Page 700 - 716 **DOI:** *https://doij.org/10.10000/IJLMH.1110812*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 5

2025

Comparing Digital Privacy Rights in Democracies and Authoritarian States: A Public Law Analysis of Data Protection and Surveillance Laws

SUKHMANDEEP SINGH[1] AND DR. AMIT KASHYAP[2]

ABSTRACT

The huge growth of data usage, projected at over 181 zettabytes by 2025, has become an issue of worrisome in individuals as safeguarding the individual privacy as well as enabling state surveillance has emerged as a pivotal public-law issue worldwide. This research paper fills up the gap with the help of comparative public-law scholarship; analysing digital privacy rights, data protection, and surveillance laws in two major democracies (E.U. & U.S.) and two authoritarian countries (China & Russia). These have been chosen based on their influence globally having different legal traditions, and having different approaches for balancing the state power with individual autonomy. We have talked about five major questions in this research such as on the matters of privacy guarantees, power of surveillance, oversight mechanisms, fallback mechanism, impact on human rights, and the privacy-security balance. This study uses doctrinal analysis of primary sources (e.g. GDPR, Fourth Amendment, PIPL, Yarovaya Law), precedents (e.g., Schrems II, Carpenter), and recent AI-integration measures (EU AI Act; China's AI reporting rules) etc. The methodology used here combines the constitution of respective countries with the available data of enforcement and practices done by institutions in their respective jurisdictions. The primary lessons we will learn from this research is that we need an independent oversight institution as well as proportionality to have a strong privacy protection but it will be of no value if it is not enforced effectively. The above-mentioned democratic countries use the surveillance techniques via necessity and proportionality test to keep it effective. In contrast, the authoritarian government works for the interests of state authorities, often giving low priority to the rights of the persons. Such type of major differences is visible in judicial remedies, transparency requirements, and regulatory independence. If there is still unchecked surveillance then they might lead to loss of civil liberties and participation of people in governance. The paper also recommends key changes and developments required at various levels to reduce the above risks. It is via this only that theory has been related to

[1] Author is a LLM Student at School of Law, Lovely Professional, University, Phagwara, Punjab, India.
[2] Author is an Associate Professor at School of Law, Lovely Professional University, Phagwara, India.

 [ISSN 2581-5369]

the enforcement, here research plays a bigger part of discussions on how the rights can be preserved along with security requirements emerging due to changing times.

***Keywords**: Surveillance, Digital privacy, Data protection, Institutional independence, Constitutional law.*

I. INTRODUCTION

The concept of digital privacy has been evolving with the rise of digital revolution as now everything has become connected from personal liberty to state power. The government has been adopting new ways to protect its nation as well as to become economically independent, with these two goals, the protecting of digital privacy has become complex. This paper employs a public-law perspective in which it look upon the constitution, judiciary and enforcement mechanism which influence the balance which is needed in between digital privacy and national security.

For the comparative purpose, we choose two democracies (E.U. & U.S.A.) and two authoritarian countries (China & Russia). In the EU, privacy takes as part of the Charter of Fundamental Rights with reference to Article 7[3] and 8[4]. It is. protected with the help of General Data Protection Regulation (GDPR)[5]. Although the U.S. lacks a single law for the whole country yet it relies on constitution (Fourth Amendment)[6] as well as sector-specific laws such as the CCPA[7], HIPAA[8] etc. Among authoritarian countries, China has Personal Information Protection Law (PIPL)[9] as well as Cybersecurity Law[10] which gives wide-ranging surveillance powers to state authorities[11], while Russia's Yarovaya amendments[12] and SORM framework enable extensive data collection and monitoring with limited judicial oversight.[13] These different approaches show a critical gap in available comparative public law scholarship which this paper addresses through its research questions.

Instead of focusing on individual freedom these governments focus on sovereign collectivism i.e. they keep interest of state or collective interests above personal freedom.[14] The kind of

[3] EU Charter of Fundamental Rights, 2000, Art. 7.
[4] EU Charter of Fundamental Rights, 2000, Art. 8.
[5] General Data Protection Regulation, 2016 (E.U.).
[6] The Constitution of the United States, 1787, Fourth Amendment.
[7] The California Consumer Privacy Act, 2018.
[8] The Health Insurance Portability and Accountability Act, 1996 (U.S.A).
[9] The Personal Information Protection law, 2021 (China).
[10] The Cybersecurity Law, 2016 (China).
[11] Mark Jia, ''Authoritarian Privacy''91 *The University of Chicago Law Review* 733-809 (2024).
[12] Yarovaya Law, 2016 (Russia).
[13] *Roman Zakharov v. Russia,* Application no. 47143/06 (2015).
[14] European Data Protection Board, "Government access to data in third countries" (2019).

developments happening now shows us the need for a comparative analysis e.g. China's tightening its grip on cybersecurity laws and Russia's increasing requirements of data localization which reinforce the state control, while in the U.S., there are huge number of state specific legislations amid federal stagnation.[15] The E.U. has recently added a detailed regulation related to AI into governance[16] along with already existing data protection laws that deal with new risks and technological issues.

Guided by five core research questions—

1. How do constitutional and statutory guarantees of privacy differ between democratic and authoritarian states?
2. How are surveillance powers justified and limited in practice across jurisdictions?
3. What institutional oversight mechanisms and remedies exist, and how effective are they?
4. What are the social and human rights implications of digital surveillance systems in democracies and authoritarian states?
5. How do the democracies and authoritarian states address the issue of maintaining equilibrium between privacy and security?

this study employs doctrinal analysis of primary legal texts and landmark judgments (e.g., Schrems II[17], Carpenter[18]) alongside contextual evaluation of institutional practices and enforcement data. By integrating constitutional theory with empirical insights, this research illuminates the divergent paths taken by democracies and authoritarian states in digital governance and assesses the implications for civil liberties, rule of law, and global data flows.

(A) Novelty and Significance of the Study

The exponential surge in global data, projected to surpass 181 zettabytes by 2025, generating approximately 402.74 million terabytes daily[19], marks a novel research frontier in digital privacy governance. Digital privacy is not merely a technological or statutory concern, but a constitutional issue that directly implicates the rule of law, fundamental rights, and democratic

[15] Data Privacy Laws: What You Need to Know in 2025, available at: https://www.osano.com/articles/data-privacy-laws (last visited on Sept 1, 2025).
[16] Marc Schuler and Taylor Wessing, "How the EU AI Act Supplements GDPR in the Protection of Personal Data" International Trademark Association.
[17] Schrems ll Case (Data Protection Commissioner v Facebook Ireland and Maximillian Schrems) (Judgement) (2020).
[18] Carpenter Case (Carpenter v. United States) (Judgement) (2016) 819 F.3d 880.
[19] Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts from 2024 to 2028, available at: https://www.statista.com/statistics/871513/worldwide-data-created/ (last visited on September 1, 2025).

 [ISSN 2581-5369]

legitimacy. Against the backdrop of exponential data growth, this research offers several original contributions that distinguish it from existing scholarship. First, by comparing two established democracies (the E.U. and the U.S.A.) alongside two prominent authoritarian states (China and Russia), it offers a comprehensive four-jurisdiction analysis that no prior study has yet undertaken. Secondly, paper sets out a three-dimensional framework i.e. normative (constitutional and statutory guarantees), institutional (mandates and independence of oversight bodies), and practical (enforcement practices and impact)—which reveals how independence of institution rather than legal text alone, determines privacy outcomes. Thirdly, the study draws on the most recent empirical data available in 2025, including enforcement statistics[20] such as 2,245 GDPR fines totalling €5.65 billion. By linking this empirical data with doctrinal analysis, the research connects to real-world enforcement, bridging theory and practice in a way not seen before. Fourth, by evaluating landmark cases (e.g., Schrems II[21], Carpenter[22]) with comparative enforcement data, the study demonstrates how political leaning influences not only laws but also their enforcement practice. Finally, it delivers targeted, evidence-based policy recommendations—ranging from creating adversarial review processes for FISA[23] to mandating limited judicial oversight in China's PIPL—that are realistic and globally applicable. Together, these innovations advance public-law theory on rights protection in the digital age and provide actionable guidance for policymakers across diverse legal and political systems. Thus, this study is justified by its theoretical contribution to comparative constitutional law and its practical relevance to pressing governance challenges of the digital age, underpinned by the comprehensive four-jurisdiction analysis.

(B) Literature Review

This review evaluates key scholarly sources, case law, and theoretical frameworks on digital privacy rights and surveillance laws in democratic (United States, European Union) and authoritarian (China, Russia) regimes, aligning with the study's framework. Existing scholarship on digital privacy and surveillance bifurcates sharply along regime lines. The study of democratic systems emphasises rights-based protections and institutional checks, while analyses of authoritarian states focus on state control and expansion of surveillance powers. Yet few works integrate a public-law framework that systematically compares constitutional guarantees, institutional independence, and enforcement practices across both regime types.

[20] Numbers and Figures, available at: https://cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures (last visited on Sept 1, 2025).
[21] Supra Note 15.
[22] Supra Note 16.
[23] Foreign Intelligence Surveillance Act, 1978 (U.S.A.).

 [ISSN 2581-5369]

Using a doctrinal and contextual methodology, the study analyses primary legal sources (e.g., EU GDPR, US Fourth Amendment, China's PIPL, Russia's Yarovaya Law) and secondary reports. Comparative analyses are limited. The available literature lacks qualitative comparative analysis (QCA) of constitutional factors. These gaps highlight the need for a public law framework integrating institutional design.

Doctrinal analyses of the EU's GDPR and U.S.'s Fourth Amendment emphasise proportionality and due process but often neglect enforcement realities and institutional variation across member states. Studies of China's PIPL and Russia's Yarovaya Law catalog broad surveillance authorizations and data-localization mandates but rarely consider the nominal constitutional privacy guarantees (Art. 40 of China's Constitution; Art. 23 of Russia's) in practice.

Building on doctrinal gaps, literature on institutional oversight has further highlighted deficiencies. As per Article 52 to 59 of GDPR, the Data Protection Authority of E.U.'s independence has been ensured. The E.U.D.B. perform a coordination role which is appreciable even though the intensity of enforcement differs among member states. In contrast, the executive gives the direction to laws in authoritarian countries such as Roskomnadzor law of Russia and Cyberspace Administration laws of China and therefore it lacks both judicial independence as well as transparency. In this research, we also compared various case laws (i.e. Digital Rights Ireland C-293/12[24]; Schrems II C-311/18[25]) which show us how courts can work in a way as to rip off the disproportionate measures as used in authoritarian countries.

This literature review leaves some gaps-

- Too much emphasis on statutory text with limited attention to how institutions and enforcement actually function.
- Strong bias towards EU-US models, marginalising the authoritarian approaches
- Lack of single analysis of constitutional design, oversight independence, and enforcement outcomes.

This study addresses those gaps by applying a three-dimensional public-law framework (normative, institutional, practical), and this framework is combined with 2025 enforcement data. The target of this study is to shape the digital privacy by comparing constitutional provisions, institutional independence and real-world enforcement in different countries.

(C) Research Methodology

[24] Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, C-293/12.
[25] Supra Note 15.

 [ISSN 2581-5369]

This study utilised both empirical and doctrinal research methodologies. The principal aim of this study is to investigate digital privacy rights, surveillance authorities, and institutional frameworks, and to analyse their interactions across four distinct jurisdictions: the European Union, the United States, China, and Russia. This methodology utilises techniques such as comparative public law, doctrinal analysis of primary sources, and contextual evaluation of institutional practices.

- **Doctrinal Analysis-** The main goal of this research is doctrinal, which means carefully analysis of primary legal sources. Some of these are parts of the Constitution, such as Article 40 of China's Constitution, the EU Charter of Fundamental Rights, the U.S. Fourth Amendment, and Article 23 of Russia's Constitution. Others are laws that set rules, such as GDPR, CCPA, HIPAA, PIPL, and the Yarovaya amendments. *Riley v. California*[26], *Carpenter v. United States*[27], *Digital Rights Ireland*[28], *and Schrems II*[29] are some of the most important court cases. This enables the identification of normative guarantees, statutory protections, and judicial interpretations that define privacy rights in each regime.
- **Contextual Analysis-** Doctrinal findings are situated within their broader political and institutional contexts. This involves examining how oversight bodies (e.g., EU Data Protection Authorities, the European Data Protection Board, the U.S. Foreign Intelligence Surveillance Court, China's Cyberspace Administration, and Russia's Roskomnadzor) operate in practice, focusing on their independence, mandates, and accountability mechanisms. Secondary sources, including scholarly articles, policy reports, and government publications, are used to evaluate institutional behaviour and enforcement realities.
- **Empirical Assessment-** To bridge theory and practice, the study incorporates enforcement statistics and regulatory reports, such as the GDPR Enforcement Tracker (2025), which recorded 2,245 fines totalling €5.65 billion. Integrating such data helps assess whether statutory guarantees translate into effective protections on the ground and reveals divergences in enforcement intensity across jurisdictions.
- **Three-Dimensional Comparative Framework**– Normative dimension: analysis of constitutional and statutory guarantees of privacy. Institutional dimension: examination

[26] Riley v. California, 573 U.S. 373 (2014).
[27] Supra Note 16.
[28] Supra Note 22.
[29] Supra Note 15.

 [ISSN 2581-5369]

of mandates, independence, and enforcement capacity of oversight bodies (e.g., DPAs, FISC, Roskomnadzor, CAC). Practical dimension: evaluation of enforcement practices, available remedies, and actual citizen impact.

By integrating rigorous doctrinal scrutiny with empirical and contextual insights, this methodology illuminates the interplay between formal legal design and real-world enforcement, highlighting the factors that underpin effective digital privacy protection or facilitate expansive state surveillance.

II. COMPARATIVE ANALYSIS OF DIGITAL PRIVACY AND SURVEILLANCE FRAMEWORKS

This section uses the comparative public-law research methodology to systematically examine digital privacy and surveillance frameworks across four exemplar jurisdictions through three analytical dimensions: normative, institutional and practical. Such holistic approach elucidates how these distinct legal systems balance privacy and state security imperatives within their political and socio-legal contexts.

(A) Constitutional Foundations and Rights Baseline

The normative dimension assesses legal texts that define the scope and limitations of digital privacy protections. The European Union expressly protects privacy and data protection as fundamental rights under Articles 7 and 8 of the Charter of Fundamental Rights, operationalised through General Data Protection Regulation (GDPR), widely known as the world's most comprehensive data protection framework. The GDPR enforces principles of consent, purpose limitation, data minimization, and transparency. The Court of Justice of the EU invalidated indiscriminate data-retention regimes in *Digital Rights Ireland(C-293/12))*[30] for failing proportionality under Article 8.

In the United States, unreasonable searches and seizures has been protected via Fourth Amendment, has been extended to digital data in *Katz v. United States*[31] and *Carpenter v. United States*[32], affirming constitutional privacy rights. However, American privacy regulation remain sector driven by statutes such as HIPAA for health data, COPPA[33] for protecting children's online privacy, and California's CCPA/CPRA[34] for consumer rights. There isn't a clear federal law about privacy, so application is not always the same. The PATRIOT Act

[30] Supra Note 22.
[31] Katz v. United States, 389 U.S. 347 (1967).
[32] Supra Note 16.
[33] Children's Online Privacy Protection Act, 1998 (U.S.A.).
[34] California Privacy Act, 2020 (U.S.A.).

 [ISSN 2581-5369]

(2001)[35] and the Foreign Intelligence Surveillance Act (FISA, 1978) give the government a lot of power to keep an eye on what people do. This broken system tries to keep people's private information safe, but it leaves gaps in comprehensive privacy protections.

People in authoritarian countries only have privacy rights on paper. For example, Article 40 of China's constitution and Article 23 of Russia's constitution. This is because these rights are limited for the sake of national security. China's laws such as Personal Information Protection Law (PIPL) and Cybersecurity Law gives state agencies access to huge tons of data without any possibility of any independent judicial oversight, also surveillance has been embedded into governance structure using the social credit system. Russia also has law named Yarovaya Law which makes it mandatory to retain telecom metadata for 1 year[36], which could be accessed by security services without court permission. The SORM system expands real-time surveillance further in wartime legislation.[37] Overall, we can say that privacy is largely symbolic and subordinated to state interests in these authoritarian countries.

This type of dual structure legitimises the authoritarian control keeping the state interests ahead of individual rights. Thus, while democratic countries codify privacy as a fundamental as well as enforceable right restricted by principles of necessity and proportionality, authoritarian countries put the privacy obligations under the broader framework subordinating the individual rights as against state sovereignty and security prerogatives.

(B) Surveillance Powers and Proportionality

A key difference in how the democracies shape its surveillance powers lies on the necessity and proportionality tests, ensuring that any sort of intrusion if done must be necessary, appropriate, and be balanced against individual rights. In E.U., any interference with fundamental rights must be suitable, necessary, and proportionate. A test is applied in CJEU rulings such as Schrems II[38] which invalidated the Privacy Shield. Surveillance is curtailed through security obligations (Article 32), data protection impact assessments (Article 35) for high-risk activities, enforced by independent supervisory authorities (Articles 51-59). Conversely, the U.S. legal framework shows ambivalence: U.S. law balances Fourth Amendment rights with national security. It has historically prioritised national security with a looser proportionality framework.

[35] Providing Appropriate Tools Required To Intercept And Obstruct Terrorism, 2001 (U.S.A.).
[36] E. Moyakine, A. Tabachnik, "Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived legislation in the age of modern technology" 40 *Computer Law & Strike Review* 105512 (2021).
[37] Andrei Soldatov, Irina Borogan, "Russia's Surveillance State" Center for European Policy Analysis. Oct. 26, 2022.
[38] Supra Note 15.

Carpenter case limited the government access to cell phone location data without a warrant, but FISA § 702 permit warrantless surveillance under broad national security mandates.[39] The PATRIOT Act expanded surveillance by authorizing roving wiretaps, delayed notification warrants, and access to business records[40] under Section 215, aimed at terrorism prevention but criticized for eroding privacy.

In authoritarian states, proportionality is largely absent or subordinated to expansive definitions of "national security" and "public interest." China's PIPL permits state agencies to bypass consent[41] for "national security" or "public interest," and the Cybersecurity Law compels companies to provide data to authorities on demand. The social credit system integrates surveillance into governance, blurring privacy protections. Russia's SORM system allows full-spectrum interception without judicial checks.[42]

These divergent frameworks result in fundamentally different surveillance practices. EU Member States conduct targeted, risk-assessed surveillance with legal proportionality checks enforced by independent DPAs and courts, while U.S. surveillance remains broad but incrementally constrained by case law. In contrast, Chinese and Russian regimes implement blanket data retention and real-time monitoring justified by sweeping security prerogatives, lacking any meaningful proportionality principle to protect individual privacy against state overreach.

(C) Institutional Oversight and Judicial Independence

The efficacy of privacy protections heavily depends on independent institutional oversight. The EU's decentralized but autonomous Data Protection Authorities and European Data Protection Board oversee GDPR under Article 52[43] with consistent effective enforcement powers,[44]. The CJEU provides judicial oversight, reviewing national measures for conformity with EU

[39] Office of the Director of National Intelligence et al., "Joint Statement for the Record: Section 702 of the Foreign Intelligence Surveillance Act" (Washington D.C.: U.S. Department of Justice, 2023) available at: https://www.justice.gov/d9/2023-06/Section%20702%20of%20the%20Foreign%20Intelligence%20Surveillance%20Act.pdf (last visited Sep. 1, 2025).

[40] Congress, "H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001" (U.S.A.) available at: https://www.congress.gov/bill/107th-congress/house-bill/3162 (last visited Sept 2, 2025).

[41] China's Draft 'Personal Information Protection Law' (Full Translation), available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/ (last visited on Sept 1, 2025).

[42] Roman Zakharov v. Russia (judgement) (2015) ECHR 47143/06.

[43] General Data Protection Regulation, 2016, Art. 52.

[44] The European Data Protection Board (EDPB), EU, available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_en (last visited on Sept 1, 2025).

fundamental rights and data protection standards.[45] It exemplifies democratic accountability in public law.

In the U.S., the Foreign Intelligence Surveillance Court works in secrecy with no adversarial process reviewing government surveillance applications ex-parte[46], while Fourth Amendment challenges are scattered across federal circuits, rendering oversight inconsistent. Nonetheless, courts have begun expanding digital privacy rights.

By contrast, in authoritarian regimes institutional independence is almost non-existent. China's Cyberspace Administration administers PIPL and Cybersecurity Law, operates under direct political control, lacking operational autonomy and independence.[47] Judicial interpretations are also limited. Russia's Roskomnadzor enforces data localization and blocks non-compliant services, yet its actions are unchallenged by courts.[48] Surveillance systems like SORM operate with minimal legal oversight, reinforcing authoritarian control over digital spaces.

These formal guarantees yield higher enforcement in democracies: EU DPAs imposed 2245 GDPR fines totalling €5.65 billion[49], compared to CCPA/CPRA where Michael Macko who is Deputy Director for Enforcement at the California Privacy Protection Agency (CPPA), presented enforcement updates reporting that the CPPA received 1,208 complaints between July 6, 2023, and February 22, 2024[50], awarding up to USD 750 per violation.[51]

By contrast, China's PIPL imposes fines up to RMB 50 million or 5% of a company's annual turnover. Companies may be suspended until compliance is confirmed. Individuals responsible can be liable for fines up to RMB 1 million.[52] And for enforcement Shanghai's Cyberspace Administration launched its first PIPL enforcement on 29 January 2024 after the "Shining Sword" campaign (June–December 2023), which investigated 6,043 companies, interviewed 520, and filed 50 violation cases. The operation was renewed in June 2024, leading to six disclosed cases against coffee chains (COSTA, Luckin) and findings of 21 non-compliant apps.[53] and Russia publishes no comparable data.

---

[45] Court of Justice of European Union, "Fact sheet Protection of personal data" (July, 2024).
[46] Brennan Center for Justice at New York University School of Law, "What Went Wrong With the FISA court" (2015).
[47] Supra Note 9.
[48] Human Rights Watch, "Disrupted, Throttled, and Blocked: State Censorship, Control, and Increasing Isolation of Internet Users in Russia" (July 30, 2025).
[49] Supra Note 18.
[50] California Privacy Protection Agency, "Enforcement Update & Priorities" (March 8, 2024).
[51] Supra Note 5.
[52] Ernst & Young, "How China's new regulations on data privacy and security could impact your business" (2022).
[53] PIPL: Navigating the Evolving Data Protection Landscape in China, available at: https://www.wr.no/aktuelt/pipl-navigating-the-evolving-data-protection-landscape-in-china (last visited on Sept 4, 2025).

These types of differences highlight how important is it to have independent regulators as well as judicial review for protecting the privacy which is not available in authoritarian countries. Thus, leading to weak enforcement mechanism.

(D) Practical Dimension: Social and Human Rights Implication

These practical points of view look at how privacy laws are followed, what rules do, and how rules about surveillance change society. People trust digital technology more in democratic countries with strong privacy laws. These laws can also make it harder for people to speak out and for free association of groups. Many countries misuse the technologies such as biometrics, social credit scoring as well as predictive policing which is a matter of grave concern especially in authoritarian countries. Many of the ruling governments also started employing surveillance to target those who try to defend their rights or go against them.[54] Example of this is clearly visible in China where it is used to silence if anyone try to go against them e.g. China uses facial recognition system for ethnic profiling, Russia also uses tech to repress digital freedom. Nowadays the authoritarian countries have increased their ambit to use these technologies even beyond the country borders, thus leading increased surveillance on the citizens. Such technological advancements allow authoritarian countries to easily target the offline as well as online dissent and target selected groups.

III. CHALLENGES IN BALANCING PRIVACY AND SECURITY IN THE DIGITAL AGE

Countries having either authoritarian or democratic governments always have trouble finding the right balance between privacy and security. Democratic countries are trying to improve their surveillance in response to new threats and advances in technology. However, they must follow the rules of necessity and proportionality. One of the rules that these rules are based on is the E.U.'s GDPR. It needs permission and only lets you collect the least amount of data, but there are some security exceptions. The talks that are still going on about how the government can get encrypted data that make the problems very clear. In democratic countries, surveillance may increase in response to threats of terrorism or cybercrime, which could put the rule of law and accountability at risk. The US government is trying to get encrypted data, but the battle to keep people's privacy safe is still going on.[55] This shows how important it is to work together to make better rules. But in authoritarian countries, these problems get worse because people have

[54] Richard Ashby Wilson, "The Anti-Human Rights Machine: Digital Authoritarianism and The Global Assault on Human Rights" *University of Connecticut* (Aug, 2022).

[55] How can we balance security and privacy in the digital world?, available at: https://www.diplomacy.edu/blog/how-can-we-balance-security-and-privacy-in-the-digital-world/ (last visited on 4 Sept, 2025).

different ideas about what is important. They say that more spying will make people safer, even if it means taking away people's rights or going after people who show dissent.[56] Ultimately, being transparent is the best way to find a balance between safety and security. Everyone who has a stake in the issue needs to work together to meet the big challenge of balancing privacy and security. This study demonstrates that regulations and statutes impact the balance between privacy and security.

(A) Findings

A comparative analysis of democracies and authoritarian regimes reveals significant differences in the conceptualisation, protection, and enforcement of digital privacy rights. This study produces substantial findings that directly address the research questions, resulting from a comparative analysis of digital privacy and surveillance frameworks in democratic and authoritarian regimes:

1. The way the constitution is written and the fact that institutions are independent are better signs of how well digital privacy is protected than just having laws about constitutional rights. The European Union's robust enforcement demonstrates this principle: by March 2025, EU Data Protection Authorities have imposed over 2,245 GDPR fines totalling approximately €5.65 billion[57], with independent DPAs operating under complete autonomy as mandated by GDPR Article 52. So we can say that, in democracies, privacy is entrenched either as an explicit right (EU Charter of Fundamental Rights, Article 7 & 8) or as an evolving judicial construct (US). By contrast, authoritarian regimes provide nominal recognition (China Constitution, (Article 40); Russia Constitution, (Article 23) but subordinate privacy to state imperatives through statutory derogations as China's Cyberspace Administration of China (CAC), which operates under Party direction and lacks operational independence, and Russia's Roskomnadzor, whose enforcement actions face virtually no judicial reversal. Hence, formal recognition alone is insufficient; privacy remains meaningful only where judicial and institutional independence enforce it.
2. Democracies condition surveillance on proportionality and necessity (CJEU, Digital Rights Ireland), whereas authoritarian states legitimize blanket surveillance through security laws. China's PIPL permits state agencies to bypass consent requirements for broadly defined "national security" or "public interest" purposes, while Russia's SORM

[56] Daniel J. Solove, "PRIVACY IN AUTHORITARIAN TIMES: SURVEILLANCE CAPITALISM AND GOVERNMENT SURVEILLANCE" *George Washington University Law School* (2025).
[57] Supra Note 18.

system grants the FSB direct access to communications metadata under the Yarovaya framework without judicial authorization. Hence, proportionality principle acts as the central differentiator between democratic and authoritarian approaches.

3. Independent data protection authorities in democracies contrast with party-controlled or state-aligned regulators in authoritarian states. Democratic systems provide meaningful individual recourse through layered administrative and judicial mechanisms. Under GDPR Articles 77-84, individuals can lodge complaints with independent DPAs, seek administrative penalties, and pursue judicial damages. This effectiveness is evidenced by enforcement statistics: Spain leads with 932 published fines, followed by Italy, Romania, and Germany with substantial enforcement activity.[58] U.S. remedies, while fragmented, include constitutional litigation (*Carpenter*)[59] and statutory actions under state laws like California's CCPA/CPRA, which provides statutory damages of $100-$750 per violation.[60] In stark contrast, China's PIPL offers no private right of action against government surveillance, and Russian courts routinely defer to security agencies, rendering legal remedies largely ineffective. Hence, presence of oversight bodies is not decisive rather their independence and capacity to sanction state actors determine their effectiveness.

4. Digital surveillance systems generate profound social and human rights consequences that vary systematically between democratic and authoritarian governance models. Research demonstrates that surveillance technologies create "chilling effects" that extend far beyond direct targets, fundamentally altering social behaviour and democratic participation.[61] In democracies, surveillance is often challenged as violating fundamental rights such as privacy. Cases like *S and Marper v UK* (2008)[62] and *Carpenter v United States*[63] highlight that excessive data retention or location tracking infringes on dignity and autonomy. It may also lead to discouraging activism, online dissent, and free association. In authoritarian regimes, however, surveillance is framed as a legitimate tool for “social stability,” with courts rarely acting as rights-protective bodies. The surveillance systems like China’s AI-driven facial recognition create

[58] Supra Note 18.
[59] Supra Note 16.
[60] Supra Note 5.
[61] Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki, Amy Stevens, “The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe” 16 1 *Journal of Human Rights Practice* 397-412 (2023).
[62] S and Marper v United Kingdom [2008] ECHR 30562/04.
[63] Supra Note 16.

pervasive self-censorship and social conformity. China's deployment of facial recognition for ethnic profiling and Russia's use of digital surveillance for political suppression demonstrate how technological advancement amplifies existing authoritarian tendencies.[64] Therefore, social and human right protections are substantive only in democracies with independent judiciary whereas authoritarian regimes institutionalize fear as a tool of governance.

5. Democracies struggle with the balance—privacy is constitutionally protected, but exceptions for security are growing. Authoritarian states do not attempt balance—security automatically prevails over privacy. Jurisdictions with codified transparency obligations (EU) maintain stronger checks on surveillance scope and foster public trust by embedding transparency and proportionality obligations. By contrast, authoritarian regimes prioritize security at the expense of privacy, with no meaningful mechanisms to balance surveillance and individual rights.

IV. LIMITATIONS

This study's comparative public-law approach provides a robust doctrinal and institutional analysis of digital privacy and surveillance across democratic and authoritarian systems. Despite the comprehensive scope of this research, several limitations must be acknowledged to contextualize the findings and prevent overgeneralization:

- Reliance on Publicly Available Sources- The analysis depends on publicly accessible legal texts, enforcement reports, and scholarly publications. Classified surveillance practices and internal regulatory deliberations in China and Russia remain opaque, limiting insight into the full scope of state surveillance operations.
- Key legal materials, regulatory guidelines, and judicial decisions in China and Russia are published primarily in Mandarin and Russian, respectively with official English translations often unavailable or selectively released. Reliance on translated versions may introduce interpretive nuances, biases or omissions, potentially affecting the accuracy of doctrinal analysis. The analysis has therefore relied on secondary sources, translations, and reports, which may carry interpretive biases or omit critical nuances
- Dynamic Nature- Digital privacy is a rapidly evolving field, particularly with

[64] European Parliament, "Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights" (May, 2024).

 [ISSN 2581-5369]

emerging technologies such as artificial intelligence, biometric surveillance, and cross-border data transfers. Laws such as the EU's GDPR, the U.S. state-level privacy acts, China's Personal Information Protection Law (2021), and Russia's evolving Yarovaya framework continue to undergo amendments and reinterpretations. Therefore, the findings reflect the legal position as of 2025, but subsequent reforms may alter the comparative balance.

- Institutional Practice vs. Formal Design- While the research distinguishes between statutory recognition and actual enforcement, measuring institutional independence and effectiveness remains inherently challenging. For example, the EU Data Protection Authorities may be formally independent under GDPR Article 52, yet enforcement intensity varies widely across Member States (European Data Protection Board, 2023). Conversely, the opaque nature of Chinese and Russian administrative practices makes it difficult to determine the full extent of surveillance operations. Chinese and Russian administrative enforcement actions lack detailed public records, impeding precise measurement of regulatory intensity.
- Jurisdictional Scope and Selection Justification- This study focuses on four exemplar jurisdictions—the United States, European Union, China, and Russia—selected for their global influence, distinct legal traditions, and contrasting governance models. These jurisdictions also offer relatively extensive publicly available data on legal frameworks and enforcement actions. In contrast, comparable data for many other democracies or hybrid regimes are less systematically documented or accessible, hindering rigorous comparative public-law analysis.

V. SUGGESTIONS

- For Democracies-

1. The U.S. should address its fragmented statutory landscape by enacting a comprehensive federal privacy legislation, harmonising state-level laws with constitutional principles. This legislation can take inspiration from the GDPR, tailored in a way it to respect U.S. federal structure, ensuring nationwide uniformity, clearer corporate obligations, and enhanced individual remedies.
2. There should be mandatory adversarial review processes or independent audits of surveillance activities carried out under statutes like FISA and PATRIOT Act. Periodic transparency reports and accountability mechanisms would foster public trust and uphold democratic oversight.

 [ISSN 2581-5369]

3. People should have more ways to get together and file complaints, like class-action lawsuits or group complaints. This will give people and groups in civil society more power to stop privacy violations that happen all the time.
4. Every year, law enforcement and intelligence agencies should have to make public reports that show how many requests they get for surveillance and data access, what kinds of requests they get, and what legal protections they have.
5. Democratic nations must prevent terrorism and cybercrime from leading into pervasive surveillance systems. When they make laws, they should think about how fair they are. Courts should also try to find a balance between safety and privacy.
6. People need to know what their privacy rights are so they can protect them from the government and businesses.
7. Countries should think about how digital rights affect similar to how we check the environment impact assessment. This would mean that businesses and governments would be legally responsible for how their digital products and policies affect people's privacy.

- For Authoritarian States
    1. Adding even small protections, like limited judicial review where judges can look at surveillance warrants or giving regulators more freedom which could make it accountable without hurting the state's claims about safety.
    2. Making it mandatory for telecom companies and state agencies to file yearly transparency reports similar to GDPR's disclosure rules, it could make people more aware and open chances for international scrutiny.
    3. Even when there are restrictive conditions, getting academics, NGOs, and international organisations involved in privacy debates could make the government change its ways and make sure that what it does is in line with international human rights standards.

- Global Standards
    1. International organisations such as U.N., O.E.C.D., and G20 shall take initiatives so that essential principles such as of proportionality, necessity, consent, transparency and redress become universally accepted in every country.

 [ISSN 2581-5369]

2. Researcher suggests there must be creation of body which act as international privacy watchdog which could work with public agencies, technology companies as well as societies to keep a check on compliance of above principles and issues independent reports on the same.

VI. Conclusion

This study shows that protecting digital privacy depends on more than just the law itself. It also depends on things like how the constitution is written, how fair the courts are, and how strictly the laws are implemented. The United States and European Union are two democratic regimes that protect privacy with laws based on rights that try to find balance between what is fair, what is necessity and what is judicially correct. But the protections aren't as strong in U.S. because the laws in the U.S. are fragmented. The GDPR in the E.U., on the other hand, sets a standard for how independent court reviews and being honest about what you are doing can help people trust you and find a balance between privacy and surveillance.

In contrast, China and Russia are authoritarian countries that have very different views. Article 40 of China's constitution and Article 23 of Russia's constitution say that privacy is only protected on face of it. These laws say that communication is private, but they are only on face of it and are always broken by laws that say they are needed for national security or public order. In real life, the needs of the state are given more importance than privacy. That is why it becomes legitimate to have lot of surveillance systems. Institutions do not have a lot of freedom because political leaders are the one who work with regulators and the courts.

The main difference is not whether there are privacy protections, but whether or not they can be enforced and whether or not there are free from oversight. Democracies aren't perfect as well, but they do have ways to hold people accountable and get things sorted. Authoritarian systems, on the other hand, put national security ahead of people's rights. The comparative lens shows how the most important constitutional ideas shape digital governance: democracies want to be seen as legitimate by protecting rights, while authoritarian regimes tries to keep things stable by controlling them.

 [ISSN 2581-5369]