Interdisciplinary Studies in Society, Law, and Politics 2026; 5(1): 1-10

ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

Privacy as Resistance: Legal Strategies Against State and Corporate Surveillance

Nikos. Papadakis[1], Mariana. Scouza[2*], Rafael. González[3]

[1] Department of Public Law, National and Kapodistrian University of Athens, Athens, Greece
[2] Department of Political Science, University of São Paulo, São Paulo, Brazil
[3] Department of Public Law, Universidad Central de Venezuela, Caracas, Venezuela

*** Corresponding author email address**: mariana.scouza@usp.br

Received: 2025-07-30 **Revised:** 2025-12-17 **Accepted:** 2025-12-24 **Published:** 2026-01-01

ABSTRACT

This study aims to examine legal strategies that serve as resistance mechanisms against state and corporate surveillance, with a focus on how privacy is conceptualized and mobilized through legal frameworks. This narrative review employs a descriptive analysis method, synthesizing scholarly literature, legal documents, judicial decisions, and international policy reports published between 2019 and 2024. The review is grounded in interdisciplinary theoretical frameworks and draws from comparative legal perspectives across jurisdictions. Legal resistance to state surveillance is primarily enacted through constitutional challenges, strategic litigation by civil society organizations, and transparency mechanisms such as Freedom of Information laws. Landmark cases have helped redefine privacy rights in the context of digital technologies. In the corporate domain, data protection laws like the GDPR and CCPA empower individuals to assert control over their personal data through consent, access, and redress mechanisms. Strategic litigation and regulatory enforcement have begun to influence the practices of major technology companies. However, legal resistance is uneven across democratic and authoritarian regimes, and disparities between Global North and Global South countries reflect broader structural inequalities. Limitations such as legal capture, public disengagement, and jurisdictional fragmentation present ongoing challenges. Legal frameworks offer critical tools for resisting surveillance and reclaiming privacy, yet their efficacy depends on political, institutional, and social contexts. While not a panacea, legal strategies form an essential component of broader resistance efforts aimed at ensuring autonomy and accountability in the digital age.

Keywords: *Privacy, Legal Resistance, Surveillance, Data Protection, Human Rights, Strategic Litigation, Digital Autonomy*

How to cite this article:

Papadakis, N., Scouza, M., & González, R. (2024). Privacy as Resistance: Legal Strategies Against State and Corporate Surveillance. *Interdisciplinary Studies in Society, Law, and Politics, 5*(1), 1-10. https://doi.org/10.61838/kman.isslp.463

1. Introduction

In recent years, the convergence of state-driven surveillance and corporate data extraction practices has reshaped the boundaries of individual privacy across the globe. This transformation, often conceptualized under the framework of "surveillance capitalism," denotes a new economic order where personal data is commodified, collected, and utilized for profit without explicit consent or transparency. Corporations, particularly within the technology sector, have developed sophisticated infrastructures to harvest user behavior, preferences, and biometric information under the guise of personalization and convenience. At the same time, states have expanded their surveillance

capabilities, often in the name of national security, crime prevention, and public health. For instance, facial recognition technologies, once confined to state intelligence operations, are now embedded in everyday financial transactions and consumer environments, creating intricate networks of monitoring that blur the line between public and private oversight. These developments have generated growing concern about the erosion of privacy and the normalization of data surveillance as an uncontested reality of modern life.

The intensification of surveillance practices has provoked critical responses from both scholars and activists who now regard privacy not merely as a personal right, but as a political stance—a form of resistance against asymmetric power structures. Privacy, in this context, transcends the notion of mere data protection and evolves into a counter-hegemonic practice. It becomes a shield through which individuals and communities can challenge the invisible reach of algorithms, automated profiling, and surveillance infrastructures. The shift from privacy as a passive entitlement to privacy as an active resistance strategy is reflected in a growing body of literature that explores how people disconnect, obfuscate, or strategically reveal information as acts of autonomy and defiance. According to Swanlund, the deliberate disconnection from digital platforms, for example, represents not just a retreat from surveillance but a conscious reassertion of agency in an environment increasingly structured by geosurveillance systems (Swanlund, 2021). Similarly, in the context of facial recognition technologies, users often exhibit resistance through avoidance behaviors or legal complaints rooted in privacy violations, highlighting the role of privacy in contesting technological overreach (Cheng et al., 2022).

Legal frameworks play a central role in enabling and legitimizing such acts of resistance. Through constitutional protections, statutory regulations, and judicial interventions, legal systems provide the scaffolding through which privacy claims can be articulated and defended. Laws such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) have emerged as potent tools for citizens to challenge unlawful data practices and demand transparency. However, the legal terrain remains uneven, often shaped by conflicting interests between state security imperatives, corporate profit motives, and individual rights. McElroy highlights the growing tension between cybersecurity responses designed to protect national infrastructure and the potential for these measures to serve as conduits for extensive information warfare and domestic surveillance (McElroy & McKee, 2023). In parallel, Rizzo underscores how corporate surveillance, particularly when gendered, can reinforce discriminatory social hierarchies, demanding nuanced legal approaches that go beyond conventional data protection paradigms (Rizzo, 2023).

This review sets out to explore the legal strategies that individuals, communities, and organizations employ to resist state and corporate surveillance. The aim is to map these strategies across multiple jurisdictions, assess their effectiveness, and evaluate the underlying legal and ethical principles that support them. By examining privacy as a form of resistance, the study shifts the focus from mere compliance with privacy laws to proactive legal mobilization against surveillance practices. Central to this analysis is the recognition that law is not a static set of rules but a dynamic field of contestation where privacy claims are negotiated, resisted, and transformed. In doing so, the review highlights both the limitations and potential of legal tools in empowering resistance and fostering democratic accountability.

To this end, the study poses several guiding questions: What legal mechanisms have been employed to resist surveillance practices? How have courts and legislatures interpreted privacy in the context of resistance? What are the key challenges and limitations of using legal frameworks to counter surveillance? And how do these strategies vary across cultural, political, and economic contexts? The scope of the review encompasses both state-led and corporate surveillance, focusing on legal responses from the past five years to ensure relevance to contemporary issues. By integrating comparative perspectives, the review seeks to uncover patterns, contradictions, and innovations in privacy jurisprudence that reflect broader shifts in the politics of digital rights.

Ultimately, the study aims to contribute to the growing field of surveillance studies by offering a legally grounded yet interdisciplinary analysis of privacy as resistance. Rather than merely cataloging legal provisions, it interrogates the relationship between law, power, and technology, revealing how resistance is crafted through legal narratives, institutional actions,

and social mobilizations. In doing so, it foregrounds privacy not as a retreat into secrecy, but as a declaration of autonomy in an age of pervasive visibility.

2. Methodology

This narrative review employs a descriptive analysis method to explore and synthesize legal strategies utilized as forms of resistance against both state and corporate surveillance. The objective is not only to map existing legal mechanisms but also to critically examine their theoretical foundations, practical implementations, and contextual variations across jurisdictions. Rather than relying on systematic review protocols, the narrative approach allows for greater flexibility in engaging with interdisciplinary sources, theoretical frameworks, and landmark legal cases that define privacy as a form of resistance. This method supports a deeper understanding of the evolving relationship between law, power, and technological surveillance in diverse sociopolitical settings.

In conducting this study, legal documents, scholarly articles, judicial decisions, and policy reports were selected and analyzed using a descriptive lens. The sources were collected from peer-reviewed law journals, public policy databases, and legal archives such as HeinOnline, Westlaw, and JSTOR. The selection of materials was limited to publications and cases between 2019 and 2024, ensuring that the review reflects the most recent legal developments and scholarly insights. Priority was given to sources that directly address legal responses to surveillance practices, including constitutional challenges, privacy legislation, regulatory frameworks, and strategic litigation. In addition to academic literature, reports from international bodies such as the United Nations and the European Data Protection Supervisor were included to provide a broader global context.

The process of data analysis involved the descriptive categorization of legal strategies into two major domains: responses to state surveillance and responses to corporate surveillance. These categories were then further examined through the lens of relevant theoretical perspectives, including critical legal studies, privacy theory, and surveillance studies. Landmark cases and legal precedents were highlighted not only to illustrate how courts have interpreted the right to privacy in resistance contexts but also to reveal the limitations and potentials of judicial mechanisms in confronting modern surveillance architectures. The descriptive analysis focused on identifying patterns, recurring legal arguments, and the role of civil society in mobilizing privacy rights within judicial and legislative arenas.

By synthesizing findings from diverse jurisdictions—including the United States, the European Union, India, and select Global South nations—the study sought to uncover both convergences and divergences in how privacy is deployed as a resistance tool. The narrative review approach also allowed for the integration of interdisciplinary perspectives, particularly those from political theory, sociology, and human rights law, enriching the legal analysis and anchoring it within broader discourses on power, autonomy, and democratic accountability. Through this method, the article presents a cohesive and critical portrait of legal resistance to surveillance in the early 21st century.

3. Theoretical and Conceptual Framework

The theoretical foundations of this study are grounded in critical theories of surveillance, particularly Michel Foucault's concept of panopticism and Shoshana Zuboff's articulation of surveillance capitalism. Foucault's panopticon metaphor, drawn from Jeremy Bentham's prison design, illustrates a system of power where individuals internalize the gaze of authority and modify their behavior accordingly. Although Foucault conceptualized this in the context of disciplinary institutions, the metaphor has been widely applied to contemporary digital environments where individuals are subject to invisible, algorithmic forms of monitoring. Lim draws on this legacy to argue that traditional notions of privacy are insufficient in countering today's digital surveillance apparatus, which not only watches but also predicts and manipulates behavior through datafication (Lim, 2023). This predictive surveillance forms the backbone of what Zuboff has termed "surveillance capitalism," a system in which personal experiences are transformed into behavioral surplus and used to shape future actions through targeted advertising, algorithmic sorting, and automated decision-making (Wagner et al., 2023).

Within this theoretical landscape, privacy is reinterpreted as both a site of power and a terrain of resistance. Rather than being merely a defensive right, privacy becomes a proactive assertion of autonomy.

Watson and Lupton explore how individuals construct digital privacy narratives not solely as concerns about exposure but as expressions of affective agency and emotional negotiation in relation to their online presence (Watson & Lupton, 2020). Their findings suggest that users adopt diverse strategies—ranging from self-censorship to technological disengagement—as ways to reclaim control over their identities and relationships in digital space. These strategies underscore the importance of conceptualizing privacy as more than a legal status; it is a form of ethical and political practice aimed at resisting domination.

The framing of privacy as resistance also draws upon international human rights law, where the right to privacy is enshrined as a fundamental liberty. Legal documents such as the International Covenant on Civil and Political Rights (ICCPR) affirm the right to privacy as essential for the dignity and freedom of the individual. However, the practical realization of this right often depends on national legal systems, which may interpret and implement it in ways that either empower or suppress resistance. For example, in jurisdictions where data protection laws are robust, individuals can file legal complaints, demand data transparency, and seek remedies for privacy violations. Cheng's research on resistance to facial recognition payment systems highlights how privacy concerns can translate into legal objections and influence user behavior, particularly when supported by regulatory frameworks that allow for legal recourse (Cheng et al., 2022). Conversely, in environments where privacy protections are weak or absent, legal resistance is often stifled or redirected through extrajudicial means.

To further analyze the relationship between privacy and resistance, the study also engages with theories of legal consciousness and resistance jurisprudence. Legal consciousness refers to the ways in which individuals perceive and interact with the law in their everyday lives. It shapes not only whether people believe the law can serve as a tool of resistance but also how they mobilize legal language and institutions in pursuit of justice. Spinello emphasizes that in the face of technological opacity and state secrecy, citizens may feel compelled to "go dark," adopting privacy-preserving technologies or rejecting digital platforms altogether as a form of ethical resistance (Spinello, 2020). This disengagement is not only technological but also symbolic, reflecting a rejection of institutional trust and a reimagining of autonomy beyond legal recognition.

Resistance jurisprudence, as a conceptual extension, considers the law not as a monolith but as a contested space where marginalized groups challenge dominant interpretations and assert alternative legal meanings. Rizzo's examination of gendered surveillance reveals how surveillance practices disproportionately affect women and other marginalized groups, making privacy not only a general concern but a site of intersectional struggle (Rizzo, 2023). In such contexts, legal strategies must be attentive to structural inequalities and the ways in which surveillance both reflects and reinforces social hierarchies.

Taken together, these theoretical and conceptual lenses provide a robust framework for analyzing legal strategies against surveillance. They allow for a nuanced understanding of privacy as a dynamic and context-dependent construct—one that is shaped by legal norms, political ideologies, technological infrastructures, and cultural practices. By grounding the analysis in these theories, the study positions privacy not as a relic of liberal individualism, but as a critical resource in the ongoing struggle for democratic accountability, social justice, and human dignity in the digital age.

4. Legal Strategies Against State Surveillance

The expansion of state surveillance powers in the digital age has prompted a significant legal backlash grounded in constitutional principles, statutory safeguards, and strategic litigation. Across democracies, constitutional provisions serve as the first line of defense against intrusive surveillance. In the United States, the Fourth Amendment protects citizens against unreasonable searches and seizures, a clause that has been reinterpreted in recent years to accommodate the challenges posed by digital technologies. One notable example is *Carpenter v. United States*, in which the Supreme Court ruled that the government must obtain a warrant to access historical cell site location information. This landmark decision recognized that individuals maintain a reasonable expectation of privacy in their digital footprints, even when that data is stored by third parties. The ruling reflected a growing judicial awareness of the implications of mass data collection and marked a shift in how courts interpret privacy rights

in the context of modern surveillance technologies (Spinello, 2020).

In Europe, similar protections are embedded in the Charter of Fundamental Rights of the European Union, particularly Article 7 (respect for private and family life) and Article 8 (protection of personal data). These rights have been central to challenges against disproportionate surveillance laws, most notably in *Digital Rights Ireland*, a case that led the Court of Justice of the European Union to invalidate the Data Retention Directive for violating fundamental rights. The court emphasized that indiscriminate retention of communication data without sufficient safeguards was incompatible with democratic principles. This ruling not only influenced subsequent EU legislation but also inspired similar legal strategies in other jurisdictions (Wagner et al., 2023).

Strategic litigation by civil society organizations has emerged as a powerful mechanism for challenging the legality and scope of surveillance programs. In the United States, groups such as the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF) have played pivotal roles in contesting surveillance laws and policies. These organizations often initiate lawsuits that test the boundaries of constitutional rights, leveraging public interest litigation to create legal precedents. For example, following the revelations of mass surveillance by Edward Snowden, the ACLU filed a series of lawsuits against the National Security Agency's (NSA) metadata collection programs, arguing that these practices violated the Fourth Amendment. These efforts not only yielded legal victories but also brought public attention to the expansive nature of state surveillance and the lack of oversight mechanisms (McElroy & McKee, 2023).

The use of transparency laws such as the Freedom of Information Act (FOIA) has also become instrumental in resisting state surveillance. FOIA allows individuals and organizations to request information from government agencies, thereby exposing the scope and methodology of surveillance practices. Although FOIA requests are often met with redactions or denials on grounds of national security, they remain an essential tool for accountability. Advocacy groups frequently use FOIA to uncover secret surveillance programs or to challenge the classification of information as state secrets. In many cases, the data obtained through FOIA serves as the basis for further legal action, creating a feedback loop of resistance. For instance, documents obtained through FOIA helped reveal the extent of facial recognition deployment by local law enforcement agencies in the United States, prompting legal challenges and policy reforms (Cheng et al., 2022).

One critical dimension of legal resistance lies in the challenge to surveillance technologies that operate without meaningful oversight. As surveillance capabilities increasingly rely on biometric and predictive technologies, the legal system is called upon to define the boundaries of lawful data collection and use. Facial recognition, predictive policing algorithms, and automated license plate readers raise novel questions about consent, proportionality, and due process. Cheng argues that public resistance to facial recognition is often driven by privacy concerns rooted in a broader mistrust of institutional data governance, which in turn motivates legal and policy actions aimed at limiting or banning such technologies (Cheng et al., 2022). These legal responses often materialize through local ordinances, moratoriums, and court rulings that assert the need for transparency and consent in state surveillance.

International human rights mechanisms also support legal strategies against state surveillance. The United Nations Human Rights Committee has emphasized that surveillance programs must comply with principles of legality, necessity, and proportionality, especially when they involve cross-border data flows. Although these declarations are not always binding, they offer normative support for legal challenges at the national level. In countries where domestic legal remedies are limited, appeals to international human rights bodies provide an alternative path for contesting surveillance practices. Wagner highlights how digital rights advocacy has increasingly embraced international forums to challenge the global reach of state surveillance and to promote transnational privacy standards (Wagner et al., 2023).

These legal strategies—constitutional litigation, strategic lawsuits, transparency laws, and international advocacy—interact in complex ways to form a multilayered resistance against state surveillance. While each approach has its own limitations, together they constitute a dynamic legal ecosystem in which privacy is continuously negotiated and defended. The resilience of this ecosystem depends not only on legal texts but also on the mobilization of civil society, the responsiveness of

courts, and the willingness of states to balance security concerns with fundamental rights. In this context, privacy becomes a legal and political project that resists the normalization of surveillance and reasserts the value of individual autonomy in democratic societies.

5. Legal Strategies Against Corporate Surveillance

The legal response to corporate surveillance has evolved in tandem with the growing influence of technology firms that harvest, monetize, and commodify user data. As platforms such as Meta, Google, and Amazon integrate data collection into every aspect of the user experience, legal frameworks have sought to regulate these practices through comprehensive data protection laws. The European Union's General Data Protection Regulation (GDPR) stands as the most prominent example, offering a rights-based approach to data governance. The GDPR grants individuals extensive control over their personal data, including the right to access, rectify, and erase data, as well as the right to object to processing. These provisions enable users to actively resist surveillance by asserting legal claims against data controllers who fail to comply with the law. According to Watson, the narrative of digital privacy has become central to how users interpret their relationship with technology companies, often resulting in demands for greater accountability and legal enforcement (Watson & Lupton, 2020).

Similarly, in the United States, the California Consumer Privacy Act (CCPA) provides users with the ability to opt out of data sales and request disclosure of information collected by companies. While the CCPA is less comprehensive than the GDPR, it reflects a growing recognition of the need for consumer-oriented legal tools to counterbalance the asymmetries of power in the digital marketplace. As Gowthami notes in her analysis of data protection in the context of autonomous vehicles, the legal landscape is increasingly shaped by the tension between technological innovation and the imperative of safeguarding personal data from misuse (Gowthami & V, 2024). These legal protections not only serve to limit corporate overreach but also empower users to make informed decisions about their digital presence.

One of the key mechanisms through which users exercise legal resistance is the framework of consumer consent. Under both the GDPR and CCPA, data processing must be based on informed and freely given consent. This requirement challenges companies to design interfaces and business models that prioritize user autonomy rather than exploit default settings or opaque policies. Lim argues that these legal constraints disrupt the architecture of surveillance capitalism by introducing friction into data flows, forcing companies to negotiate with users over the terms of data access and use (Lim, 2023). Although critics have pointed out that consent fatigue and information asymmetry undermine the effectiveness of opt-in models, legal requirements around consent have nonetheless become a battleground for contesting exploitative data practices.

Beyond individual consent, legal resistance to corporate surveillance is increasingly manifested through litigation and regulatory scrutiny. Strategic lawsuits against technology companies have emerged as a powerful tool to enforce data rights and hold corporations accountable for privacy violations. One of the most influential legal actors in this domain is Austrian activist Max Schrems, whose litigation against Facebook led to the invalidation of two major transatlantic data transfer frameworks—Safe Harbor and Privacy Shield. These decisions by the Court of Justice of the European Union underscore the inadequacy of U.S. privacy protections and affirm the primacy of EU data protection standards in cross-border data exchanges (Wagner et al., 2023).

The Schrems cases exemplify how legal strategies can have far-reaching implications for corporate surveillance practices, forcing companies to reassess their data governance structures. These legal victories also inspire similar actions in other regions, contributing to the globalization of data protection norms. Dc highlights how legal concerns about tactical privacy violations in specific sectors, such as sports technology, mirror broader anxieties about corporate surveillance in everyday life (Dc, 2023). As such, legal action serves not only to penalize non-compliance but also to reshape industry standards and foster regulatory innovation.

Regulatory enforcement complements litigation by imposing penalties and setting precedents for acceptable corporate behavior. Data protection authorities in the EU, such as the Irish Data Protection Commission, have issued substantial fines against tech giants for violations of the GDPR. These fines signal a shift from soft regulation to active enforcement, demonstrating that legal resistance can influence even the most powerful corporate actors. Rizzo contends that gendered dimensions of surveillance capitalism often go

unaddressed by mainstream legal frameworks, calling for more intersectional approaches that recognize how data extraction disproportionately affects marginalized groups (Rizzo, 2023). Incorporating these perspectives into legal strategies is essential for ensuring that resistance is inclusive and responsive to diverse experiences of surveillance.

While legal frameworks have made significant strides in curbing corporate surveillance, challenges remain. Many companies operate across jurisdictions with varying privacy standards, creating loopholes that allow for data exploitation. Moreover, the fast pace of technological development often outstrips the capacity of legal systems to adapt, resulting in regulatory lag. Nonetheless, the legal tools currently available—data protection laws, consent mechanisms, litigation, and regulatory enforcement—form a robust foundation for resistance. They provide individuals and civil society actors with avenues to challenge surveillance, demand transparency, and shape the ethical contours of the digital economy.

In this legal terrain, privacy is not merely a technical setting or contractual clause; it is a dynamic practice of resistance. It involves the assertion of rights, the mobilization of legal narratives, and the engagement with institutions that have the power to restrain corporate surveillance. By examining these strategies, this review underscores the transformative potential of law in confronting the structural and pervasive nature of surveillance capitalism.

6. Comparative and International Perspectives

The global landscape of legal resistance to surveillance reveals stark contrasts between privacy regimes in the Global North and the Global South, shaped by different political histories, institutional capacities, and developmental priorities. In the Global North, particularly in regions like the European Union, privacy is institutionalized as a fundamental right with enforceable legal frameworks such as the General Data Protection Regulation (GDPR). These regions tend to have strong regulatory bodies, independent judiciaries, and active civil societies that can hold both states and corporations accountable. For instance, the European Court of Justice has consistently acted as a bulwark against mass surveillance, most notably in decisions such as *Digital Rights Ireland*, which struck down blanket data retention laws due to their incompatibility with the EU Charter of Fundamental Rights (Wagner et al., 2023). This legal environment has enabled robust forms of legal resistance, from class-action lawsuits to public interest litigation, fostering a culture of rights assertion that extends across national borders.

In contrast, many countries in the Global South face significant obstacles in establishing and enforcing privacy protections. While some have adopted data protection laws modeled after the GDPR, the implementation and enforcement of these laws often remain weak due to limited institutional resources, politicized regulatory agencies, and underdeveloped judicial systems. Moreover, in several cases, surveillance practices are not only state-sanctioned but also embedded within broader strategies of political control. For example, authoritarian regimes may deploy biometric identification systems and digital monitoring tools to suppress dissent, monitor minority populations, or manipulate elections. In such contexts, legal resistance becomes exceedingly difficult. Swanlund observes that in many parts of the Global South, disconnection—rather than legal mobilization—emerges as a practical form of resistance, especially where state institutions are complicit in surveillance or unresponsive to legal challenges (Swanlund, 2021).

Despite these disparities, international human rights frameworks provide a normative foundation for global privacy advocacy. The International Covenant on Civil and Political Rights (ICCPR), ratified by most countries, enshrines the right to privacy in Article 17, mandating states to protect individuals from arbitrary or unlawful interference. The United Nations Special Rapporteur on the right to privacy has issued multiple reports highlighting the dangers of unchecked surveillance and emphasizing the need for legal safeguards that meet the standards of legality, necessity, and proportionality. These frameworks not only inform domestic legal reforms but also serve as tools for transnational advocacy. Civil society organizations often invoke international norms to pressure governments, raise awareness, and build coalitions across borders. Watson and Lupton argue that digital privacy narratives frequently transcend national contexts, suggesting that privacy consciousness is increasingly shaped by global discourses on rights and autonomy (Watson & Lupton, 2020).

A comparative lens also reveals notable differences in how democratic and authoritarian regimes address—or suppress—privacy rights. In liberal democracies, the presence of independent courts, free media, and participatory political systems creates an environment conducive to legal resistance. For example, organizations like the American Civil Liberties Union (ACLU) in the U.S. and Privacy International in the UK have effectively used litigation and policy advocacy to challenge surveillance laws and practices. McElroy notes that democratic systems often face internal contradictions between the imperative of national security and the constitutional commitment to civil liberties, leading to judicial interventions that delineate the permissible boundaries of state surveillance (McElroy & McKee, 2023). These tensions, while difficult to resolve, generate legal debates and precedents that incrementally shape privacy jurisprudence.

In authoritarian contexts, however, the law is frequently instrumentalized to legitimize surveillance rather than to constrain it. Legal systems in such regimes are often characterized by limited judicial independence, restricted civil liberties, and pervasive state control over digital infrastructure. Lim contends that under these conditions, privacy may be deemed subversive, and legal efforts to resist surveillance can result in retaliation or criminalization (Lim, 2023). Nevertheless, even in restrictive environments, forms of legal resistance persist—often through international litigation, encrypted communication, or alliances with global NGOs that offer legal and technical support. These efforts illustrate the resilience of privacy advocacy even under adverse political conditions.

The convergence of international legal norms and domestic legal strategies offers opportunities for cross-border learning and coalition-building. Comparative analyses underscore the need for adaptable legal models that consider local political contexts while aligning with universal human rights principles. As Gowthami observes in her examination of sector-specific data protections, the efficacy of legal resistance often depends on how well global standards are localized and enforced in domestic law (Gowthami & V, 2024). By engaging with both global and local frameworks, privacy advocates can craft more effective and context-sensitive legal strategies.

In sum, the comparative and international dimensions of legal resistance reveal a complex interplay between institutional capacity, political will, and normative commitments. While the Global North often sets the legislative and jurisprudential benchmarks, the Global South offers insights into grassroots resistance, normative resilience, and the creative adaptation of international legal tools. Together, these perspectives enrich our understanding of privacy as a global struggle shaped by uneven legal geographies and contested notions of sovereignty, rights, and resistance.

7. Challenges and Limitations of Legal Resistance

While legal strategies against surveillance have made notable advances, they remain constrained by several structural and practical limitations. One of the most pressing challenges is legal capture, where powerful corporate interests exert disproportionate influence over legislative and regulatory processes. Technology companies such as Meta and Google possess significant lobbying power and often shape the very regulations designed to oversee their operations. Rizzo points out that such corporate influence frequently results in diluted privacy laws that fail to address the systemic nature of surveillance capitalism, particularly its gendered and racialized dimensions (Rizzo, 2023). This imbalance not only undermines regulatory efficacy but also narrows the scope of meaningful legal resistance.

Jurisdictional fragmentation further complicates efforts to regulate surveillance, especially in cross-border data flows. While data protection laws like the GDPR apply extraterritorially, enforcement remains challenging when companies operate across multiple legal regimes with varying levels of protection. The Schrems cases illustrate the difficulty of reconciling European data protection standards with weaker U.S. privacy laws, raising questions about legal sovereignty and interoperability (Wagner et al., 2023). Moreover, data localization laws, often introduced to enhance state control over data, can paradoxically reinforce surveillance by mandating that data remain within jurisdictions where privacy protections are minimal or nonexistent.

Public disengagement and digital illiteracy pose additional obstacles to legal resistance. Watson emphasizes that many users lack the knowledge or resources to understand complex privacy settings, let

alone engage in legal action (Watson & Lupton, 2020). This gap between legal rights and public awareness limits the effectiveness of consent mechanisms and reduces the collective pressure needed to enforce privacy standards. In regions with lower internet literacy, such as parts of the Global South, this disengagement is often compounded by socioeconomic inequalities, making privacy an elite concern rather than a universal right.

Ethically, legal strategies can also fall short by prioritizing procedural compliance over substantive justice. Legal victories that impose fines or mandate policy changes may do little to challenge the structural dynamics of surveillance or to protect vulnerable populations. Spinello warns that even well-intentioned legal frameworks may inadvertently normalize surveillance by institutionalizing minimal standards, thereby shifting the discourse from abolition to regulation (Spinello, 2020). This risk underscores the importance of maintaining a critical perspective on legal resistance—one that acknowledges its achievements without overlooking its limitations.

Ultimately, while law remains a vital tool in the struggle for privacy, its capacity to resist surveillance is constrained by political, economic, and institutional factors. Recognizing these limitations is essential for developing more holistic strategies that combine legal advocacy with technological innovation, public education, and transnational solidarity.

8. Conclusion

The evolving architecture of digital surveillance—spanning both state and corporate domains—has significantly reshaped the concept and function of privacy in contemporary society. Far from being a passive or purely personal concern, privacy has become a site of active resistance, embedded within legal strategies that seek to push back against the unchecked expansion of monitoring technologies. This article has explored the multifaceted ways in which legal mechanisms are mobilized to counter surveillance, positioning privacy not simply as a right to be protected, but as a political and legal tool used to challenge power asymmetries and reclaim individual autonomy.

Legal resistance to state surveillance has gained momentum through constitutional litigation, strategic lawsuits, and the invocation of transparency laws. Courts in democratic societies have increasingly recognized the dangers posed by mass data collection, redefining traditional understandings of search, consent, and expectation of privacy in light of technological change. Legal precedents in the United States and the European Union have demonstrated that when civil liberties are threatened, judicial bodies can act as crucial guardians of democratic values. Strategic litigation by advocacy organizations and the use of transparency frameworks have played a key role in uncovering unlawful practices and demanding state accountability. These efforts, while not always successful, have shifted public discourse and elevated privacy concerns to the level of fundamental rights.

Parallel developments in the corporate domain have seen the emergence of data protection laws and consumer rights as mechanisms of resistance. Regulations such as the GDPR and CCPA have granted individuals greater control over their personal data and imposed significant obligations on companies to ensure transparency and accountability. Legal challenges to the business models of major technology firms have not only resulted in landmark court decisions but have also compelled corporations to reassess their data practices. The emphasis on informed consent, data minimization, and user autonomy has begun to shift the power dynamic between individuals and tech giants, even if unevenly and incompletely.

However, the effectiveness of these legal strategies is not uniform across contexts. The comparative analysis reveals a clear disparity between the Global North and the Global South in the robustness and enforcement of privacy protections. While some countries in the Global South have enacted progressive legislation, challenges such as weak institutional capacity, political interference, and digital illiteracy continue to hinder meaningful legal resistance. International human rights frameworks offer a universal normative foundation, but their impact often depends on the political will and judicial independence of national governments. Moreover, in authoritarian settings, the legal system may be used to legitimize rather than resist surveillance, complicating efforts to promote privacy as a universal value.

Legal resistance also faces structural limitations that curtail its transformative potential. Corporate lobbying, jurisdictional conflicts, and rapid technological change

often outpace the ability of legal frameworks to respond effectively. Public disengagement, fueled by the complexity of legal language and digital systems, further weakens the collective momentum needed to enforce privacy rights. Ethical concerns also arise when legal solutions prioritize compliance over justice, potentially normalizing surveillance by creating thresholds of acceptability. These limitations suggest that law, while necessary, is not sufficient on its own to dismantle or fully counter the systems of surveillance capitalism and state control.

Nevertheless, the legal strategies examined in this review provide critical entry points for resistance. They offer avenues for contestation, spaces for advocacy, and platforms for redefining the meaning and boundaries of privacy in the digital age. When coupled with broader social movements, technological innovation, and public education, these legal mechanisms can serve as catalysts for systemic change. The future of privacy as resistance will depend on our ability to build legal infrastructures that are inclusive, adaptable, and grounded in the evolving realities of digital life. In this ongoing struggle, the law remains both a battlefield and a beacon—a domain where the contours of freedom, dignity, and agency are negotiated and defended.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Cheng, X., Qiao, L., Yang, B., & Xiao-ping, Z. (2022). Investigation on Users' Resistance Intention to Facial Recognition Payment: A Perspective of Privacy. *Electronic Commerce Research*, *24*(1), 275-301. https://doi.org/10.1007/s10660-022-09588-y

Dc, S. (2023). Umpiring Technology and Tactical and Strategic Privacy in Cricket. *Unity Journal*, *4*(01), 82-93. https://doi.org/10.3126/unityj.v4i01.52232

Gowthami, M., & V, G. (2024). Autonomous Vehicle Data Protection : A Review of Security Threats, Challenges and Protective Mechanism. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, *10*(5), 524-528. https://doi.org/10.32628/cseit2410429

Lim, E. (2023). Revolutionary Tactics: Abolish Privacy. *Aoir Selected Papers of Internet Research*. https://doi.org/10.5210/spir.v2023i0.13665

McElroy, S., & McKee, L. (2023). Developing Privacy Incident Responses to Combat Information Warfare. *International Conference on Cyber Warfare and Security*, *18*(1), 256-263. https://doi.org/10.34190/iccws.18.1.958

Rizzo, J. (2023). Asking for It: Gendered Dimensions of Surveillance Capitalism. *Emancipations*. https://doi.org/10.55533/2765-8414.1010

Spinello, R. A. (2020). The Ethical Consequences of "Going Dark". *Business Ethics the Environment & Responsibility*, *30*(1), 116-126. https://doi.org/10.1111/beer.12313

Swanlund, D. J. (2021). Disconnection and Reconnection as Resistance to Geosurveillance. 23-40. https://doi.org/10.1093/oso/9780197571873.003.0002

Wagner, B., Sanchez, A., Sekwenz, M.-T., Dideriksen, S., & Murray-Rust, D. (2023). The Politics of Digital (Human) Rights. https://doi.org/10.1093/acrefore/9780190846626.013.694

Watson, A., & Lupton, D. (2020). Tactics, Affects and Agencies in Digital Privacy Narratives: A Story Completion Study. *Online Information Review*, *45*(1), 138-156. https://doi.org/10.1108/oir-05-2020-0174