*Journal of Social Science Studies Vol. 3, No. 2, July 2023, pages 285 – 294*

# From Personal Space to Control Society: The Transformation of Privacy and Surveillance Synergies in the Big Data Era

Bayar Gardi, Abdul Gani

*Gasha Technical Institute Kurdistan Region, Iraq*
*Universiti Malaysia Sabah*

ARTICLE INFO

***Article history:***
*Received 9 February 2023*
*Revised 25 April 2023*
*Accepted 4 June 2023*

**Key words:**
*Data privacy,*
*Surveillance society,*
*Surveillance capitalism,*
*Autonomy,*
*Civil liberties,*
*Corporate-state convergence,*
*Control society.*

ABSTRACT

*This literature review examines the profound transformation of privacy and the rise of a convergent surveillance society in the big data era. Through a qualitative thematic synthesis, the study addresses two core questions: the conceptual and structural shifts in the meaning of privacy, and the synergistic power dynamics between corporate and state surveillance. The analysis reveals that privacy has evolved from a right to seclusion into a struggle for contextual integrity and autonomy against predictive profiling and data commodification within surveillance capitalism. Furthermore, the study demonstrates that corporate-state surveillance operates through a deeply integrated ecosystem, forming a hybrid power regime fueled by the surveillance-industrial complex and mutual data dependencies. This convergence fundamentally reshapes power relations, eroding individual autonomy through pervasive chilling effects and restructuring civil liberties by subordinating digital public spaces to commercial and state logics. The result is the crystallization of a control society where social sorting and behavioral modulation become normalized functions of governance. The study concludes that addressing these challenges requires moving beyond individual-centric privacy frameworks towards structural interventions that limit data extraction, regulate concentrated power, and foster technological alternatives designed to uphold democratic sovereignty and collective freedom. The findings underscore the urgent need for integrated analytical perspectives, bold public policy, and a reimagined digital common.*

## INTRODUCTION

The concept of privacy has become one of the important foundations in the formation of modern society, especially in protecting individual autonomy from state and public intervention. In the liberal tradition of thought, privacy is understood as a personal space that is protected from external observation, which allows for self-development, freedom of thought, and intimate relationships. With the development of information and communication technology, particularly the internet and digital-based services, the traditional boundaries of privacy have begun to shift significantly. Social, economic, and administrative interactions that increasingly take place through technology platforms generate continuous and documented data trails, making data a central element in contemporary social life. This phenomenon reflects the role of big data as a new foundation in shaping the social, economic, and cultural relations of modern society (Wahyudi et al., 2021).

The era of big data accelerates and deepens the fundamental transformation of the meaning of privacy. The volume, speed, and variety of data generated by humans through digital devices, sensors, and online platforms have exceeded the capacity of conventional understanding. Privacy, in the sense of individual control over personal information, is becoming increasingly difficult to maintain because data is often collected passively, combined from various sources, and analyzed with algorithms to reveal patterns, preferences, and even predict behavior. An individual may consciously keep certain information confidential, but from their other digital traces location, time online, browsing patterns sensitive information can be

* *Corresponding author, email address:* ***bayargardi@gmail.com***

inferred. Thus, privacy is no longer just about hiding discrete facts, but about the ability to protect the meaning and inferences that can be drawn from large and heterogeneous data sets. The main threat has shifted from the disclosure of a single piece of embarrassing information to the potential for manipulation, categorization, or judgement based on incomplete or incorrect data profiles. This transformation is in line with the view that the integration of technology and big data also influences psychological dimensions and the way individuals understand themselves in the digital environment (Darmawan et al., 2021).

This development has given rise to what sociology and critical studies refer to as the surveillance society. This concept describes a social condition in which the collection, processing and use of data for surveillance purposes has become so widespread, routine and embedded in the operations of social institutions that it has become a defining characteristic of that society. The surveillance society is not characterized by a single authoritarian central overseer, as in Orwellian depictions, but rather by a network of dispersed surveillance, often carried out by corporate and state actors with different but complementary motives. Surveillance has become a normal administrative function, part of the logic of risk management, efficient marketing, and security assurance. In these conditions, individuals constantly generate data that fuels the surveillance process, often without meaningful opposition because the process is invisible and normalized through rewards of convenience, security, or access to services. However, this normalization does not always occur evenly, given the continuing gaps in access and skills in the use of technology-based services (Ramle & Mardikaningsih, 2022).

Corporate actors, particularly giant technology companies that control digital platforms and online services, have become powerful engines of capitalist surveillance. Their business models often rely on the extraction and analysis of user data to target advertising, refine services, or sell behavioral predictions. This corporate surveillance operates through a logic of voluntarism, whereby users exchange their personal data for free access to platforms. However, the imbalance of information and power between platforms and users makes this consent problematic. Furthermore, the data collected by companies can be used to shape behavior, influence choices, and create filter bubbles that limit users' insights. Such a large concentration of data in the hands of a few private companies raises questions about their social and political power, which can rival that of the state, and its impact on autonomy and diversity in society. The use of smart technology in various sectors shows that personal data is now a source of innovation as well as an increasingly complex instrument of surveillance (Khayru, 2022).

In parallel, the state is also expanding its surveillance capabilities by utilizing big data technology, artificial intelligence, and facial recognition systems. The motives often cited are national security, law enforcement, and public administration efficiency. However, this expansion risks leading to digital authoritarianism, a form of government in which surveillance technology is used to monitor, control, and suppress the population, stifle criticism, and perpetuate power. States can access data from private companies, develop their own mass surveillance systems, or use cyber tools to spy on citizens. The convergence of state and corporate surveillance capacities creates a highly comprehensive surveillance infrastructure, in which individuals' movements, relationships, and thoughts can be mapped and analyzed in real time. This literature review will analyse the changing meaning of privacy, the dynamics of surveillance society involving both actors, and the consequences for civil liberties and social structures. Technology plays an active role in shaping social behavior and psychological responses in society (Darmawan et al., 2021).

The main problem that arises is structural privacy erosion, which is difficult to contain through existing legal or technical frameworks. Traditional privacy laws often focus on the concepts of notification and consent, as well as protection against unlawful data collection. However, in the big data ecosystem, data is continuously collected, aggregated, and processed for purposes that are not specified from the outset, rendering the principle of consent ineffective. Furthermore, the danger often lies not in the collection of a single piece of data, but in the inferences and automated decisions generated from the analysis of aggregated data, which are difficult to attribute to a specific violation. Technical protections such as encryption also have limitations because much data must be processed in readable form to provide services, and metadata analysis can also provide deep insights. Thus, there is a regulatory and protective gap in which contemporary surveillance practices operate, so that individual privacy is continuously eroded without adequate protection.

Another fundamental issue is how this logic of

pervasive surveillance changes the nature of freedom and social behavior. The theory of the chilling effect explains how the awareness of being monitored can encourage individuals to censor themselves, avoid exploring unpopular ideas, or change their online and offline behavior to conform to perceived norms of safety. This effect does not require actual surveillance; the mere perception or uncertainty of surveillance is sufficient to produce conformity. On a societal scale, this can reduce diversity of expression, stifle political innovation, and weaken democratic public spaces. Furthermore, algorithm-driven surveillance systems tend to categories and judge individuals, potentially leading to automated discrimination, denial of opportunity, or data-based prejudice. When important decisions about credit, employment, or security are left to opaque systems, the principles of procedural justice and accountability are threatened, altering the relationship between citizens, companies, and the state. These impacts are particularly relevant for younger generations who are developing their creativity, economic participation, and social identity in digital spaces (Djaelani & Putra, 2021).

The speed of surveillance technology adoption during and after the Covid-19 pandemic has provided a clear illustration of how emergencies can be used to normalize and accelerate the expansion of surveillance. Contact tracing applications, digital health passport systems, and mobility monitoring through mobile phone data were introduced in many countries for public health purposes. However, many of these systems remain in place or their infrastructure can be easily repurposed for other surveillance purposes after the crisis ends. These events highlight how the line between surveillance for public welfare and for social control can quickly become blurred, and how public acceptance of surveillance can change rapidly under the pressure of certain circumstances. A critical examination of these developments is essential to understand the socio-political conditions that enable the normalization of surveillance and to anticipate how the technologies introduced today may shape freedoms in the future.

At the same time, the rise of the data economy and the technological war between global powers have made data sovereignty and cybersecurity major geopolitical issues. Countries are debating and implementing different data regulations, such as the General Data Protection Regulation in the European Union or a more restrictive stance in China. This debate is not only about privacy protection, but also about digital governance models, economic influence and national security. In this situation, individuals are often caught between the interests of global corporations and nation states. Understanding the dynamics of today's surveillance society is important not only for defending civil rights, but also for navigating the ongoing transformation of global governance, in which data has become a strategic resource that various powers are vying to control.

This literature review aims to conduct a critical synthesis analysis of the body of scientific literature on the relationship between privacy, surveillance, and the control society in the era of big data. Specifically, this study seeks to trace and reconstruct the conceptual transformation of privacy from the protection of personal space to a commodity in the data economy, as well as to analyses the mechanisms and impacts of the convergence of surveillance by corporate and state actors. The expected theoretical contribution is the presentation of an analytical framework that integrates perspectives from the sociology of technology, critical surveillance studies, and power theory to understand the formation of contemporary control societies. Practically, this synthesis is expected to provide a strong foundation for understanding data protection policy advocacy, privacy-cent red technology design, and critical digital literacy education for the public in an effort to stem the erosion of civil liberties.

## RESEARCH METHOD

This research was designed as a systematic qualitative literature study. This approach was chosen because of its suitability for exploratory and interpretative research objectives, namely to understand the complexity and nuances of the conceptual transformation of privacy and the dynamics of surveillance society. This study focuses on an in-depth analysis of relevant academic texts, such as journal articles, books, and book chapters, to identify themes, patterns of argument, and relationships between concepts that have developed in the scientific discourse on this topic. The main method applied is thematic synthesis, which allows researchers to organize and integrate findings from various literature sources into a coherent and meaningful framework of understanding, without aggregating quantitative data. Thus, this study serves to map the intellectual landscape of this field of study, highlighting points of consensus, debate, and knowledge gaps that need to be filled.

The literature search strategy was conducted in a phased and comprehensive manner. The main academic databases used included Scopus, Web of Science, JSTOR, and specialized repositories such as the ACM Digital Library for more technical literature. The search was conducted using a combination of keywords in English that reflect the core topics of the research, such as "privacy big data", "surveillance society", "surveillance capitalism", "digital authoritarianism", "dataveillance", "social control", "chilling effect", and other key terms. The publication year range focused on the period in which the discourse on big data and surveillance society experienced rapid development, to ensure the relevance and currency of the discussion. The inclusion criteria applied are: (1) publications that substantively discuss the social, political, or sociological aspects of privacy and surveillance in the digital age; (2) works that contain theoretical or empirical analyses of the role of corporations or the state in surveillance practices; (3) literature written in English or Indonesian. Works that purely discuss positive legal aspects without social analysis, or publications that are popular and non-academic in nature, were not included in the study.

Data analysis followed procedural stages that have been standardized in qualitative research methodology. After the literature was collected and selected, each text was read deeply and repeatedly. In this process, open coding was carried out to mark key concepts, propositions, and arguments that emerged. These initial codes were then grouped based on thematic similarities through axial coding, which linked the categories formed with their subcategories. The next stage was theme selection, in which potential themes were tested for accuracy against the overall data and refined to form a solid thematic map that could answer the research question. To maintain the credibility of the analysis, triangulation is carried out by comparing interpretations from various sources and disciplinary perspectives. In addition, the analysis process is carefully documented through analytical memo notes, which track the development of ideas and justifications for each interpretation constructed, thus ensuring the transparency and auditability of the entire research process.

## RESULTS AND DISCUSSION

### Privacy Transformation: From Personal Space to Data Commodity in a Surveillance Society

The transformation of the meaning of privacy in the era of big data can be traced from a paradigm shift from privacy as "the right to be left alone" to a more fluid and fragmented understanding of control over the flow of personal information. In his seminal work, Daniel Solove (2006) criticizes the traditional approach that views privacy as merely withdrawal from society. He proposes a taxonomic framework that understands privacy through the lens of harm, which includes activities such as information collection, processing, dissemination, and invasion. This approach is relevant because in a surveillance society, threats often come not from a single act of spying, but from the aggregation of seemingly harmless data from various sources, which is then processed to make harmful inferences or decisions. Privacy, therefore, must be understood as protection against various types of harm arising from complex information ecosystems, where individuals lose the ability to understand how their data is used and what the consequences are. This condition is increasingly felt in everyday digital interactions, where social relations and interpersonal trust are formed and mediated by data-based platforms (Oluwatoyin, 2021).

Helen Nissenbaum (2010) made an important contribution with her theory of "privacy as contextual integrity". She argues that privacy is not about hiding information, but about compliance with norms of information flow that are appropriate in a particular social context. Each context, such as healthcare, banking, or social media, has norms that govern who can provide what information, to whom, and under what conditions. Privacy violations occur when the norms of information flow in a context are violated. This theory is particularly helpful for analyzing the erosion of privacy in the era of big data, as the practice of cross-context data collection and exchange by technology companies systematically violates the principle of contextual integrity. Data provided in a social context (such as friendships on Facebook) is taken and analyzed for a completely different advertising context, a normative violation that is difficult to capture by traditional privacy laws that focus on individual consent. Violations of this information flow norm have been shown to have an impact on declining levels of trust between individuals, particularly among younger generations who are intensive users of social media (Negara et al., 2022).

Shoshana Zuboff (2019), in her analysis of "surveillance capitalism," articulates the most radical structural transformation. She defines surveillance capitalism as a new economic logic that claims human experience as free raw material to be

translated into behavioral data. This data is then processed into predictive products that are traded in a new market for future behavior. In this logic, privacy is no longer merely eroded; it is actively eliminated as an obstacle to capital accumulation. Privacy transforms from a right or social norm into an interference with the efficiency of data extraction. Resistance to data collection is seen as irrational behavior that hinders progress and personalization. This transformation is structural because it is embedded in the dominant business model of the digital economy, changing the fundamental relationship between individuals and companies from a consumer-service provider relationship to a subject-object relationship of data extraction. This economic logic is also reinforced by the dependence of social and economic activities on digital platforms that make user data a primary source of value (Infante & Mardikaningsih, 2022).

Conceptually, this transformation marks a shift from spatial privacy to informational privacy, and ultimately to privacy as autonomy. Spatial privacy relates to the integrity of one's physical territory, such as one's home or body. Informational privacy focuses on control over personal data. However, under conditions of surveillance capitalism and state surveillance, the greatest threat is to autonomy, namely the ability to make decisions and shape one's life without unfair manipulation, prejudice, or coercion based on data profiles. When algorithms predict and influence choices from the news one reads to the partner one dates, the core of individual autonomy is threatened. Therefore, the most important meaning of privacy today is the protection of conditions that allow personal and collective autonomy to flourish, which goes beyond simply maintaining the confidentiality of information.

At the practical level, this transformation is manifested in the normalization of data exchange as a condition for social and economic participation. To access social networks, search engines, or map services, individuals must accept lengthy terms and conditions that grant broad permission for data collection. This practice transforms privacy from an inherent condition into a negotiable commodity, where the exchange value is convenience, connectivity, or access. However, the imbalance of power in these negotiations is so great that it results in a well-known "privacy paradox": although individuals express high concerns about privacy in general, they often readily disclose personal data in practice. This paradox can be understood not as irrationality, but as a rational response to a lack of real choice, technical complexity, and interface designs that encourage disclosure.

The technical infrastructure of the surveillance society, consisting of sensors, platforms, algorithms, and data centers, creates a condition in which data collection is pre-emptive and ambient. Data is no longer collected only when someone performs an explicit transaction; it is passively collected from always-connected devices, smart city environments, and online interactions. This condition blurs the line between public and private space. A person's digital footprint in physical public spaces, such as that captured by city surveillance cameras, can be analyzed to infer political beliefs, sexual orientation, or mental health status. Thus, traditional privacy practices such as maintaining secrecy at home become ineffective, as too much can be inferred from behavior in spaces traditionally considered public. Privacy must be maintained through technical tools such as encryption and through political demands to limit data collection itself. Urban studies also emphasize that environmental data infrastructure enables continuous conclusions that transform public spaces into locations for constant monitoring and behavioral prediction (Kitchin, 2014; Andrejevic & Burdon, 2015). From a public governance perspective, this condition underscores the importance of leadership and regulatory frameworks that orient digital governance toward public service values, accountability, and the protection of citizens' rights within technologically mediated public spaces (Rojak, 2021).

The role of time in the construction of privacy has also changed dramatically. Privacy is often understood within a limited temporal framework, relating to current or past information. In a predictive surveillance society, the highest value lies in data that can be used to predict future behavior and preferences. Thus, privacy is not only about protecting past secrets, but also about protecting a person's future possibilities from unfair determination and restriction. When a system predicts that a job applicant is likely to leave their job based on their social media patterns, it limits their future now. Adequate privacy practices for this era must include the right to uncertainty and the right not to be judged based on statistical probabilities generated from population data.

The language and legal framework governing privacy are also struggling to keep pace with these conceptual changes. Instruments such as the European Union's General Data Protection Regulation attempt to respond by introducing

principles such as privacy by design and provisions for data processing limited to specific purposes. However, the law often lags behind technological practices. Legal concepts such as "personal data" or "valid consent" are constantly being challenged by new techniques such as data inference and machine learning, where personal data is created from non-personal information. This structural transformation demands an evolution in legal thinking from data-cent red privacy towards power-centred privacy, which focuses on regulating asymmetrical relationships and preventing the abuse of power that arises from control over data, regardless of whether that data is technically considered "personal".

Ultimately, this transformation in the meaning and practice of privacy leads to the individualization of responsibility for privacy protection. Public narratives often place the burden on individuals to "protect themselves" by using complex privacy settings, encryption tools, and smart consumer decisions. While these tools are important, the focus on individuals diverts attention from the structural nature of the problem. When entire economic models or state security logics depend on mass data extraction, individual actions have very limited impact. The conceptual transformation required is to view privacy not as an individual property to be defended, but as a collective social condition to be regulated and protected through democratic governance, alternative technological design, and structural constraints on corporate and state power.

Overall, the transformation of the meaning and practice of privacy in a big data-driven surveillance society is profound and multidimensional. Conceptually, there has been a shift from privacy as withdrawal to privacy as protection from intrusion in the information ecosystem, compliance with contextual information flow norms, and ultimately as a prerequisite for autonomy. Structurally, privacy has changed from a legally protected social norm to a commodity traded in the data economy and to an intrusion that must be overcome in the logic of surveillance capitalism and state security. Individual privacy practices are becoming increasingly inadequate in the face of ambient and predictive surveillance infrastructures that blur the boundaries of space and time. This transformation demands an equally transformative response, moving beyond individualistic legal frameworks towards collective and structural approaches that limit the power generated by control over data and create technological and social conditions in which human autonomy can flourish.

## Convergence of Corporate-State Oversight and the Formation of a Control Society

The synergy between corporate and state surveillance no longer operates as two separate domains, but has merged into an integrated and mutually reinforcing surveillance ecosystem. This convergence reshapes power relations by creating a hybrid surveillance regime, where the market logic of technology companies meets the logic of state sovereignty and security. At the most basic level, the state depends on companies for access to their data and analytical capabilities. Companies hold deep information about populations that often exceeds what state intelligence agencies possess. Through formal mechanisms such as court orders, data access requests, or contractual partnerships, and informally through political pressure or economic incentives, this corporate data flows to the state apparatus. Conversely, companies need the state to create a stable regulatory environment, protect intellectual property rights, and sometimes open up foreign markets. This symbiotic relationship results in a data power alliance, where the boundaries between the public and private sectors become blurred, and citizens or consumers face a much more cohesive and formidable bloc of power than they would face separately. Governance oversight also observes that contemporary power is increasingly exercised through collections of public-private data that normalize surveillance as an administrative and economic function, rather than as an exceptional security practice (Ball & Snider, 2013; Lyon, 2014).

A theoretical foundation for understanding this convergence can be found in the concept of the "surveillance-industrial complex," as outlined by scholars such as Kirstie Ball. This concept, an adaptation of the military-industrial complex, describes a complex network between surveillance technology companies, government agencies, and research institutions that share a common interest in the expansion and normalization of surveillance technology. Companies do not simply sell finished products to the state; they actively shape demand by promoting narratives of uncertainty and risk that require surveillance solutions, and engage in lobbying for policies that support their interests. This surveillance-industrial complex drives rapid innovation in surveillance technology, creating supply that then generates its own demand. This dynamic also intersects with changing social values and practices in the digital age, where technology is

gradually reshaping how societies understand security, efficiency, and social normality (Al Hakim et al., 2021). In this dynamic, the state is often the primary client, but corporate commercial logic that drives efficiency, scalability, and profitability ultimately shapes how state surveillance is carried out, transforming it from a targeted, suspicion-based practice to a mass, data-driven operation that collects information on everyone.

David Lyon, in his work on "surveillance as social sorting," highlights how the synergy of corporate-state surveillance operates to classify, assess, and allocate populations. Companies classify us as consumers with certain predictive values, while the state classifies us as citizens with certain levels of risk or eligibility. These classification systems increasingly overlap and reinforce each other. The literature on social stereotypes shows that such classification processes are never neutral, but rather have the potential to reproduce pre-existing biases and social inequalities (Sajjapong et al., 2022). Social credit scores developed by companies to assess creditworthiness can, with or without consent, be taken into account in risk assessments by government agencies. Spending or travel patterns detected by credit card companies or telephone providers can be used for security risk profiling. These social ranking algorithms have real material consequences, determining access to loans, insurance, employment, and even freedom of movement. When the state adopts corporate classification systems, it essentially outsources its administrative and normative functions to opaque and undemocratic market logic, thereby depoliticizing decision-making processes that affect citizens' lives.

The most direct impact on individual autonomy lies in the erosion of space for identity experimentation and self-formation free from surveillance. Classical autonomy requires the ability to explore, make mistakes, and change one's mind without permanent consequences or constant surveillance. In digital society, identity formation increasingly takes place through online interactions that open up new spaces for expression while placing individuals in a system of continuous observation and assessment (da Costa et al., 2022). This process also intersects with existing cultural traditions and social norms that historically shape identity formation, which may be reinterpreted or constrained when identity expression is mediated and recorded through digital systems (Binti Ismail, 2021). Converged surveillance societies create environments in which every digital action, and increasingly physical actions, leave data traces that can be stored indefinitely, analyzed, and used to make assumptions about a person's character and potential. Awareness of the ever-watchful eye, whether from platform algorithms that assess engagement or from the state monitoring activism, results in what is termed "self-censorship" or the "chilling effect". Individuals may avoid seeking information on sensitive topics, be reluctant to join certain online groups, or alter how they express themselves, even before any direct intervention occurs. Autonomy is thus eroded preventively, through self-adjustments in behavior in response to a perceived surveillance environment.

Collective civil liberties, such as the right to assemble and express opinions, are also reconfigured under this surveillance regime. Physical protests can now be mapped and analyzed through the integration of data from participants' mobile phones, facial recognition from city cameras, and social media activity. This information can be used not only for post-facto criminal investigations, but for the prediction and prevention of protests, limiting the right to assemble before it occurs. Social media platforms, which have become new public spaces for political debate, operate under state pressure to moderate content, often with overly broad algorithms that suppress legitimate discourse. The ability to coordinate collective action or criticize the government online can be limited by a combination of state pressure on companies and the platforms' own algorithmic design, which promotes non-controversial content to maximize user engagement. Civil liberties become conditioned by the technical requirements and commercial logic of the digital infrastructure that mediates them.

These reconfigured power relations also manifest in unequal capacities to resist or navigate surveillance. Economic and political elites often have the resources to purchase privacy through secure services, cybersecurity consultants, and legal influence. In contrast, marginalized communities, migrants, and vulnerable groups are often the targets of the most intense surveillance, both from the state through social assistance programmed that require biometric verification, and from corporations through predictive marketing that exploits vulnerabilities. The convergence of surveillance thus not only monitors existing inequalities, but actively produces and reinforces them by creating different layers of

surveillance for different classes. Surveillance becomes a tool of differential social discipline, consolidating power in one hand while increasing vulnerability in the other.

The technical infrastructure underpinning this convergence, such as cloud data centers, digital identity platforms, and integrated analytics systems, creates new points of concentration of power. When governments migrate to cloud services provided by large technology companies, they are not only purchasing data storage, but also surrendering sovereignty over vital digital infrastructure to private entities subject to complex legal and economic pressures. This creates a structural dependence of the state on corporations. On the other hand, companies depend on the state to provide legal legitimacy and coercion, when necessary, for example to enforce terms of service or protect their data monopolies. Within this concentrated data regime, individuals increasingly experience the shaping of self-identity and social perception through algorithmically mediated interactions, as digital platforms influence how individuals present themselves and are evaluated by others (Darmawan & de Jesus Isaac, 2022). International surveillance studies have similarly highlighted how platform-based data infrastructures operate as mechanisms of social sorting and power concentration that reshape subjectivity and democratic governance (Lyon, 2018; Zuboff, 2019). This mutual dependence results in a data oligarchy, a form of governance in which collective decisions about how society is monitored and controlled are made through closed interactions between a few corporate and state actors, bypassing public democratic processes.

The implications of this synergy for the rule of law and accountability are profound. Traditional legal principles such as due process, presumption of innocence, and the right to face one's accuser become difficult to apply when decisions are made based on data profiles generated by proprietary corporate algorithms. How can one contest a decision based on statistical correlations from large datasets whose sources and methodologies are kept secret on grounds of trade secrets or national security? Increasing power is shifting from transparent judicial institutions to opaque technical and bureaucratic systems. This convergence thus results in a significant democratic accountability deficit, where the actual decision-making centers become increasingly invisible and inaccessible to legal or public challenge.

The Covid-19 pandemic has served as a catalyst that accelerates and exposes this convergence. Contact tracing applications, often developed through public-private partnerships, digital vaccine passport programmed, and quarantine monitoring via telephone data demonstrate how emergencies can rapidly normalize the integration of sensitive health data between technology companies and governments. At the same time, the widespread implementation of remote working arrangements during the pandemic further expanded the collection and mediation of personal and professional data through digital platforms, reinforcing dependence on technological infrastructures managed by both corporate and state actors (Mendrika et al., 2021). Much of this infrastructure and power relationship remains in place after the crisis, setting a precedent for similar interventions in the future for public health, security, or welfare. These events show how corporate-state surveillance synergies can develop rapidly under the right conditions, building permanent surveillance capacities that far exceed their original purpose.

Finally, these synergies reshape the political imagination of what is possible and desirable. Narratives driven by the surveillance-industrial complex often promote visions of "smart cities", "government efficiency", and "personalized services" as an inevitable technological destiny requiring total data collection. These narratives shift public discourse away from normative questions such as "Should we be monitored?" to technical questions such as "How can we monitor more efficiently?". By framing surveillance as a technical necessity for progress and security, this convergence reduces the space for meaningful political resistance. Collective autonomy to determine the future of society's technology is thus compromised, as the path seems to have been determined by the collaboration between market forces and the state.

Overall, the synergy between corporate and state surveillance has produced a distinctive regime of power for the twenty-first century. Power relations have been reconfigured through the formation of data alliances, industry-surveillance complexes, and infrastructural interdependencies that combine market logic with state sovereignty. This convergence negatively impacts individual autonomy by creating a surveillance environment that inhibits self-exploration and triggers preventive self-adjustment. Collective civil liberties are redefined and limited by the technical infrastructure and economic pressures that regulate

the digital public sphere. Inequality is deepened through the differential application of surveillance, and democratic accountability becomes blurred. The society emerging from this convergence is a society of control, where behavioral regulation and social ordering are achieved through the subtle integration of corporate surveillance and state coercion, challenging the foundations of a democratic project that relies on autonomous citizens and a free public sphere.

## CONCLUSION

This literature review has revealed a profound transformation in the meaning of privacy and surveillance mechanisms in contemporary societies driven by big data. The analysis shows that privacy has undergone a conceptual shift from the protection of personal space to a struggle to maintain individual autonomy in the face of a complex information ecosystem. Privacy must now be understood as the contextual integrity of data flows and as a fundamental prerequisite for freedom from manipulation and determination based on predictive profiling. Furthermore, this study asserts that the dynamics of surveillance today are characterized by a synergistic and structural convergence between corporate and state actors. This synergy is not accidental but embedded in the logic of surveillance capitalism and the surveillance-industrial complex, which produces a hybrid regime of power. This regime reshapes power relations by creating interdependence and data alliances, which in turn significantly erode individual autonomy through chilling effects and limit collective civil liberties by altering the infrastructure of digital public space. The end result is the formation of a control society in which social ordering and behavior modulation become normal functions of governance, threatening the democratic foundations that depend on free and equal citizens.

The findings of this study have serious implications for social theory, public policy, and technology design. Theoretically, this study calls for a more integrated analytical approach capable of linking political economy theory with the study of technology, law, and power to understand contemporary surveillance regimes. The framework that separates state surveillance from corporate surveillance is becoming increasingly inadequate. For public policy, the main implication is the need for a much more ambitious and bold regulatory approach. Privacy regulations that focus on individual consent and transparency, such as the GDPR, need to be complemented by structural interventions that limit the ability to collect data in the first place (data minimization mandates), prohibit certain practices such as political microtargeting, and break the dangerous symbiotic relationship between data companies and state agencies. Regulation must shift from a consumer protection model towards one that defends democratic sovereignty and the social conditions for freedom. For technology design, these findings emphasize the importance of promoting and subsidizing alternatives such as federated learning technologies, ad-free subscription-based services, and platforms built on privacy-by-design and digital commons principles, which can reduce dependence on extractive business models.

Based on the analysis conducted, several suggestions are proposed for further research and action. First, in-depth and comparative empirical research is needed on the specific operations of the surveillance-industrial complex across jurisdictions. Such research should map the flows of capital, lobbying, contracts, and personal exchanges between surveillance technology companies and various branches of government, to uncover the concrete mechanisms of power convergence. Second, it is essential to develop and promote critical literacy education on surveillance for the public. This education must go beyond individual digital security tips to include an understanding of extractive business models, collective digital rights, and political advocacy tactics to demand accountability from corporate and state actors. Third, academics, activists, and policymakers must actively engage in imagining and building institutional alternatives. This includes supporting cooperative data ownership models, campaigning for a global moratorium on the use of facial recognition and social scoring systems by governments, and creating a truly independent technology oversight body with the authority to audit algorithms and break up data power concentrations. The future of democracy may depend on the success of such efforts.

## REFERENCES

Al Hakim, Y. R., Rojak, J. A., & Triono, B. (2021). Transformation of Cultural Values and Social Practices in the Digital Age. *Journal of Social Science Studies*, 1(1), 173-178.

Andrejevic, M., & Burdon, M. (2015). Defining the Sensor Society. *Television & New Media*, 16(1), 19–36.

Ball, K. (2010). Workplace Surveillance: An Overview. *Labor History*, 51(1), 87-106.

Ball, K., & Snider, L. (2013). *The Surveillance-Industrial Complex: A Political Economy of Surveillance.* Routledge / Information, Communication & Society.

Binti Ismail, A. (2021). Tradition and Social Identity Formation in Society. *Journal of Social Science Studies*, 1(2), 221-226.

da costa, S., Darmawan, D., & Isaac, A. de J. (2022). Self-Identity Formation and Social Perception of Individuals through Interaction on Social Media in a Digital World. *Journal of Social Science Studies*, 2(2), 273-278.

Darmawan, D., Utama, A. G. S., Marasabessy, S. A., Larasati, D. A., Roosinda, F. W., & Aziz, I. (2021). *Psychological Perspective in Society 5.0.* Zahir Publishing.

Darmawan, D., & de Jesus Isaac, A. (2022). Self-Identity Formation and Social Perception of Individuals through Interaction on Social Media in a Digital World. *Journal of Social Science Studies,* 2(2), 273-278.

Djaelani, M., & Putra, A. R. (2021). Youth Empowerment to Grow Creative Business Interest. *Journal of Social Science Studies (JOS3),* 1(2), 52-54.

Gilliom, J., & Monahan, T. (2012). *Supervision: An Introduction to the Surveillance Society*. University of Chicago Press.

Infante, A., & Mardikaningsih, R. (2022). The Potential of Social Media as a Means of Online Business Promotion. *Journal of Social Science Studies*, 2(2), 45-49.

Khayru, R. K. (2022). Transforming Healthcare: The Power of Artificial Intelligence. *Bulletin of Science, Technology and Society*, 1(3), 15-19.

Kitchin, R. (2014). The Real-Time City? Big Data and Smart Urbanism. *GeoJournal*, 79(1), 1–14.

Lyon, D. (2003). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Routledge.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society,* 1(2), 1–13.

Lyon, D. (2018). The Culture of Surveillance: Watching as a Way of Life. *Information, Communication & Society,* 21(6), 825–842.

Mendrika, V., Darmawan, D., Anjanarko, T. S., Shaleh, M., & Handayani, B. (2021). The Effectiveness of the Work from Home (WFH) Program During the Covid-19 Pandemic. *Journal of Social Science Studies,* 1(2), 44-46.

Negara, D. S., Darmawan, D., & Saktiawan, P. (2022). Privacy Violations on Social Media and Interpersonal Trust Among Young Generations. *Journal of Social Science Studies*, 2(2), 151-156.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Oluwatoyin, F. (2021). The Dynamics of Social Interaction in the Digital Age: Technological Implications for Interpersonal Relationships and Psychosocial Well-Being. *Journal of Social Science Studies*, 1(2), 137-142.

Pakpahan, N. H., Darmawan, D., & Rojak, J. A. (2022). Racial Discrimination and How Psychological Wellbeing and Social Engagement Impacts: A Review of the Literature on Identity, Stigma, and Coping Strategies in Multicultural Societies. *Journal of Social Science Studies,* 2(1), 87-94.

Ramle, N. L. B., & Mardikaningsih, R. (2022). Inclusivity in Technology-Based Services: Access and Skills Challenges. *Journal of Social Science Studies*, 2(2), 225-230.

Rojak, J. A. (2021). The Effectively Leading Manifestation of Public Service-OrientedGovernance. *Journal of Social Science Studies*, 1(2), 89-96.

Sajjapong, T., Darmawan, D., & Marsal, A. P. (2022). The Role of Social Stereotypes in Shaping Opportunities and Inequalities in Society: Their Impact on Education, Employment, and Intergroup Interactions. *Bulletin of Science, Technology and Society,* 1(1), 44-49.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477–564.

Wahyudi, W., R. N. K. Kabalmay, & M. W. Amri. (2021). Big Data and New Things in Social Life. *Studi Ilmu Sosial Indonesia,* 1(1), 1–12.

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

*Gardi, B., & A. Gani. (2023). From Personal Space to Control Society: The Transformation of Privacy and Surveillance Synergies in the Big Data Era, *Journal of Social Science Studies* 3(2), 285 – 294.