

SURVEILLANCE CAPITALISM AND ITS IMPACT ON SOCIAL RELATIONSHIPS: A SOCIOLOGICAL PERSPECTIVE

Deepa S V

Associate Professor of Sociology, GFGC, Yelahanka, Bengaluru

ABSTRACT

This article explores the phenomenon of surveillance capitalism through a critical sociological lens, focusing specifically on its profound and often subtle impacts on human social relationships and digital rights. Coined by Shoshana Zuboff, surveillance capitalism is conceptualized as a new economic order where the extraction of human experience as raw material for behavioural data (or "surplus value") is monetized through prediction products sold on behavioural futures markets. Drawing on critical theory, particularly the Frankfurt School's analysis of the culture industry and Foucault's concept of the Panopticon, this study analyses how the ubiquitous nature of digital monitoring restructures social interactions, fostering a climate of calculated visibility and perpetual performance. The investigation reveals a dual effect: while digital platforms facilitate expansive social networks, the underlying mechanisms of surveillance erode authentic connection by incentivizing conformity, diminishing privacy boundaries, and weaponizing personal information in social contexts. The article argues that the commodification of the self leads to a "datafied alienation," replacing autonomous sociality with algorithmically-mediated interaction. Furthermore, it examines the consequent erosion of digital rights, positing that the current paradigm necessitates urgent policy interventions and a robust reassertion of human autonomy against the logic of extraction. The final section proposes concrete sociological and legal suggestions to mitigate the deleterious effects of surveillance capitalism on the social fabric.

Keywords: Surveillance Capitalism, Social Relationships, Digital Rights, Datafied Alienation, Sociological Frameworks, Privacy Erosion.

INTRODUCTION

The dawn of the twenty-first century promised a digital renaissance—a world connected, informed, and democratized by networked computing. This promise, however, has been profoundly reconfigured by a dominant economic logic that leverages connectivity not merely for communication, but for **extraction and control**. This new order is what Shoshana Zuboff (2019) terms **surveillance capitalism**: an economic mechanism where human experience is unilaterally claimed as free raw material, converted into data, analysed for behavioural prediction, and sold in opaque markets. Unlike previous iterations of capitalism that focused on the production of goods or the management of services, this model pivots on the **prediction and modification of human behaviour** to secure economic certainty.

While the economic framework of surveillance capitalism is now a recognized subject of critical inquiry, its **sociological consequences** for the fundamental structures of human social life—how we establish trust, maintain intimacy, express autonomy, and form community—remain insufficiently scrutinized. The digital apparatus is not simply a neutral tool; it is an environment governed by an extractive logic that fundamentally restructures the conditions of sociality.

This article posits that surveillance capitalism constitutes a radical challenge to human autonomy and social integrity. By embedding monitoring and predictive modeling into the very channels of social communication, it subtly yet powerfully transforms interpersonal dynamics, institutional trust, and the

civic sphere. Understanding this transformation requires moving beyond technical assessments to a deep sociological engagement with power, alienation, and the redefinition of the self in the age of the algorithm.

OBJECTIVES OF THE STUDY

The primary objectives guiding this comprehensive sociological analysis are:

1. To review and synthesize the core sociological literature related to surveillance, datafication, power dynamics, and the political economy of the internet, establishing a robust theoretical foundation for the analysis.
2. To clearly articulate and apply foundational sociological frameworks—specifically Neo-Marxism (Alienation), Foucault (Panopticon), and Giddens (Trust)—to explain the core mechanics and social control inherent in surveillance capitalism.
3. To conduct a detailed analysis of the positive and, more critically, the profound negative impacts of surveillance capitalism on fundamental aspects of human social relationships, including trust, intimacy, spontaneity, and community formation.
4. To critically assess the implications of the current paradigm for the realization, defense, and practical application of **digital rights** as essential components of human autonomy and civic life.
5. To propose actionable, multi-level suggestions encompassing legal, policy, educational, and technological reforms designed to mitigate the deleterious effects of surveillance capitalism and reassert human sovereignty over data and social interaction.

REVIEW OF LITERATURE

The body of literature relevant to surveillance capitalism is multidisciplinary, drawing heavily from sociology, communication studies, critical theory, and political economy. This review synthesizes key works into three domains: the economic definition of surveillance, the theoretical sociological critique, and the observed impact on sociality.

a. The Conceptual and Economic Foundation of Surveillance Capitalism

The foundational text for this inquiry is **Zuboff's (2019) *The Age of Surveillance Capitalism***. Zuboff distinguishes this new economic logic from general data use. She argues that surveillance capitalism operates by unilaterally claiming private human experience as **behavioural raw material**, translating it into **behavioural data**, and refining this into **prediction products** (what people will do now, soon, and later). These products are traded in a novel invention she names the **behavioural futures market**. Crucially, the aim is not just to predict behaviour but to subtly, and often invisibly, **modify it** toward commercial ends. This mechanism creates a vast, uncompensated economic flow derived from the human life world.

Building on this, **Couldry and Mejias (2019) in *The Costs of Connection*** introduce the concept of **data colonialism**, arguing that the appropriation of human life for data extraction mirrors historical colonial processes. They contend that the data relation is fundamentally asymmetrical, institutionalizing a new form of power where life is systemically rendered into an asset for capital. This shifts the focus from simple privacy infringement to the wholesale colonization of social structures.

Van Dijck (2014) provides insight into the ideological underpinnings with her discussion of **"datafication" and "Dataism."** Datafication is the transformation of social action into quantified, real-time data, while Dataism is the accompanying ideology that trusts data (and algorithms)

inherently over human judgment or subjective experience. This ideological framework naturalizes the extraction process, making surveillance appear as a beneficial or necessary condition of modern life.

b. Sociological Frameworks of Power, Control, and Alienation

To understand the social restructuring enabled by surveillance capitalism, classical and contemporary critical theory provides indispensable analytical tools.

Foucault's (1975) concept of the Panopticon (He popularized the Concept given by **Jeremy Bentham**) is universally adopted to describe the environment of perpetual visibility. The Panopticon, a structural design for prisons, ensured inmates never knew when they were being watched, inducing an internalized state of self-discipline. **Deleuze (1990)** updated this with the idea of "**societies of control**," shifting the spatial metaphor from the enclosed institutions (prison, factory) to the dispersed, continuous modulation of control via dynamic digital interfaces. Surveillance capitalism perfects this; the monitoring is not static but adaptive, modulating behaviour through personalized nudges and suggestions, thereby creating a pervasive culture of **calculated visibility** and self-optimization.

The Marxist tradition, particularly the theory of **alienation**, is reinterpreted for the data economy. **Marx's (1867/1976)** core concept of **surplus value**, the difference between the value a worker produces and the wages they receive, translated into Zuboff's **behavioural surplus value**. **Fuchs (2014)** explicitly connects data labour to uncompensated digital labour, arguing that the social interactions and content creation performed by users are forms of digital labour that produce value extracted by platform owners. This results in **datafied alienation**, where individuals are separated from the data their actions produce, from the process of monetization, and ultimately, from their authentic, non-instrumental social selves.

Giddens (1990) and his work on risk and trust in modernity is crucial for assessing institutional impact. In high modernity, individuals rely on **abstract systems of trust** (e.g., in the financial system, legal structures). Surveillance capitalism disrupts this by creating highly powerful, yet non-transparent, abstract systems (algorithms) that manage crucial social and economic access (e.g., information, employment, credit). The sheer opaqueness of these systems erodes fundamental societal trust and injects massive, complex, and unmanageable risks into everyday life, such as the risk of algorithmic bias or identity theft.

c. Observed Impacts on Social Relations and Identity

The literature focusing on the direct social impact highlights the paradox of increased connection and deep social fracturing. **Turkle (2011) in *Alone Together*** critiques how the expectation of instant, constant digital connection leads to a reliance on technology at the expense of deep, unmediated, face-to-face interaction. She argues that digital relationships are often performed to manage anxiety, allowing individuals to maintain control over the "edit" button of their social lives, thus diminishing the capacity for messy, spontaneous, and authentic intimacy.

Baym (2010) and Zhao (2005) examined how identity is managed and performed online, showing that while digital spaces offer opportunities for identity exploration, the presence of surveillance and the pressure of platform-based metrics (likes, shares) can narrow the performance of self toward an optimized, conformist, and palatable data profile. This pressure to perform an ideal self for the gaze of both peers and the algorithm is a key factor in social stress.

Finally, **Harcourt (2015) in *Exposed*** details the social impulse to willingly disclose information, even in the face of known surveillance. He explores the psychological trade-off where the desire for social connection, validation, and belonging (utility) often overrides concerns about privacy (autonomy), illustrating how the social architecture of the platforms weaponized inherent human desires against

self-preservation.

SOCIOLOGICAL FRAMEWORKS OF SURVEILLANCE CAPITALISM

Surveillance capitalism is fundamentally a sociological phenomenon because it targets, transforms, and exploits the human life world—the sphere of social relationships, meaning, and subjective experience. These frameworks provide the necessary lens for critique.

a. The Neoliberal Panopticon and the Calculated Self (Foucault and Deleuze)

Foucault's (1995) concept of the Panopticon described a disciplinary society that enforced norms through the architectural arrangement of power. Surveillance capitalism represents the **ubiquitous digital Panopticon**, where the monitoring mechanism is no longer a physical tower but the very infrastructure of social life. Every interaction—a scroll, a pause, a 'like', a message—is recorded, quantified, and rendered into data.

This digital surveillance transcends the mere observation of behaviour; it aims at its **pre-emption and modification**. Deleuze's (1992) "societies of control" are evident here: control is continuous, enacted through feedback loops (algorithms) that are highly personalized. The result is a profound sociological effect: the internalization of surveillance leads to the **calculated self**. Individuals are subtly coerced into performing the version of their social identity that is most legible and profitable to the platform. This self-discipline is reinforced by social metrics (likes, followers) which are themselves derivatives of the platform's commercial logic. Authenticity is replaced by optimization, and spontaneous sociality is sacrificed for the sake of measurable engagement.

b. Datafied Alienation and the Digital Appropriation of Surplus Value (Neo-Marxism)

Classical Marxist analysis is centered on the alienation of the worker from the product of their labour, the process of production, their species-being, and other human beings. Surveillance capitalism updates this analysis for the **immaterial economy**.

The extraction of **behavioural surplus value** is the heart of this Neo-Marxist critique. Unlike the wage labourer who sells their labour power for compensation, the digital user offers their entire lived experience (data) without formal compensation or recognition of the exchange. This data is the raw material, and the user's social activity constitutes the uncompensated labour.

This mechanism leads to profound **datafied alienation**:

- **Alienation from the Product:** The user's data—the product of their social activity—is immediately seized, owned, and controlled by the surveillance capitalist. The user never sees the prediction products derived from their life.
- **Alienation from the Process:** The mechanisms of data refinement and algorithmic deployment are opaque, hidden from the user, preventing any understanding or influence over how their sociality is monetized.
- **Alienation from the Self (Authenticity):** By continually performing for algorithmic approval and social validation metrics, the self becomes instrumentalized. The individual loses touch with their non-instrumental, non-data-generating self, leading to the erosion of genuine autonomy.
- **Alienation from Others (Sociality):** Relationships are filtered through engagement-maximizing algorithms that prioritize contentious or polarizing content. This mediation prevents spontaneous, open, and authentic social discourse, replacing it with algorithmically-curated interactions that often promote conflict or conformity.

c. Structuration Theory, Risk, and the Erosion of Institutional Trust (Giddens)

Anthony Giddens' (1990) work emphasizes that modern societies require trust in "abstract systems" that organize social life. Surveillance capitalism fundamentally destabilizes these systems by introducing complex, non-transparent, and high-stakes **digital risks**.

The sheer scale of data collection and deployment creates a pervasive uncertainty. Individuals cannot reasonably assess the risk that their data will be misused, weaponized, or lead to future discrimination (e.g., in employment, insurance, or credit). This unknowable risk is privatized and downloaded onto the individual.

More critically, it erodes **institutional trust**. The surveillance capitalist firms (e.g., major tech platforms) operate as powerful, global abstract systems, yet they lack the accountability mechanisms of traditional state or financial institutions. When these systems fail—through massive data breaches or political manipulation—the entire societal infrastructure of trust is weakened. Social relationships, therefore, are conducted within an environment where the infrastructure itself is known to be fundamentally untrustworthy and extractive, placing immense pressure on interpersonal trust.

Positive and Negative Impact on Social Relations and Digital Rights

Surveillance capitalism presents a classic double-edged sword: it supercharges the potential for connection while simultaneously corrupting the underlying quality and integrity of those connections.

Positive Impact on Social Relations (The Utility Paradox)

The utility provided by surveillance capitalist platforms is the primary reason for their ubiquitous adoption, representing the initial, powerful lure that masks the extractive logic (Zuboff, 2019).

- **Enhanced Connectivity and Weak Ties:** Digital platforms are highly effective at overcoming geographical and temporal boundaries, enabling the rapid formation of new ties and the maintenance of **weak ties** (Granovetter, 1973) crucial for professional networking, casual acquaintances, and accessing diverse information. For diasporic communities, this utility is paramount.
- **Social and Political Mobilization:** Platforms facilitate high-speed, decentralized coordination, allowing for effective **social mobilization** and collective action, as analysed by **Tufekci (2017)**. They offer a space for organizing protests, disseminating counter-narratives, and building community around shared socio-political goals, bypassing traditional, often controlled, media structures.
- **Identity Exploration and Support:** For marginalized groups, digital spaces can provide critical, safe venues for **identity exploration, affirmation, and finding support networks** that may be unavailable in their immediate physical environment. This utility in fostering belonging and shared experience is undeniable.

Negative Impact on Social Relations (The Corrosive Effects)

The negative impacts are structural, eroding the quality, authenticity, and spontaneity required for deep, meaningful social life.

The Corrosion of Trust and Intimacy

Intimacy and close social relationships are built upon the ability to be vulnerable, spontaneous, and non-instrumental, often requiring a protected space of privacy. Surveillance capitalism systematically undermines this by making **private life public property** and normalizing constant monitoring.

- **Self-Censorship and Calculated Disclosure:** Knowing that all communication is recorded, analysed, and potentially weaponized by the platform (or future algorithms) encourages rampant **self-censorship**. Individuals avoid discussing sensitive topics, curtailing emotional range, and presenting only a curated, risk-mitigated version of themselves. This calculated performance undermines the authenticity required for deep trust.
- **The Dissolution of Contextual Integrity:** Nissenbaum (2010) argues that privacy is contextual integrity—data should flow according to appropriate social norms. Surveillance capitalism destroys this by stripping data of its context (e.g., a private moment between partners) and repurposing it for commercial prediction or social shaming, thereby making *all* digital interactions potentially high-stakes.
- **Weaponization of Data in Relationships:** The permanent record created by platforms can be used in interpersonal conflicts, divorce proceedings, or social ostracism, turning past social expressions into future liabilities. This inherent risk fosters a low-level anxiety that permeates digital social interaction.

Algorithmic Mediation and Social Fragmentation

The algorithm is not a neutral manager of information; it is the **Chief Operating Officer of surveillance capital**, optimized purely for maximizing engagement (and thus data extraction). This optimization warps the social landscape.

- **Filter Bubbles and Polarization:** Algorithms prioritize content deemed most likely to provoke interaction, often favouring emotionally charged, divisive, or sensational material. This creates **filter bubbles** that systematically exclude diverse viewpoints and reinforce existing biases, contributing to social **fragmentation** and deepening political and social polarization (Pariser, 2011). Authentic discourse is replaced by the performance of ideological loyalty.
- **The Culture of Constant Competition and Metrics:** Social media metrics (likes, shares, views) translate social value into quantifiable data points. Relationships become a site of **social competition**, where personal worth is tied to data performance. This hyper-competitive, performance-driven environment undermines genuine supportive social bonds, fostering anxiety and narcissistic tendencies (Turkle, 2011).

Erosion of Digital Rights and Human Sovereignty

The sociological impact culminates in a systemic challenge to fundamental human rights, specifically the emergent category of **digital rights**.

Data Right	Impact of Surveillance Capitalism	Sociological Consequence
Right to Privacy	Continuous, non-consensual harvesting of intimate behavioural data	Obliteration of the protected space necessary for self-development and private relationships.
Right to Autonomy	Algorithmic “nudging” and pre-emptive behavioural modification	Diminishment of free will; reducing the individual to a predictable, controllable vector for capital
Right to Non-Discrimination	Use of opaque datasets to make life-altering social decisions (credit, employment, policing)	Institutionalization and scaling of historical social bias through technical means (algorithmic bias).
Right to	Opaque terms of service, trade	Disempowerment of the citizenry;

Know/Transparency	secrecy protecting algorithms.	inability to understand the forces governing their social environment.
-------------------	--------------------------------	--

Surveillance capitalism converts the human right to autonomy into a negotiable asset, positioning individuals not as citizens or autonomous social agents, but as **data subjects** whose lives are continuously monitored for surplus value generation. The freedom to be left alone (the core of privacy) is replaced by the obligation to be *visible* and *legible* to the market.

Suggestions for Mitigating the Impact

Addressing the deep sociological intrusion of surveillance capitalism requires interventions that move beyond simple privacy tweaks to structural reforms that re-establish human sovereignty over social life and data.

a. Legal and Regulatory Suggestions (Reasserting the Rule of Law)

The current regulatory landscape is ill-equipped to handle the asymmetry of power between individuals and surveillance capitalist firms.

1. **A Ban on Behavioural Futures Trading:** Following Zuboff's critique, the state must outlaw the commercial trade of prediction products derived from surveillance capital. This would strike at the economic heart of the problem by eliminating the lucrative market incentive for mass behavioural data extraction.
2. **Reinforcing Contextual Integrity and Purpose Limitation:** Data protection legislation must mandate that data collected for one explicit purpose (e.g., to send a message) cannot be repurposed for an entirely different, undisclosed purpose (e.g., behavioural modification). Consent must be granular, specific, and revocable without penalty.
3. **Algorithmic Accountability and Transparency:** For all high-stakes social systems (e.g., employment, credit, welfare), a "**Right to Explanation**" of algorithmic decisions must be enshrined. Furthermore, independent, non-governmental bodies must have the power to conduct compulsory, public, and source-code level audits of socially impactful algorithms to check for bias and discriminatory effects.

b. Sociological and Educational Suggestions (Cultivating Autonomy)

Mitigation requires changing how individuals perceive and interact with the digital environment, empowering them as autonomous social agents.

1. **Critical Digital Literacy as a Public Good:** Education must shift from simply teaching users *how* to use technology to teaching them about the *political economy* of the platforms they use. This includes instruction on the data extraction model, the mechanisms of algorithmic manipulation, and the sociological consequences of the surveillance economy.
2. **Fostering Digital Commons and Non-Commercial Social Spaces:** Public investment and support should be directed toward the development of non-commercial, cooperative, and open-source social networking platforms that are fundamentally designed to protect user autonomy, privacy, and the integrity of social discourse, free from the profit motive of data extraction.
3. **Advocacy for Data Unionization:** Encourage the formation of **Data Unions** where individuals collectively bargain for the use, sharing, and compensation of their data. This would reassert collective social power and challenge the unilateral appropriation of behavioural surplus value by treating data as the collective product of social labour.

c. Technological and Design Suggestions (Engineering Privacy)

The architecture of technology must be redesigned to support human sociality, not exploit it.

1. **Privacy and Security by Default and Design:** Legislation must enforce that all new digital products and services adopt the most privacy-respecting and security-conscious settings by default, shifting the burden of protecting autonomy away from the user.
2. **Decentralized and Federated Social Architectures:** Encourage the adoption of decentralized or federated social network protocols (like Mastodon or Activity Pub) that distribute data control and prevent the massive accumulation of behavioural surplus value in single corporate silos.
3. **Differential Privacy and Noise Integration:** Promote the use of advanced technological methods like **differential privacy**, which mathematically adds noise to datasets to allow for aggregated analysis while making individual identification highly improbable, thus protecting the social integrity of the collected information.

CONCLUSION

The phenomenon of surveillance capitalism is the defining socio-economic challenge of the early twenty-first century. This article, grounded in critical sociological frameworks—the Panopticon, datafied alienation, and the erosion of institutional trust—has demonstrated that the system’s primary impact extends far beyond commercial profiling. It is, at its core, a profound and corrosive force acting upon the integrity of human **social relationships** and the realization of **digital rights**.

By commodifying intimacy, fostering self-censorship, fragmenting social discourse through algorithmic bias, and systematically undermining the autonomy of the individual, surveillance capitalism transforms the social sphere from a site of spontaneous interaction into a meticulously managed environment optimized for profitable behaviour. The utility of connectivity has come at the steep price of sovereignty.

To safeguard the human future, the response must be equally structural and comprehensive. The suggestions proposed here—ranging from banning the behavioural futures market to promoting critical digital literacy and advancing decentralized social architectures—aim to re-establish a balance of power. The goal is to separate the immense social utility of digital connection from the destructive, extractive logic of surveillance capitalism, ensuring that technology serves human flourishing and authentic sociality, rather than exploiting it. The fight for human autonomy in the digital age is, fundamentally, a sociological struggle for the right to an unmonitored life.

REFERENCES

1. Baym, N. K. (2010). *Personal connections in the digital age*. Polity Press.
2. Couldry, N., & Mejiias, R. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
3. Deleuze, G. (1990). Postscript on the societies of control. *October*, 59, 3–7.
4. Foucault, M. (1975). *Discipline and punish: The birth of the prison*. Vintage.
5. Fuchs, C. (2014). Social media and the public sphere. *Media, Culture & Society*, 36(6), 751–770.
6. Giddens, A. (1990). *The consequences of modernity*. Stanford University Press.
7. Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology*, 78(6),

1360–1380.

8. Harcourt, B. E. (2015). *Exposed: Desire and disobedience in the digital age*. Harvard University Press.
9. Marx, K. (1867/1976). *Capital: A critique of political economy, Vol. 1*. Penguin Classics.
10. Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
11. Pariser, E. (2011). *The filter bubble: What the internet is hiding from you*. Penguin Press.
12. Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.
13. Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*. Basic Books.
14. Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208.
15. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.