INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 2 [2025] | Page 271 - 280

RIGHT TO PRIVACY AND THE EXPANDING SCOPE OF SURVEILLANCE

-Mohini Tripathi[1]

ABSTRACT

The right to privacy stands as a fundamental pillar of democratic societies, yet it is increasingly challenged by the expansion of surveillance in the digital age. From mass data collection by governments to pervasive tracking by corporations, modern surveillance has blurred the lines between security and intrusion. This article critically examines the legal foundations of the right to privacy and traces the evolution of surveillance from traditional observation to sophisticated digital ecosystems. It analyzes responses by various jurisdictions, with a focus on the United States, the European Union, and India, and explores the role of civil society and technology in preserving privacy. In light of rising authoritarian practices and corporate overreach, the article argues for a multidimensional strategy encompassing legal reform, international cooperation, and ethical technology design to protect the right to privacy. The article concludes that privacy must be re-framed as both a legal right and a societal imperative in the face of expanding surveillance.

INTRODUCTION

The rise of digital technology has triggered a profound transformation in how information is collected, analyzed, and disseminated. While this has improved efficiency and connectivity, it has simultaneously eroded individuals' ability to maintain privacy. Surveillance, once a targeted and labor-intensive endeavor, has evolved into an omnipresent infrastructure that is often silent and invisible. The digital footprint of nearly every human interaction search queries, social media usage, biometric data, Geo location history is now potentially accessible to governments and corporations alike.

Privacy is not merely a personal concern; it underpins democratic participation, autonomy, and the rule of law. It ensures that individuals can think, communicate, and associate freely without

[1] X Semester BBA LLB (H), Babasaheb Bhimrao Ambedkar University, Lucknow.

unwarranted observation. In liberal democracies, privacy is essential for the functioning of a pluralistic society where dissent, diversity, and innovation can flourish without fear of retaliation. However, it faces existential threats from both state actors seeking national security and corporations pursuing economic gain through data monetization. The power imbalance between data subjects and data controllers has led to asymmetries that risk reducing individuals to mere data points. This article examines how legal systems have responded to this challenge and proposes mechanisms for protecting privacy in a surveillance-saturated environment.

CONCEPTUALIZING THE RIGHT TO PRIVACY

Privacy is a complex, multifaceted concept encompassing bodily integrity, informational autonomy, decisional freedom, and spatial seclusion. It allows individuals to control how their personal data is accessed, shared, and used. Legally, the modern recognition of privacy began with the landmark 1890 article by Samuel D. Warren and Louis D. Brandeis, defining it as "the right to be let alone."[2] This articulation emerged as a response to the encroachment of mass media into personal lives, and it laid the foundation for future privacy jurisprudence.

At the international level, the Universal Declaration of Human Rights (UDHR) recognizes in Article 12 that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."[3] Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides for protection against unlawful or arbitrary interference.[4] The European Convention on Human Rights (ECHR) guarantees privacy under Article 8, emphasizing respect for private and family life.[5] These provisions underscore the universal importance of privacy as a human right.

However, privacy is not absolute. Courts and legislatures have allowed reasonable restrictions in pursuit of legitimate aims, such as national security and public order. The challenge lies in maintaining proportionality and oversight in an era where surveillance is constant and largely invisible. The lack of transparency in surveillance operations often undermines public trust and accountability, necessitating stronger legal safeguards. Moreover, privacy must evolve to address

2 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

3 Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810, art. 12 (1948).

4 International Covenant on Civil and Political Rights, Dec. 16, 1966, art. 17, 999 U.N.T.S. 171

5 European Convention on Human Rights, Nov. 4, 1950, art. 8, 213 U.N.T.S. 221

the implications of emerging technologies such as biometric recognition, neural interfaces, and quantum computing each with the potential to redefine the very boundaries of private life.

THE EVOLUTION OF SURVEILLANCE

A. FROM PHYSICAL SURVEILLANCE TO THE DIGITAL PANOPTICON

Surveillance has undergone a seismic shift. In the past, surveillance required substantial resources and was constrained by physical limitations. Today, the digital age has introduced "surveillance" the continuous tracking of individuals through digital footprints. Governments and corporations increasingly rely on data analytics, artificial intelligence, and pervasive connectivity to monitor individuals at unprecedented scales.

This transformation is typified by three overlapping forms:

MASS SURVEILLANCE

Post-9/11 security frameworks empowered intelligence agencies to monitor communications at scale. Edward Snowden's disclosures in 2013 revealed the NSA's PRISM program, which collected data from major tech companies without individualized warrants.[6] This surveillance included phone metadata, emails, and online chats, affecting both American citizens and foreign nationals. The lack of transparency and judicial oversight raised concerns about constitutional rights and democratic accountability.

CORPORATE SURVEILLANCE

Major technology companies engage in systematic data mining to monetize user behavior. These companies track browsing habits, search queries, app usage, and even offline behavior through IoT devices. Shoshana Zuboff characterizes this phenomenon as "surveillance capitalism," wherein human experience is rendered into behavioral data for profit.[7] Targeted advertising, algorithmic recommendations, and behavioral nudging further entrench corporate influence in

6 Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (2014).

7 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power(2019).

personal lives. This commodification of personal data raises profound questions about digital consent, autonomy, and power asymmetry.

PREDICTIVE SURVEILLANCE

AI and big data have enabled predictive policing, risk assessments, and algorithmic decision-making. Law enforcement agencies now use tools to forecast potential criminal activity based on behavioral patterns.[8] Similarly, financial institutions, employers, and insurers rely on algorithms to assess individuals. These systems, however, frequently lack transparency and can perpetuate existing biases, leading to unjust outcomes.

LEGAL RESPONSES TO SURVEILLANCE

A. UNITED STATES

The Fourth Amendment protects against unreasonable searches and seizures, yet jurisprudence struggled for decades with adapting to technological realities. In *Carpenter v. United States*, the Supreme Court ruled that accessing historical cell-site location information requires a warrant, recognizing that individuals have a legitimate expectation of privacy in digital data.[9] This decision marked a significant step in extending constitutional protections to the digital realm.

Nonetheless, significant surveillance persists under the Foreign Intelligence Surveillance Act (FISA) and related programs, with limited public oversight. The lack of a comprehensive federal data protection statute creates a patchwork of sector-specific rules. The California Consumer Privacy Act (CCPA) represents one of the most robust state-level efforts.[10] However, uniform protections across the country remain lacking.

B. EUROPEAN UNION

The GDPR, adopted in 2018, establishes a robust framework for data protection.[11] It mandates transparency, user consent, and accountability, with heavy penalties for violations. The CJEU has also played a pivotal role, striking down data transfer agreements with the U.S. in the *Schrems*

8 Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (2017).

9 Carpenter v. United States, 138 S. Ct. 2206 (2018).

10 California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 (West 2023).

11 Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1 (General Data Protection Regulation).

I and *Schrems II* decisions due to insufficient safeguards for EU citizens.[12] Additionally, the *Digital Rights Ireland* case invalidated blanket data retention laws, reinforcing privacy as a fundamental right.[13]

C. INDIA

In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court of India declared privacy a fundamental right under Article 21.[14] This led to increased scrutiny of the Aadhaar biometric ID program and calls for a data protection framework. Despite the 2023 Digital Personal Data Protection Act, concerns remain regarding broad exemptions granted to the state.[15] Civil society groups argue for stronger safeguards and independent oversight.

CASE STUDIES IN SURVEILLANCE AND PRIVACY

A comparative study of notable global surveillance incidents reveals the scale, complexity, and implications of modern surveillance regimes:

A. THE PEGASUS SPYWARE SCANDAL

The Pegasus spyware incident was a watershed moment in global digital rights discourse. Pegasus, developed by the Israeli firm NSO Group, allows remote and covert access to mobile devices. The 2021 revelations indicated that this tool had been used to surveil journalists, human rights defenders, and political figures across more than 40 countries. In India, the spyware allegedly targeted opposition leaders, journalists, and civil society members. The Supreme Court of India appointed an independent technical committee to investigate these claims, citing potential violations of the *Puttaswamy* judgment[16] on privacy.

This case underlined the inadequacy of legal protections in preventing state abuse of surveillance tools. The lack of transparency regarding surveillance authorization mechanisms continues to threaten democratic freedoms.

12 Schrems I, Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015).

13 Schrems II, Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (July 16, 2020).

14 Digital Rights Ireland Ltd. v. Minister for Communications, Joined Cases C-293/12 & C-594/12, ECLI:EU:C:2014:238.

15 The Digital Personal Data Protection Act, No. 22 of 2023 (India)

16 (2017) 10 SCC 1

B. SNOWDEN REVELATIONS AND THE NSA (UNITED STATES)

Edward Snowden's disclosures in 2013 exposed mass surveillance operations by the U.S. National Security Agency (NSA), including programs like PRISM, XKeyscore, and Tempora. These programs collected vast amounts of data from individuals, often without warrants, using partnerships with major tech companies. While proponents cited national security, critics highlighted constitutional infringements and lack of oversight. The revelations sparked global outrage and led to the USA FREEDOM Act (2015), which limited bulk metadata collection [(Carpenter v. United States, 138 S. Ct. 2206 (2018))].

Yet many reforms remain superficial, and significant surveillance practices persist under the Foreign Intelligence Surveillance Act (FISA), often operating in secrecy with minimal external checks.

C. CAMBRIDGE ANALYTICA AND FACEBOOK DATA SCANDAL

In 2018, it emerged that Cambridge Analytica harvested data from over 87 million Facebook users without consent, using personality tests and app permissions to profile and target voters. The scandal highlighted the dangers of corporate surveillance and its manipulation for political ends impacting major democratic events like Brexit and the 2016 U.S. presidential election. Investigations by the U.K.'s Information Commissioner's Office and U.S. Congress triggered public debate around consent, platform accountability, and algorithmic governance [(Regulation (EU) 2016/679)].

This incident accelerated regulatory push back in the form of stronger data protection laws and scrutiny over tech monopolies.

D. AADHAAR AND BIOMETRIC DATA COLLECTION (INDIA)

India's Aadhaar projecta unique biometric identification system was introduced to improve public welfare delivery. However, it also raised significant concerns regarding state surveillance, exclusion due to authentication failures, and potential data breaches. In *Puttaswamy II*,[17] the Indian Supreme Court upheld the program's constitutionality but restricted its use beyond welfare schemes. The

17 (2018) 10 SCC 1

judgment emphasized that Aadhaar could not be made mandatory for private services such as banking or telecommunications.

Despite judicial scrutiny, questions remain about the implementation, oversight, and centralized storage of biometric data. Activists continue to push for more robust data protection mechanisms and independent regulators.

E. CHINA'S SOCIAL CREDIT SYSTEM

China's social credit system integrates government and corporate data to assign scores to individuals and businesses. These scores affect access to services, job opportunities, loans, and even travel. The system functions as a tool for enforcing conformity and punishing dissent, raising serious human rights concerns. While still in pilot phases in some regions, it illustrates the dangers of an all-encompassing surveillance infrastructure [(Creemers, R., 2018)].

China's model poses a challenge to liberal democracies, demonstrating how surveillance can be normalized and institutionalized without adequate redress mechanisms.

F. UNITED KINGDOM'S CCTV AND FACIAL RECOGNITION

The U.K. has one of the highest densities of CCTV cameras in the world. Facial recognition technology, trialed by police departments, faced backlash over racial bias and privacy violations. In *R (Bridges) v. Chief Constable of South Wales Police*,[18] the Court of Appeal ruled that automated facial recognition lacked a clear legal basis and failed to comply with the Human Rights Act.

The judgment was a landmark victory for privacy advocates, reinforcing the necessity of legal clarity and proportional safeguards in the deployment of biometric technologies.

G. GOOGLE STREET VIEW DATA COLLECTION SCANDAL

In 2010, Google admitted that its Street View cars had inadvertently collected personal data from unsecured Wi-Fi networks. The incident sparked investigations by regulators in Canada, Germany, and the U.S., leading to fines and policy changes. The Federal Communications Commission

18 (2020) EWCA Civ 1058

(FCC) found that Google had violated data protection norms but imposed minimal penalties, raising questions about the enforcement powers of regulatory bodies [(FCC, DA 12-592)].

This case illustrated how unregulated corporate data practices can lead to significant privacy breaches even without malicious intent.

SURVEILLANCE AND DEMOCRACY

Surveillance has a chilling effect on democratic processes. It creates an atmosphere of fear and caution, leading individuals to self-censor their speech, suppress activism, and disengage from political life. This "chilling effect" has been documented across contexts from the United States post-Snowden to Hong Kong amid pro-democracy protests.[19]

In authoritarian regimes, surveillance facilitates repression. In Iran, Belarus, and Russia, digital monitoring is used to identify protesters and suppress dissent.[20] Even in democratic societies, governments have used mass surveillance to monitor climate activists, labor unions, and religious minorities. Tools like facial recognition and predictive policing risk reinforcing systemic biases, especially against already marginalized groups.[21]

Furthermore, algorithmic targeting by corporations undermines informed political discourse. Micro targeted ads and misinformation campaigns manipulate voter behavior without transparency or accountability. The economic incentives of surveillance capitalism clash directly with the public good, privileging profit over participatory democracy.[22]

A democracy that tolerates unchecked surveillance risks devolving into a surveillance state where citizens are viewed not as rights-bearing individuals but as data points to be monitored, managed, and manipulated.[23]

THE ROLE OF CIVIL SOCIETY AND TECHNOLOGY

19 PEN America, Global Chilling: The Impact of Mass Surveillance on International Writers (2016), https://pen.org/report/global-chilling/.

20 U.N. Human Rights Committee, General Comment No. 34, U.N. Doc. CCPR/C/GC/34 (2011).

21 R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058 (UK); Andrew Guthrie Ferguson, The Rise of Big Data Policing (2017).

22 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019)

23 Julie E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice (2012).

Civil society plays a crucial role in resisting the normalization of surveillance. Organizations like the Electronic Frontier Foundation (EFF), Access Now, and Privacy International have spearheaded advocacy, litigation, and education efforts.[24] They've challenged laws permitting bulk data collection, filed amicus briefs in key cases, and published transparency reports that hold both governments and corporations accountable.

Strategic litigation has yielded notable victories, such as the invalidation of mass data retention laws in the EU[25] and limitations on predictive policing in the U.S.[26] In India, civil society was pivotal in the *Puttaswamy* litigation, with lawyers, academics, and activists contributing to the jurisprudential recognition of privacy as a fundamental right.[27]

At the same time, technology can offer tools to protect privacy:

1. Decentralized Social Networks: Platforms like Mastodon provide alternatives to data-harvesting giants like Facebook. These open-source models prioritize user control and transparency.
2. Data Minimization Tools: Services like Duck Duck Go and Start page allow anonymous browsing and prevent behavioral profiling.
3. Secure Communication: Innovations in zero-knowledge proofs, homomorphic encryption, and multi-party computation are expanding the frontiers of secure and private data handling.

However, technological solutions alone cannot suffice. Many privacy-enhancing technologies are inaccessible to non-technical users. Moreover, when governments legislate to weaken encryption or mandate data localization, they can undermine these tools. Thus, legal protections must accompany technological innovations.

RE-IMAGINING PRIVACY: A WAY FORWARD

The future of privacy requires collective re-imagination. Legal frameworks must evolve alongside technological capabilities. The path forward includes:

24 Electronic Frontier Foundation, About EFF, https://www.eff.org/about (last visited May 1, 2025)

25 Digital Rights Ireland Ltd. v. Minister for Commc'ns, Joined Cases C-293/12 & C-594/12, ECLI:EU:C:2014:238

26 Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (2017)

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

- ❖ Inter-sectional Privacy Policy: Laws must consider the differential impact of surveillance on gender, race, class, and ability. Inclusive policy making ensures equitable protections.[28]
- ❖ Stronger Global Governance: Just as climate change requires cross-border coordination, so does privacy. International data protection treaties, modeled after GDPR, should be developed under UN or OECD frameworks.[29]
- ❖ Rights-based Tech Design: Developers must be educated in ethical design principles. Privacy should be a core module in engineering curricula. Product development must include impact assessments and diverse stakeholder consultation.[30]
- ❖ Whistleblower Protections: As Snowden's case illustrates, insiders play a key role in exposing abuses. Stronger legal protections and support systems for whistleblowers can enhance transparency.[31]
- ❖ Digital Constitutionalism: Citizens should have enforceable digital rights including the right to anonymity, data portability, and algorithmic transparency. These rights must be justifiable and embedded into constitutional or quasi-constitutional frameworks.[32]

CONCLUSION

The digital age has brought unprecedented capabilities to collect, analyze, and exploit personal data. While surveillance is sometimes justified for legitimate state objectives, its unchecked expansion jeopardizes core democratic and human values. The right to privacy must be re-conceptualized not merely as a defense against intrusion but as a proactive shield that empowers individual autonomy and democratic participation.

Privacy is foundational to human dignity. In an era where every click, movement, and word can be tracked, defending privacy is defending freedom itself. The law must evolve to meet the realities of the digital age, but so too must public consciousness. Through legal reform, ethical innovation, civic engagement, and international solidarity, privacy can be preserved not as a relic of the past, but as a right fit for the future.

28 Julie E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice (2012).

29 Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1; Inter-Am. Comm'n H.R., Privacy and Freedom of Expression in the Americas, OEA/Ser.L/V/II. Doc. 34 (2013).

30 Solon Barocas & Helen Nissenbaum, Big Data's End Run Around Procedural Privacy Protections, 57 Comm. ACM 31 (2014).

31 Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (2014).

32 Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1; Inter-Am. Comm'n H.R., Privacy and Freedom of Expression in the Americas, OEA/Ser.L/V/II. Doc. 34 (2013).