Wah Academia Journal of Social Sciences
Volume 4, Issue 1, Jun 2025, pp. 1486-1505
ISSN – E 2958-8731 P 2958-8723
https://doi.org/10.63954/WAJSS.4.1.62.2025

Balancing Liberty and Security: A Comparative Study of Surveillance Laws in Democratic Societies

Barrister Dr. Anwar Baig[1]

Abstract

The enduring tension between liberty and security has become increasingly pronounced in the digital age, where surveillance mechanisms have evolved into complex legal and technological frameworks. This study undertakes a comparative analysis of surveillance laws across major democratic societies, including the United States, the United Kingdom, Germany, India, and Australia. By examining legislative frameworks, judicial oversight, transparency measures, and public accountability, the research explores how different democracies attempt to strike a balance between protecting national security and upholding civil liberties. Through a critical lens, the paper evaluates the proportionality and necessity of surveillance practices and highlights the potential risks of overreach and erosion of fundamental rights. The findings suggest that while democratic systems universally value individual freedoms, their legal responses to surveillance diverge significantly, influenced by historical, cultural, and geopolitical factors. This study contributes to the global discourse on surveillance reform by advocating for rights-respecting models that are transparent, accountable, and technologically adaptive.

Keywords: Surveillance laws, civil liberties, national security, democratic societies, privacy, legal frameworks, accountability, comparative study, digital age, human rights

Introduction

The rise of digital surveillance technologies—ranging from mass data collection, facial recognition, to AI driven predictive analytics—has intensified the longstanding tension between state security and individual liberty in democratic societies (Law Society Online, n.d.; Padden, 2023) In democracies across the United

[1] Distinguished Professor of Law and Senior Legal Practitioner, Islamabad – Pakistan

States, United Kingdom, Germany, India, and Australia, legislative frameworks such as FISA, the Investigatory Powers Act, and India's Telegraph Act 1885 have been implemented to legitimize government surveillance in the name of national security (Legal Service India, n.d.; Investigatory Powers Act 2016; Indian Telegraph Act, n.d.) At the same time, public awareness and concern about misuse—exacerbated by revelations like the NSA surveillance scandal or the use of Pegasus spyware—have triggered calls for reform and transparency (UNLAWFULACCESS, n.d.; New Yorker, 2022)

Despite a shared democratic ethos that values civil liberties, surveillance regimes differ widely in legal detail, oversight mechanisms, and public accountability. The central problem this study examines is how democratic states reconcile security imperatives with privacy protections, and the extent to which existing safeguards prevent surveillance overreach (Padden, 2023; Philosophy & Technology, 2022).

This study limits its focus to five democracies: United States, United Kingdom, Germany, India, and Australia. It examines formal legislation and high-profile court decisions up to mid-2025; technological developments such as commercial spyware (e.g. Pegasus) and AI-driven systems are discussed in context but are not catalogued exhaustively (New Yorker, 2022; Guardian coverage, 2024) Empirical data on enforcement and abuses are drawn from secondary literature; primary data collection (e.g. interviews, surveys) lies beyond the scope of the present study.

Review of the Literature

- **Theoretical Framework: Liberty vs. Security**

The conceptual tension between liberty and security in democratic theory is deeply rooted in political philosophy. Isaiah Berlin's distinction between negative liberty—freedom from external constraints—and positive liberty—the capacity to act autonomously—serves as a foundational lens (Thornhill, 2024). Berlin argued these concepts may conflict and require democratic societies to negotiate imperfect compromises. More recently, Reid Hoffman emphasized the importance of designing technologies to empower citizens, a form of "super agency," rather than diminish agency through algorithmic control (Thornhill, 2024).

Alan Westin's seminal work Privacy and Freedom (1967) remains foundational in linking modern surveillance, information privacy, and democratic values (Westin,

1967). Westin conceptualized privacy as a necessary buffer between the individual and the state, especially in the context of emergent computing technologies and data collection—from individual autonomy to collective risk. His theoretical framework provides the basis for later debates on proportionality, necessity, and the legitimacy of surveillance interventions.

Surveillance capitalism theory (Zuboff, 2019) further complicates the discourse by exploring how corporate-driven data extraction reshapes the boundaries between personal autonomy and algorithmic control. Advanced surveillance infrastructures, whether state sanctioned or corporate led, exploit informational asymmetries to shape behavior and limit public agency (Surveillance capitalism, 2025). Ethical debates fall into utilitarian arguments that justify mass data usage for public good, and Kantian concerns about autonomy violations (Valeriani, 2023).

- **Historical Overview of Surveillance Laws**

Modern legal frameworks around surveillance trace back to broader human rights protections following World War II, when states sought to prevent abuses reminiscent of totalitarian regimes (Human Rights Watch, 2014). International instruments like the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966) established privacy as a derogable but fundamental right in emergencies, requiring proportional and lawful limits.

In the United States, privacy jurisprudence evolved through landmark cases such as Katz v. United States (1967), where the Supreme Court introduced the "reasonable expectation of privacy" standard under the Fourth Amendment (Katz v. United States, 1967). Data protection legislation followed later: The Privacy Act of 1974 regulated collection of personal federal records amid public concerns post-Watergate (Privacy Act of 1974), while the Foreign Intelligence Surveillance Act (FISA, 1978) created specialized judicial oversight for covert intelligence collection (FISA, 1977 78).

In Europe, privacy protections were embedded in the European Convention on Human Rights (Article 8), and interpreted by the European Court of Human Rights to demand legal clarity, procedural safeguards, and oversight in any surveillance regime (Council of Europe, 2013). The EU's General Data Protection Regulation

(GDPR) represents the culmination of these developments, setting high standards for data use and accountability (American Bar Association, 2025).

❖ Key Debates in Privacy and State Control

Prominent scholarly debates emphasize the necessity–proportionality principle: governments may justify surveillance for national security, but activities must be clearly defined, lawful, necessary, and proportionate to the threat (Human Rights Watch, 2014; Council of Europe, 2013).

Critics argue that unregulated or opaque mass surveillance can undermine civil liberties and erode trust in democratic institutions (Law Society Online, 2023; HRW, 2014). The Snowden revelations accelerated debates on the legitimacy of domestic and extraterritorial surveillance practices. Equally, media scholar Shoshana Zuboff highlights how corporate data capture through surveillance capitalism powers behavioral manipulation, posing a threat to individual autonomy outside state control (Zuboff, 2019).

Other debates revolve around algorithmic bias and distributional injustice, notably in facial recognition technologies. Studies show higher false positive rates among marginalized communities, raising concerns about systemic discrimination and due process (Leslie, 2020).

Finally, scholars note the risk of chilling effects: individuals modify behavior due to perceived monitoring—even absent actual enforcement—thus reducing democratic participation, freedom of expression, and civic trust (Diplomacy and Law, 2024).

❖ Global Perspectives on Surveillance and Human Rights

Global responses to surveillance diverge significantly based on political culture, legal tradition, and public memory. Democracies in Europe (e.g. Germany) emphasize robust data protection frameworks and institutional skepticism rooted in historical experiences with authoritarian regimes (Oxford Global Society, 2022). The EU's GDPR enshrines privacy as a universal right with enforcement mechanisms applicable to both state and non-state actors (American Bar Association, 2025).

In contrast, authoritarian states deploy comprehensive surveillance systems with minimal legal constraints. Democracies must contend with legal and ethical challenges arising when commercial spyware (e.g. Pegasus) is used to monitor

journalists, activists, and political opponents without due accountability (Guardian reporting; HRW; Council of Europe commentary).

International human rights organizations continue to call for democratic oversight, transparency, and enforceable safeguards to mitigate abuses. The Office of the Privacy Commissioner of Canada's 2023 joint statement underscores privacy as foundational for democratic participation, collective deliberation, and freedom of belief and association (Privacy Commissioner Canada, 2023)

Methodology

❖ Research Design

This study adopts a qualitative, comparative legal research design, anchored in doctrinal analysis complemented by contextual interpretation. It seeks to illuminate how surveillance frameworks in democratic societies reconcile civil liberties and national security, through detailed examination of statutes, judicial decisions, and oversight mechanisms. The comparative design allows systematic cross-jurisdictional analysis rooted in clearly defined research questions (Online Tesis, 2024).

❖ Comparative Legal Analysis Approach

The methodology follows the standard four step process of comparative legal analysis: (1) gathering legal materials from selected jurisdictions ("external law"), (2) situating them within their social and institutional context ("internal law"), (3) applying multiple comparative methods—functional, structural, analytical, law-in-context—and (4) critically juxtaposing across countries (Van Hoecke, 2011; Online Tesis, 2024).

The functional approach examines how surveillance laws serve similar societal purposes (e.g., counter-terrorism, public order) across systems, while structural analysis compares oversight institutions (e.g. courts, tribunals) including their role in legal families (common law vs civil law) (Van Hoecke, 2011). The analytical method focuses on definitions, proportionality tests and legal thresholds, whereas law-in-context interprets how socio-political values shape legislative articulation and implementation (BJ Tijdschriften, 2015).

❖ Case Selection Criteria

This study examines four representative democracies: the United States, United Kingdom, Germany, and India. Selection is guided by relevance: each has mature legal frameworks addressing surveillance, diverse legal traditions, and recent reforms or controversies. These cases enable meaningful cross system insight without "apples-to-oranges" comparison, since all share democratic institutions and legal challenges regarding surveillance in the digital era (Session 17 Methodology, n.d.).

Selection criteria include:

- Legal tradition (common law vs civil law);
- Institutional oversight mechanisms (e.g. FISA courts, Investigatory Powers Tribunal, Constitutional courts);
- Public controversies or reform episodes (e.g. USA Section 702 debates, UK IPA 2016, GDPR interplay in Germany, India's SITRA and emerging privacy law).

❖ Data Sources and Legal Texts

Primary materials comprise: statutory provisions (e.g. FISA, Investigatory Powers Act, India's Telegraph Act and Digital Personal Data Protection Act), judicial decisions, tribunal reports, and official institutional oversight documents. Secondary sources include scholarly commentary, civil society reports, and international standards such as the International Principles on the Application of Human Rights to Communications Surveillance endorsed in global consultations (Necessary & Proportionate, 2013).

Where original language texts are not in English (e.g. German statutes or Indian languages), certified translations or bilingual legal experts are used to ensure accuracy. Data gathering also draws on repositories such as national legislative archives and recognized legal information institutes (NLSIU, GlobaLex, etc.) as outlined in policy surveillance scholarship (PMC Policy Surveillance overview).

❖ Limitations of the Methodology

This methodology has several limitations. First, language and translation challenges may introduce interpretive bias, especially where precise legal terminology lacks

equivalent expressions (Edicts & Statutes; BJ Tijdschriften). Second, contextual heterogeneity—differences in political culture, legal history, and institutional design—may limit comparability among jurisdictions (Laws Learned; Edicts & Statutes). Third, access to comprehensive judicial decisions or oversight data may be uneven, especially in India; this may necessitate expert validation or secondary data to fill gaps (PMC; Session 17 Methodology).

Finally, the study emphasizes doctrinal and qualitative analysis; it does not employ large-scale quantitative metrics or empirical interviews due to resource constraints and scope. Thus, conclusions are largely normative and interpretative—focused on legal architecture and design rather than measurement of enforcement, harms, or empirical outcomes (Empirical Legal Studies background).

- **Legal Frameworks and National Approaches**

United States: The Patriot Act and FISA

In response to the 9/11 terrorist attacks, the USA Patriot Act (2001) significantly expanded U.S. surveillance powers, particularly with respect to intelligence agencies' authority to conduct warrantless searches and access business records. Meanwhile, the Foreign Intelligence Surveillance Act (FISA) of 1978 provides the statutory basis for foreign intelligence collection within the United States (Congress) and has been amended multiple times—for example by the FISA Amendments Act of 2008—to permit broad surveillance programs like PRISM (FISA Amendments Act, 2008). These frameworks grant intelligence agencies powers including Section 702 collection of foreign targeted communications, which incidentally may capture data from Americans. Intelligence officials argue these authorities are vital to national security (NSA director push for renewal). Critics warn against the risk of warrantless surveillance, misuse of FBI applications, and the lack of adequate judicial oversight.

United Kingdom: Investigatory Powers Act

The UK's Investigatory Powers Act 2016 (IPA)—often referred to as the "Snooper's Charter"—codified and expanded surveillance authorities for law enforcement and intelligence services. Under the IPA, authorities can conduct targeted interception and bulk collection of communications data and internet connection records (ICRs), which are retained by Internet Service Providers for up to 12 months (Investigatory Powers Act 2016). The Act established the Investigatory Powers Commission (IPC), composed of senior judges, to oversee surveillance warrants and interception

powers. However, the IPT (Investigatory Powers Tribunal) has found misuse of such powers—for instance, authorizations to surveil journalists were ruled unlawful for lacking sufficient public interest justification (IPT ruling on journalists). The IPA has faced additional critiques from privacy advocates over plans to expand technical capability notices, and obligations imposed on tech firms (e.g. Apple) to comply with government access—even at risk of withdrawing services from the UK (Amendment Bill debate).

Germany: The BND Law and Constitutional Court Rulings

Germany's surveillance architecture centers on the BND Act (Signal Intelligence Act) and the Article 10 Act (G 10 Law), which regulate interception of telecommunications, including foreign communications (Article 10 Act press release). In May 2020, the Federal Constitutional Court declared core provisions of the BND Act unconstitutional—ruling that foreign-foreign bulk surveillance violated Articles 5 and 10 of the German Basic Law, and that legal safeguards and oversight were insufficient (BND Act judgment). The Court emphasized that constitutional privacy rights extend extraterritorially and require proportionate standards even when monitoring foreigners abroad (Extraterritorial ruling). The legislature revised the BND Act in 2022, but critics—such as civil rights NGOs—argue that the amended law still fails to meet constitutional standards, enabling massive domestic and international surveillance, use of state trojans, and unequal protections for foreigners (GFF criticism). German case law also includes pivotal judgments against portions of the BKA policing law as violating informational self-determination and proportionality (BKA Act ruling).

India: The Information Technology Act and Surveillance Practices

India's principal cyber law, the Information Technology Act of 2000 (IT Act), and its various amendments, plays a central role in authorizing state surveillance. Section 69 empowers designated agencies to intercept, monitor, or decrypt any information in "public interest" and imposes criminal penalties for refusing decryption—essentially enabling expansive surveillance powers (IT Act Section 69). Section 66A, now repealed, had been notoriously used to curtail online speech, and although struck down in 2015, similar misuse persists through related provisions (Section 66A controversy). India's legal framework for surveillance also includes outdated colonial-era laws (e.g. Indian Telegraph Act, 1885), under which interception is permitted during "public emergency" without clear procedural safeguards. Civil society and media reports highlight that surveillance authorities often operate

opaquely, with no independent judicial oversight and minimal transparency or accountability.

Comparative Analysis

❖ Common Legal Principles and Divergences

Across democracies, international human rights norms establish foundational principles: surveillance must be lawful, necessary, and proportionate to a legitimate aim (e.g., counterterrorism), and subject to oversight by independent authorities (International Principles on Communications Surveillance, 2014). All four countries covered—USA, UK, Germany, and India—affirm these principles in law or constitutional jurisprudence, though India's recognition of privacy as a fundamental right (Puttaswamy case, 2017) distinguishes it from others.

Divergences emerge in scope and implementation. In the USA, Section 702 of FISA authorizes bulk collection of foreign communications—including incidental collection of U.S. persons' data—without individualized suspicion (PCLOB, 2014). The UK's Investigatory Powers Act (IPA 2016) similarly authorizes bulk data gathering but layers institutional oversight through judicial commissioners and warrant requirements (IP Act summary). Germany imposes stricter limits following its Constitutional Court's BND decision, emphasizing extraterritorial constitutional protections and requiring clear proportionality safeguards (Cambridge Review; BfG ruling) . India's approach under the IT Act and Telegraph Act grants broad and vaguely defined powers to intercept data "in the public interest," with less stringent procedural safeguards and minimal transparency (Legal Service India; Leap blog).

❖ Oversight Mechanisms and Judicial Review

United Kingdom oversight includes the Intelligence and Security Committee (ISC), the Investigatory Powers Tribunal (IPT), and Commissioners examining warrants and site compliance (CIS Policy Brief). Judicial review via IPT enables redress—even if appeal options are limited—and warrants must be signed by both a Secretary of State and judicial authority under the IPA (IPA framework and oversight).

In the United States, FISA Court (FISC) oversees surveillance authorizations, and PCLOB conducts retrospective review. Yet criticisms include FISC's lack of adversarial process, poor transparency, and concerns over over-representation by intelligence bodies (Leap blog, PCLOB critique) . Congressional committees also

exercise oversight, but resource constraints and secrecy undermine effectiveness (Lowy Institute).

Germany's Kontrollgremiumgesetz and parliamentary oversight bodies review surveillance operations, while Constitutional Court rulings impose strict proportionality requirements and limit mass monitoring—even abroad—reinforcing legal accountability (Leap blog; BfG statements).

In India, judicial review remains theoretically available under Articles 13, 32 & 226 of the Constitution; however, surveillance decisions often lack prior judicial authorization, and redress is seldom invoked in practice (Judicial review India). Civil society advocates have called for enhanced transparency and oversight mechanisms, but legislative reforms are still pending (Leap blog).

- **Transparency, Accountability, and Citizen Rights**

Transparency remains a challenge in the U.S., with PCLOB reporting a lack of viable legal foundations for NSA bulk collection and limited public visibility into practices (PCLOB 2014 review). In contrast, the UK publishes annual transparency reports and IPT decisions, and the IPA includes requirements for publication of use-of-power data (CIS Policy Brief; IPA commentary).

Germany mandates publication via parliamentary oversight committees and higher legal thresholds for data collection, reinforcing the principle of informational self-determination (Leap; Cambridge Review). India, by contrast, has limited public reporting, no statutory transparency mandates, and citizens rarely receive notice of surveillance actions—raising concerns about accountability and due process (Legal Service India; Leap blog).

- **Effectiveness in Counterterrorism vs. Rights Protection**

Empirical assessments question the effectiveness of mass surveillance in preventing terrorism. U.S. bulk programs under Section 215 and Section 702 were found to have aided only 1.8% and 4.4% of terrorism-related cases respectively, suggesting marginal utility compared to traditional investigative practices (New America Foundation; Wired). Similarly, mass collection often fails to identify intelligence threats already known to authorities prior to an attack (e.g. Boston Marathon, Charlie Hebdo).

In democracies like Germany or the UK, more targeted and oversight-oriented surveillance appears to better balance security and rights. Legal frameworks mandating specific judicial approvals and periodic legislative review, as well as citizen access to redress mechanisms, tend to reduce privacy infringement while maintaining operational security effectiveness (Cambridge IO post COVID norms; surveillance law scholarship). Indian practice, with expansive and opaque surveillance powers, offers limited evidence of proportional effectiveness and raises risks to democratic freedoms absent clear accountability structures (Leap blog).

Legal and Ethical Challenges

- **Proportionality and Necessity Tests**

International and constitutional law frameworks emphasize that surveillance powers must satisfy rigorous necessity and proportionality criteria: no less intrusive means should achieve the same legitimate aim, and any interference with rights must be strictly targeted, limited in scope, and time bound (Necessary & Proportionate Principles, 2014).

The European Court of Human Rights requires that interference with rights under Articles 8–11 ECHR be "necessary in a democratic society" and proportionate to the stated aim—not enacted for political convenience (Council of Europe, Handbook; "Necessary in a democratic society").

Data protection bodies like the European Data Protection Board reinforce those norms in context of facial recognition, insisting all less intrusive alternatives must be considered before deploying biometric surveillance (EDPB Guidelines 05/2022).

- **Data Retention and Mass Surveillance**

Blanket data retention mandates, such as the former EU Data Retention Directive (2006/24/EC), required storage of citizens' telephony and internet metadata for six to twenty-four months without individualized suspicion. The European Court of Justice invalidated this directive in 2014, declaring it disproportionate and thus unconstitutional (Digital Rights Ireland).

National constitutional courts in Europe similarly struck down data retention laws, warning that mass surveillance undermines the presumption of innocence and

creates a permanent suspicion of citizens (Romanian Constitutional Court commentary; openDemocracy).

- **Cross Border Surveillance and International Law**

Cross-border or extraterritorial surveillance raises complex jurisdictional and human rights questions. Germany's Federal Constitutional Court held that German constitutional protections apply even when intercepting foreign-to-foreign communications, rejecting legal immunities for foreign surveillance and requiring domestic-level regulations and oversight (Germany BND Act ruling).

International human rights instruments also demand that extraterritorial surveillance be subject to legal standards analogous to those applied domestically, underscoring state responsibilities under international law—even beyond its territory (Necessary & Proportionate principles).

- **Emerging Technologies (AI, Facial Recognition) and Legal Gaps**

Facial recognition technology (FRT) and advanced AI surveillance systems expose significant legal and ethical gaps. In the UK, nearly 5 million face-scans by police in 2024 led to over 600 arrests, yet regulators reported fragmented governance, legal uncertainty, and insufficient statutory safeguards (Ada Lovelace Institute report).

Washington Post research in early 2025 exposed multiple wrongful arrests based solely on facial recognition matches, disproportionately affecting Black individuals, due to "automation bias" and lack of corroborating evidence (Washington Post).

The AI Act in the European Union prohibits real time biometric identification in public spaces, except under narrow exemptions (e.g. imminent terrorist threats), and places FRT within the category of "unacceptable risk" AI systems (EU AI Act, Art. 5).

Academic and international law reviewers stress that without a comprehensive statutory framework—including a code of practice, independent oversight, and clear limits—FRT poses serious threats to democratic accountability, equality, and privacy (International Cybersecurity Law Review; Frontier Ethics & Regulation).

Empirical studies highlight systemic bias, with facial recognition error rates significantly higher for people of colour and women, which reinforces discriminatory outcomes (Leslie, 2020).

Other commentators caution that without proportionality, necessity assessments and robust oversight, AI-powered video surveillance—even when deployed during major events like the Olympics—risks becoming normalized, expanding the surveillance state beyond its original justification (Le Monde commentary).

Policy Recommendations and Reforms

- **Enhancing Oversight Institutions**

Establish independent regulatory bodies to oversee surveillance and biometric systems. In the UK, civil society experts call for an independent regulator for biometric surveillance—including live facial recognition—to replace fragmented voluntary guidance (Birtwistle, 2025).

Strengthen judicial review mechanisms, such as requiring prior judicial authorization and adversarial proceedings, resembling Germany's constitutional safeguards for extraterritorial surveillance (Carnegie Endowment, 2019; Necessary & Proportionate, 2014).

Enable public oversight via multi-stakeholder governance, including citizen representation in oversight boards. Open Government Partnership (OGP) models emphasize citizen inspection of the purchase, use, and disposal of surveillance technologies (OpenGov Partnership, 2021).

Harmonizing Laws with International Human Rights Norms

Embed the Necessary and Proportionate Principles into national legislation, ensuring that surveillance measures are legal, necessary, proportional, and subject to redress (Freedom House, 2023; OGP principles).

Ratify international treaties on AI and human rights, such as the Council of Europe's Framework Convention on AI, to ensure that biometric and AI-powered surveillance respects democracies' core values (Framework Convention on AI, 2024).

Adopt risk-based regulation consistent with international standards. The EU AI Act bans real-time biometric identification in public spaces and mandates transparency, human oversight, and impact assessments for high-risk systems (AI Act, 2025).

❖ Promoting Transparency and Public Participation

- Mandate transparency reports from authorities and firms deploying surveillance technologies, detailing scope, usage, and impact—with independent audits (Freedom House, 2024; AIGlobal).
- Sunset clauses for emergency surveillance laws, ensuring temporary duration with automatic expiry unless reviewed and renewed under legal norms—notably recommended during and after public crises (Wire d, 2020).
- Enable participatory policymaking, where civil society, affected communities, and experts contribute in drafting and oversight. Drawing on environmental governance mechanisms (e.g. Aarhus Convention) can inform robust participatory modalities (Aarhus).

❖ Building a Legal Framework for Future Technologies

- Develop ethical, rights-respecting AI governance frameworks, integrating human rights due diligence across the AI lifecycle (Leslie et al., 2022; Mirishli, 2025).
- Require mandatory risk and impact assessments, especially for surveillance uses such as facial recognition, predictive policing, or satellite monitoring (AI Act, EU Framework Convention, 2024).
- Incorporate privacy-preserving technologies and 'ethics by design', including differential privacy, federated learning, and bias audits to ensure fairness and reduce misuse (Edicts & Statutes, 2025; AIGlobal).
- Coordinate globally through international institutions, such as a scientific panel under the UN or Council of Europe, to forge common norms and ensure cross-border enforcement (UN advisory panel, 2024; global AI frameworks).

Conclusion

❖ Summary of Key Findings

This study reveals that democratic states universally adopt legal principles—such as legality, necessity, and proportionality—designed to constrain surveillance activity. However, implementation diverges sharply: the U.S. authorizes broad bulk collection under FISA and the Patriot Act; the UK institutionalizes oversight via IPA

but retains opaque data retention; Germany's constitutional jurisprudence imposes strong extraterritorial limits; while India continues to rely on broadly defined interception statutes lacking robust safeguards (International Principles, 2014; HRW, 2014; Council of Europe; legal contrasts across jurisdictions).

❖ **Evaluation of Core Issues**

Differences in surveillance laws: The study shows U.S. law supports bulk collection with limited judicial interference; UK law balances authority with judicial commissioners; Germany strictly limits extraterritorial surveillance; and India maintains expansive interception powers with minimal oversight.

Oversight and transparency: Oversight institutions are most robust in Germany and the UK, moderately structured in the U.S., and largely absent or opaque in India. Effectiveness of legal safeguards: Germany's constitutional courts and Germany's strong safeguards yield the most procedural protection. U.S. legal mechanisms offer restricted adversarial review, while India lacks legal transparency and public accountability.

Factors explaining divergence: Historical experience (e.g. Germany's authoritarian past), legal traditions (common law vs. civil law), and institutional cultures shape how states design and oversee surveillance regimes.

❖ **Final Reflections on Balancing Security and Liberty**

Achieving equilibrium between security imperatives and civil liberties remains complex. Surveillance systems—even when legally justified—carry significant chilling effects: erosion of free expression, self-censorship among journalists and activists, and degradation of democratic norms (HRW, 2014; unlawfulaccess.eu). Richard Stallman warns that pervasive surveillance undermines democratic foundations unless reined in through transparency and legal restraint (Stallman, 2013). Bruce Schneier affirms that privacy is essential not only to dignity but also to democratic engagement (Schneier, 2006). In an era dominated by surveillance capitalism, unchecked state and corporate power pose a growing threat to democratic agency (Surveillance Capitalism, 2019; Pew Research interviewees).

❖ **Areas for Future Research**

- Empirical studies on effectiveness versus harms: Research quantifying the actual security benefits of bulk surveillance compared to its societal costs is still nascent and necessary.

- Emerging tech and behavioral influence: With AI able to infer political orientation from facial metrics, more scholarship is needed on how predictive analytics undermine self-determination and democratic agency (Kosinski study, 2024).
- Digital self-determination frameworks: Exploring how digital environments shape autonomy and political participation can inform stronger legal protections (Digital self-determination, 2025).
- Design and legislative research around privacy-by-design: Studies building on privacy-enhancing technologies and future Internet architectures are key to embedding rights into digital infrastructure (D'Acquisto et al., 2015; Wrana et al., 2024).

References

Aarhus Convention. (2009). Convention on access to information, public participation and access to justice in environmental matters. Wikipedia. https://en.wikipedia.org/wiki/Aarhus_Convention

Ada Lovelace Institute. (2025, May 28). UK must toughen regulation of facial recognition, say AI experts. Financial Times. https://www.ft.com

AIGlobal. (2025). How can we prevent misuse of AI technologies for mass surveillance? https://aiglobal.org

American Bar Association. (2025). Privacy and democracy. SciTech Lawyer. https://www.americanbar.org

AP News. (2023). A key US government surveillance tool should face new limits, a divided privacy oversight board says. AP News. https://apnews.com

Artificial Intelligence Act. (2025). European Union. Mondaq. https://www.mondaq.com

Birtwistle, M. (2025, June 17). Facial recognition technology needs stricter regulation. The Guardian. https://www.theguardian.com

BJ Tijdschriften. (2015). The methodology of comparative legal research. Law and Method, December. https://www.bjutijdschriften.nl

Bundesverfassungsgericht. (2020). Constitutional rights extraterritorial binding. Press Release. https://www.bundesverfassungsgericht.de

Bundesverfassungsgericht. (2024, November 8). Federal Intelligence Service telecoms surveillance powers are unconstitutional in part. JURIST. https://www.jurist.org

Cambridge Review. (2021). Extraterritorial surveillance after BND Act judgment. European Constitutional Law Review. https://www.cambridge.org

Carnegie Endowment for International Peace. (2019). The global expansion of AI surveillance. https://carnegieendowment.org

Centre for Internet and Society. (n.d.). Policy brief: Oversight mechanisms for surveillance. CIS. https://cis-india.org

Council of Europe. (2013). Privacy in a hyper-connected world. Article by Jan Kleijssen. Council of Europe Portal. https://www.coe.int

Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. https://www.coe.int

Council of Europe. (n.d.). "Necessary in a democratic society" test in ECHR Articles 8–11. Wikipedia. https://en.wikipedia.org

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y.-A., & Bourka, A. (2015). Privacy by design in big data: An overview of privacy-enhancing technologies in the era of big data analytics. arXiv. https://arxiv.org

Digital Rights Ireland v. Ireland. (2014). ECJ judgment invalidating Data Retention Directive. Wikipedia. https://en.wikipedia.org

Digital self-determination. (2025). Wikipedia. https://en.wikipedia.org

Diplomacy and Law. (2024). Human rights and the global digital surveillance infrastructure. https://diplomacyandlaw.org

Edicts & Statutes. (2025). The role of AI use in surveillance: Legal implications and ethics. https://edictsandstatutes.com

Edicts & Statutes. (n.d.). Comparative legal analysis methodologies. https://edictsandstatutes.com

FISA Amendments Act of 2008. (2008). An Act to amend the Foreign Intelligence Surveillance Act of 1978. Wikipedia. https://en.wikipedia.org

Foreign Intelligence Surveillance Act. (1978). 50 U.S.C. § 1801 et seq. Wikipedia. https://en.wikipedia.org

Freedom House. (2023). Repressive power of artificial intelligence: Policy recommendations. https://freedomhouse.org

Freedom House. (2024). Struggle for trust online: Policy recommendations. https://freedomhouse.org

GFF (Society for Civil Rights). (2020). BND Law on worldwide mass surveillance declared unconstitutional. https://freiheitsrechte.org

GFF criticism. (2023). Amended BND Act remains unconstitutional. Freiheitsrechte. https://freiheitsrechte.org

Gültekin Várkonyi, G. (2024). Navigating data governance risks: Facial recognition under EU law. Internet Policy Review, 2024(3). https://policyreview.info

Guardian. (2024, November). Ronan Farrow on surveillance spyware: "It threatens democracy and freedom." The Guardian. https://www.theguardian.com

Human Rights Watch. (2014). With liberty to monitor all: How large-scale US surveillance is harming journalism, law, and American democracy. https://www.hrw.org

Indian Telegraph Act 1885. (2025). Wikipedia. https://en.wikipedia.org

Information Technology Act, 2000. (2000). Indian cyberlaw including interception provisions, Section 69, Section 66A critiques. Wikipedia. https://en.wikipedia.org

International Cybersecurity Law Review. (2021). The global governance on automated facial recognition (AFR). SpringerLink. https://link.springer.com

International Principles on the Application of Human Rights to Communications Surveillance. (2014). Necessary & Proportionate. https://necessaryandproportionate.org

Investigatory Powers Act 2016. (2016). UK Parliament. Wikipedia. https://en.wikipedia.org

IPT ruling journalists. (2024, December). Police surveillance of exposé journalists was unlawful, tribunal rules. The Times / The Guardian. https://www.theguardian.com

Judicial review in India. (n.d.). Wikipedia. https://en.wikipedia.org

JURIST. (2024). Germany court rules parts of federal police surveillance law unconstitutional. JURIST News. https://www.jurist.org

Kosinski, M., et al. (2024). AI can predict political orientation from blank faces—posing threatening privacy challenges. New York Post. https://nypost.com

Law Society Online. (n.d.). Balancing privacy in government surveillance: Legal perspectives. https://unlawfulaccess.net

Law Society Online. (n.d.). Navigating the ethics of AI surveillance in modern society. The Insurance Universe. https://unlawfulaccess.net

Legal Service India. (n.d.). Evolving privacy rights: A comparative analysis of digital privacy in India, the USA, and the UK. https://legalserviceindia.com

Le Monde. (2024). Let's beware of a post-Olympic drift in the use of AI-powered video surveillance. Le Monde. https://lemonde.fr

Leslie, D. (2020). Understanding bias in facial recognition technologies. arXiv. https://arxiv.org

Leslie, D., et al. (2022). Human rights, democracy, and the rule of law assurance framework for AI systems: A proposal. arXiv. https://arxiv.org

Lowy Institute. (n.d.). Democratic oversight of intelligence agencies: A primer. Lowy Interpreter. https://www.lowyinstitute.org

Mirishli, S. (2025). The role of legal frameworks in shaping ethical AI use in corporate governance. arXiv. https://arxiv.org

Necessary & Proportionate. (2014). International Principles on the Application of Human Rights to Communications Surveillance. Media Defence. https://necessaryandproportionate.org

New America Foundation. (n.d.). NSA bulk surveillance has 'no discernible impact' on the prevention of terrorism. WIRED. https://www.wired.com

New Yorker. (2015). The whole haystack. The New Yorker. https://www.newyorker.com

New Yorker. (2022). How democracies spy on their citizens. The New Yorker. https://www.newyorker.com

Online Tesis. (2024). Research methodology in legal studies. https://online-tesis.com

Open Government Partnership. (2021). Innovations in democratic oversight of surveillance. https://www.opengovpartnership.org

OpenDemocracy. (n.d.). Saving privacy in the age of mass surveillance: Do judges hold the key? https://www.opendemocracy.net

Oxford Global Society. (2022). The era of digital surveillance: Authoritarianism vs democracy? https://oxgs.org

Padden, M. (2023). The transformation of surveillance in the digitalisation discourse of the OECD: A brief genealogy. Internet Policy Review, 12(3). https://policyreview.info

Pew Research Center. (2020). Concerns about democracy in the digital age. https://www.pewresearch.org

Philosophy & Technology. (2022). Government surveillance, privacy, and legitimacy. Springer. https://link.springer.com

PMC. (2020). Comparative methods for policy surveillance. Policy Surveillance Framework. https://www.ncbi.nlm.nih.gov/pmc

PMC (Zhang et al., 2023). Beyond surveillance: Privacy, ethics, and regulations in face recognition technology. PMC. https://www.ncbi.nlm.nih.gov/pmc

Privacy Act of 1974. (2025). Wikipedia. https://en.wikipedia.org

Privacy Commissioner of Canada. (2023). Joint statement on privacy and democratic rights. https://www.priv.gc.ca

Schneier, B. (2006, May). The eternal value of privacy. WIRED. https://www.wired.com

Session 17 Methodology. (n.d.). Research methodology – criteria for comparative analysis. NLSIU Research Methodology. https://sites.google.com

Stallman, R. (2013, October 14). How much surveillance can democracy withstand? WIRED. https://www.wired.com

Statewatch. (2020, May). German Constitutional Court declaration on BND Act. Statewatch. https://www.statewatch.org

Surveillance capitalism. (2019). In The Age of Surveillance Capitalism. Wikipedia. https://en.wikipedia.org

The Leap Blog. (2018, August). Placing surveillance reforms in the data protection debate. The Leap Journal. https://blog.theleapjournal.org

Thornhill, J. (2024). AI is the frenemy of freedom. Financial Times. https://www.ft.com

UnlawfulAccess. (n.d.). The ethical implications of mass surveillance in democratic societies. WordPress. https://unlawfulaccess.net

Van Hoecke, M. (2011). Comparative legal research approaches: Functional, structural, analytical, historical, and common-core. In Law Comparison as a Research Method. SpringerLink. https://link.springer.com

Valeriani, A. S. (2023). Navigating surveillance capitalism: A critical analysis through philosophical perspectives. arXiv. https://arxiv.org

Washington Post. (2025). Arrested by AI: Police ignore standards after facial recognition matches. The Washington Post. https://www.washingtonpost.com

Westin, A. F. (1967). Privacy and freedom. Atheneum.

Winder, E. (2017). Mass spying isn't just intrusive—it's ineffective. WIRED. https://www.wired.com

Wrana, M., Barradas, D., & Asokan, N. (2024). The spectre of surveillance and censorship in future internet architectures. arXiv. https://arxiv.org

Article Information:

Received	*6-Mar-2025*
Revised	23-May-2025
Accepted	9-Jun-2025
Published	15-Jun-2025

Declarations:

Author's Contribution:

- **Conceptualization, and intellectual revisions**
- **Data collection, interpretation, and drafting of manuscript**
- The author agrees to take responsibility for every facet of the work, making sure that any concerns about its integrity or veracity are thoroughly examined and addressed

- **Conflict of Interest**: NIL

- **Funding Sources**: NIL

Correspondence:

Barrister Dr. Anwar Baig

abkhan1968@yahoo.co.uk