LEGAL AND REGULATORY RESPONSES: 2025 DEVELOPMENTS

4.1 Global Legislative Trends

- **India**: Enacted the Digital Personal Data Protection Act (DPDPA, July 2025), introducing notice, consent, limited retention, breach notification, and steep fines for violations[9].
- **United States**: Fourteen states now have comprehensive privacy laws; six more take effect in 2025-2026, giving residents rights to access, delete, or object to personal data processing[10].
- **Europe**: The General Data Protection Regulation (GDPR) remains highly influential, with ongoing updates and new AI regulations to address surveillance in digital ecosystems[11].
- **Quebec**: Canada's Law 25 (in force 2025) expands privacy protections and breach notifications[9].

[image:2]

Figure 2: Comparative Global Privacy Legislation (2025)

4.2 Key Principles and Rights

Principle	Definition	Example Jurisdictions
Consent & Notice	Informed opt-in required for data collection	EU (GDPR), India (DPDPA)
Data Minimization	Limit on data type/amount collected	EU, US (state laws)
Breach Notification	Mandatory prompt reporting of data breaches	EU, Canada, India
Purpose Limitation	Data used only for specified purposes	EU, India

Right to Erasure/Opt-out	Users may delete data or object to profiling	EU, US, India

Table 1: Major Regulatory Principles in 2025

4.3 Ongoing Enforcement and Litigation

- Record fines have been levied for unauthorized surveillance and violations of privacy policies.
- Courts have recognized the need for warrants and legal safeguards for digital data access (Carpenter v. United States, US Supreme Court, 2018), and have mandated privacy assessments for large-scale monitoring programs[8].

5. Current Challenges and Controversies

- **Legal Fragmentation**: No unified global standard exists; compliance and enforcement vary by jurisdiction[9][10].
- **Advances vs. Rights**: Predictive analytics and large-scale monitoring increase security but risk disproportionate intrusions and discrimination[7][5].
- **Surveillance Capitalism**: Corporate data harvesting by major tech firms is under scrutiny; tracking via cookies, device fingerprinting, and behavioral targeting is facing mounting regulation[11].
- **Digital Divide and Bias**: Surveillance often disproportionately targets marginalized groups and raises concerns about algorithmic bias and social inequality[7][8].

[image:3]

Figure 3: Privacy Risks Associated with Surveillance and Data Collection

6. Pathways Forward and Future Trends

6.1 Harmonizing Privacy and Security

- Stronger oversight of state and corporate surveillance through independent regulatory bodies and transparency requirements.
- Calls for international standards, adoption of UN and OECD guidelines, and data protection authorities to monitor cross-border data flows[1][12].
- Privacy-by-design approaches in surveillance technology development.

6.2 Technological Countermeasures

- Encryption, anonymization, and AI-ethics auditing tools for users to protect privacy.
- Privacy-enhancing technologies (PETs) like zero-knowledge proofs and federated learning growing in adoption.

6.3 Policy Recommendations

- Establishing baseline global privacy standards, tailored national regulations, and consistent enforcement.
- Continuous update of legal frameworks to respond to emerging technologies (e.g., edge AI, deepfake detection).
- Promoting public awareness and digital literacy to empower users against unwarranted surveillance.

CONCLUSION

As surveillance technologies proliferate and privacy becomes a top-tier policy concern, the world is witnessing an urgent re-negotiation of what it means to be safe, free, and private in the digital age. Legal and technological advances have created pathways to harmonize surveillance for public good with the safeguarding of civil liberties—yet persistent gaps in regulatory harmonization and technological overreach remain major challenges. Going forward, collaboration between states, corporations, and civil society will be essential to defend privacy rights, foster innovation responsibly, and ensure democratic values in a surveilled society.

[image:1]
[image:2]
[image:3]

REFERNCES

1. https://polioeradication.org/global-polio-surveillance-action-plan-2025-2026-2/
2. https://www.marketsandmarkets.com/Market-Reports/video-surveillance-market-645.html
3. https://www.ciol.com/tech/top-five-e-surveillance-trends-shaping-the-tech-landscape-by-2025-8595282
4. https://bigid.com/blog/2025-global-privacy-ai-and-data-security-regulations/
5. https://gchragd.org/wp-content/uploads/2023/06/GCHRAGD-SURVEILLANCE-AND-HUMAN-RIGHTS-background-paper.pdf
6. https://ecam.com/security-blog/top-security-technology-trends-to-watch-in-2025
7. https://kustomsignals.com/blog/89-7-billion-global-video-surveillance-by-2025
8. https://www.ohchr.org/en/special-procedures/sr-privacy/international-standards
9. https://polioeradication.org/wp-content/uploads/2025/01/Global-Polio-Surveillance-Action-Plan-2025-2026.pdf
10. https://www.who.int/initiatives/global-influenza-surveillance-and-response-system

11. https://www.globalsurveillance.eu
12. https://www.nyulawglobal.org/globalex/right_to_privacy_international_perspective.html