

Surveillance, Control and Consent: A Survey of Data Privacy and Governance in the Age of Platform Society

Emily Nguyen¹

¹Australian National University, Canberra, Australia

emilynguyen07@protonmail.com¹

Abstract

In the digital age, platform-based technologies such as social media, search engines, and mobile applications have become central to everyday life. These platforms collect, process, and monetize massive amounts of personal data, often in ways that users neither fully understand nor explicitly consent to. This paper investigates the evolving dynamics of surveillance, control, and consent within the broader context of the platform society. It focuses on how digital platforms act as powerful intermediaries that shape social behaviour, economic participation, and political engagement through algorithmic design and data governance practices. Drawing on interdisciplinary sources from media studies, data ethics, and political economy, the study highlights how surveillance has shifted from state-led monitoring to a complex ecosystem driven by corporate interests. This shift has resulted in new forms of asymmetrical power, where users are constantly tracked, profiled, and nudged without meaningful opportunities for resistance or withdrawal. The paper also explores how the concept of consent is undermined by opaque data policies, interface manipulation, and legal loopholes that prioritize business models over user autonomy. Furthermore, it evaluates emerging frameworks of data privacy regulation, such as the General Data Protection Regulation (GDPR), and their effectiveness in holding platforms accountable. Special attention is given to the socio-political implications of data governance, including issues of digital inequality, algorithmic bias, and surveillance capitalism. By surveying recent developments in data governance and user rights, this paper aims to clarify the ethical and legal complexities of digital surveillance and control. It concludes by advocating for stronger regulatory mechanisms, greater transparency, and user-centred approaches to data consent and privacy, to ensure a more democratic and fair digital society in the age of platforms.

Keywords: California Consumer Privacy Act (CCPA), Digital Surveillance, General Data Protection Regulation (GDPR), Platform Society, Surveillance Capitalism.

1. Introduction

The increasing dominance of digital platforms has profoundly transformed how individuals communicate, interact, work, and participate in society. Companies such as Google, Meta, Amazon, and others operate vast digital ecosystems where data flows seamlessly, enabling real-time personalization, targeted advertising, predictive analytics, and algorithmic decision-making (Zuboff, 2019; Van Dijck, Poell and De Waal, 2018). These platforms are no longer just tools of communication or commerce; they have become governing entities in the digital realm, mediating social norms, market behaviour, and even political discourse (Pasquale, 2015; Gorwa, 2019). As such, questions of surveillance, control, and consent have become central to contemporary debates on data privacy and digital governance (Schneier, 2015; Solove, 2013).

In this platform-driven society, surveillance is often embedded in routine online interactions. Personal data is continuously collected through apps, smart devices, and digital infrastructures without users having full knowledge or control over its usage (Sadowski, 2019; Citron and Pasquale, 2014). The consent mechanisms offered are typically buried in long, complex terms of service, which users are compelled to accept in exchange for access (Illman and Temple, 2019). This dynamic raises concerns about the legitimacy of consent and the asymmetrical power held by platforms over users' personal information. Furthermore, the logic of platform capitalism encourages data maximization, reinforcing systems that prioritize profit over privacy and autonomy.

The introduction of GDPR, has attempted to restore user control by mandating transparency and accountability (EU, 2016). However, challenges remain regarding enforcement, platform compliance, and cross-border governance (Jia and Chen, 2022). The broader implications extend to democratic governance, social equity, and digital citizenship, making it essential to critically assess how data is governed in the platform era.

This paper explores these themes through a multidisciplinary lens. Section 2 outlines the conceptual framework of surveillance and platform society. Section 3 examines forms of data control and algorithmic governance. Section 4 discusses the challenges of meaningful consent. Section 5 analyses current privacy regulations, and Section 6 concludes with recommendations for ethical data governance and user empowerment.

2. Surveillance and the Platform Society

The concept of surveillance has evolved significantly in the digital era. Traditionally associated with state monitoring, surveillance today is increasingly conducted by private corporations operating large-scale digital platforms (Schneier, 2015; Sadowski, 2019). In the platform society, a term popularized by José van Dijck (Van Dijck, Poell and De Waal, 2018), surveillance is not merely an act of watching but a structural mechanism that enables the extraction, analysis, and commercialization of personal data. This shift marks a transformation in how power operates in digital spaces moving from hierarchical oversight to decentralized, continuous, and often invisible forms of control (Gorwa, 2019).

Digital platforms function as both facilitators of connectivity and instruments of data surveillance. Social media platforms, search engines, and mobile apps gather extensive behavioural data including location, preferences, interactions, and emotional responses. These data points are used to build predictive profiles of users, shaping their experiences through personalized content, targeted advertising, and recommendation algorithms (Pasquale, 2015). Unlike surveillance in earlier eras, which was often overt and centralized, contemporary digital surveillance is ambient and embedded within user-friendly interfaces (Citron and Pasquale, 2014).

One of the core features of surveillance in platform society is its asymmetrical nature. Users are observed, measured, and influenced, often without knowing how their data is used or who has access to it. At the same time, platforms remain opaque about their algorithms and data-sharing practices.

This "black box" condition (Pasquale, 2015) reinforces an imbalance in knowledge and power, where corporations know far more about individuals than individuals know about them.

Moreover, the logic of surveillance capitalism (Zuboff, 2019) drives platforms to continuously monitor user activity to feed algorithmic systems designed to predict and manipulate behaviour. This commodification of human experience erodes the boundaries between public and private, voluntary and coerced, and ultimately challenges democratic values and individual autonomy. In this context, surveillance becomes not only a technological feature but a governing principle of the platform society.

3. Data Control and Algorithmic Governance

As digital platforms have become central to everyday life, control over user data has emerged as a critical point of power. Unlike earlier information systems that relied on mutual exchange and consent, today's platforms operate through centralized infrastructures and algorithmic mechanisms that allow them to collect, store, and exploit personal data with minimal oversight (Sadowski, 2019). This section explores how data control and algorithmic governance function as key tools of platform power, shaping user behaviour and influencing decision-making in ways that are often hidden from public view

3.1. Centralized Data Collection and Storage

In platform society, control over data begins with large-scale collection and centralized storage systems. Major technology platforms collect vast amounts of user data ranging from browsing history and purchase behaviour to voice recordings and biometric identifiers (Iwuanyanwu, 2023). This data is stored in privately owned data centres, giving platforms exclusive access and control over information that was once scattered across multiple social institutions. The concentration of data ownership allows these corporations to shape digital ecosystems, create detailed user profiles, and monopolize insights derived from predictive analytics.

3.2. Algorithmic Decision-Making

Algorithms have become the invisible infrastructure through which data control is exercised. Whether recommending content, filtering information, or moderating speech, algorithmic systems act as gatekeepers in the digital realm. Platforms use machine learning models that adapt in real-time to user behaviour, increasing engagement while reinforcing specific content pathways. This personalised curation limits user agency by narrowing exposure to diverse viewpoints and reinforcing behavioural patterns based on past actions. It also raises concerns about filter bubbles and algorithmic manipulation (Pariser, 2011).

3.3. Opaque and Proprietary Systems

The opacity of algorithmic systems undermines transparency and accountability. Many platforms treat algorithms as proprietary trade secrets, offering little to no insight into how decisions are made or what data is used (Gorwa, 2019). This lack of visibility makes it difficult to challenge harmful outcomes such as biased moderation, discrimination, or the amplification of disinformation. Scholars argue that this algorithmic opacity functions as a form of "automated control," where users are governed by unseen processes that shape their digital lives without explicit consent (Citron & Pasquale, 2014).

3.4. Power Asymmetry and User Disempowerment

Control over data and algorithms reinforces power asymmetries between platforms and users. While companies have the tools to collect, analyze, and act on behavioural data, users typically lack mechanisms to monitor how their own data is used. Even when privacy settings are offered, they are

often complex, limited, or designed to discourage meaningful user control. This imbalance not only marginalizes user agency but also challenges the democratic values of openness, fairness, and accountability.

4. Consent and the Illusion of Choice

The foundation of ethical data practices in digital platforms rests on the principle of informed consent. In theory, users are expected to give voluntary, informed agreement before their personal data is collected, processed, or shared. However, in the practical context of platform society, consent often becomes a symbolic gesture rather than a meaningful exercise of autonomy. This section critically examines how consent is structured, the limitations of current models, and why many scholars consider it illusory in today's digital environment.

4.1. Consent Fatigue and Information Overload

Digital platforms typically require users to accept terms and conditions before gaining access to services. These documents are often lengthy, legalistic, and difficult to understand, leading users to click "agree" without reading or comprehending the implications. This phenomenon, known as consent fatigue results in a passive form of consent where users participate in data sharing not because they agree, but because they feel they have no other option. As a result, consent becomes procedural rather than purposeful.

4.2. Manipulative Interface Design

Many platforms employ interface strategies that nudge users towards agreeing with data collection practices. These include default settings that enable tracking, prominent "accept all" buttons, and buried privacy options. Known as "dark patterns," these design choices intentionally obscure the ability to make informed decisions, creating environments where consent is manipulated rather than freely given (Mathur *et al.*, 2019). This undermines the ethical basis of user agreement and contributes to a culture of coerced participation.

4.3. Lack of Real Alternatives

The monopolistic nature of major platforms further limits genuine choice. Services such as Google, Facebook, or Amazon have become so embedded in personal, social, and professional life that opting out is not a realistic option for most users. Without viable alternatives, users are effectively forced to agree to data terms as a condition for social inclusion, employment, or even access to government services in some cases. This compulsory participation challenges the voluntary nature of consent.

4.4. Rethinking Consent in Platform Society

Scholars and policy-makers have increasingly called for a redefinition of consent in digital contexts. Rather than relying on one-time, static agreements, new models suggest dynamic, ongoing consent that adapts to changing data practices and user preferences (EU, 2016; Jia and Chen, 2022). There is also a push for consent mechanisms that are more transparent, accessible, and grounded in user comprehension. These proposals aim to restore trust and empower users by aligning digital consent with ethical standards and human rights.

5. Data Privacy Regulations and Governance Models

As concerns over digital surveillance and data misuse have grown, governments and institutions worldwide have introduced legal frameworks to protect users' personal data. These regulations aim to enhance transparency, enforce accountability, and empower users with greater control over their digital identities. However, the implementation and effectiveness of these models vary significantly across regions. This section reviews the most influential data privacy laws, analyses their core principles, and assesses their impact in governing platform power (Jia and Chen, 2022).

5.1. The General Data Protection Regulation

Introduced by the European Union in 2018, the GDPR is widely regarded as the most comprehensive and influential data privacy framework. It establishes strong protections for individuals, including the right to access, correct, delete, and transfer personal data. GDPR also mandates explicit, informed consent and requires organizations to demonstrate data processing accountability through documentation, impact assessments, and clear privacy notices. Despite its strengths, critics argue that enforcement remains uneven and that large platforms often find ways to comply formally without changing exploitative practices (Gorwa, 2019).

5.2. The California Consumer Privacy Act

The CCPA, implemented in 2020, provides residents of California with rights similar to those under GDPR, including the right to know what data is collected, the right to delete it, and the right to opt out of its sale. However, the CCPA is often seen as less stringent, particularly in terms of consent and enforcement mechanisms. While it marks progress in U.S. privacy law, its scope is limited to specific businesses and does not guarantee a universal standard across the country.

5.3. Governance Gaps in Global Contexts

Many countries still lack robust data protection laws or have only minimal regulations in place. In regions where digital governance is weak or fragmented, platforms operate with little oversight, leading to widespread violations of privacy and consent. Moreover, cross-border data flows complicate governance, as data collected in one country is often processed or stored in another with different legal standards (Poell and De Waal, 2018). This fragmentation creates challenges for global accountability and user protection.

5.4. Comparative Overview of Major Privacy Regulations

To illustrate key similarities and differences between major data privacy laws, the following table presents a comparative overview:

Table 1: key similarities and differences between major data privacy laws

Regulation	Region	Consent Requirement	User Rights	Enforcement Power	Scope
GDPR	EU	Explicit & informed	Access, delete, correct, data portability	Strong (significant fines, DPA oversight)	Broad (all data processors targeting EU users)
CCPA	US (California)	Implied or opt-out	Access, delete, opt-out of sale	Moderate (Attorney General enforcement)	Limited (only businesses meeting thresholds)
LGPD	Brazil	Freely given, specific, informed	Confirm, correct, delete, portability	Moderate	Broad but newer and evolving
PDPA	Singapore	Reasonable & informed	Access, correct, withdraw consent	Moderate	Sector-based exceptions apply
None / Partial	Many Global South nations	Varies / minimal	Often limited or unclear	Weak	Limited or absent

5.5. Toward Global Data Governance

The absence of harmonized global standards poses a major challenge for regulating transnational platforms. A growing movement among scholars, policy-makers, and civil society advocates calls for the creation of international data governance norms that respect human rights and limit corporate overreach. Proposals include global data treaties, stronger enforcement cooperation, and data localization policies to protect national sovereignty. Such initiatives are crucial in countering the asymmetries of power that dominate the current platform landscape.

6. Conclusion and Recommendations

The transformation brought about by platform society has deeply altered the nature of surveillance, data control, and consent. Digital platforms now operate as powerful infrastructures of governance, not only collecting and storing vast volumes of user data but also using algorithms to shape behaviour, communication, and decision-making in often invisible ways. These practices are largely enabled by opaque systems of control and nominal forms of consent that rarely reflect genuine user autonomy. While users are often presented with choices regarding their data, these are constrained by manipulative design, legal complexity, and the lack of viable alternatives, resulting in a system that privileges platform power over individual rights. Regulatory responses such as GDPR and CCPA have introduced significant safeguards, including clearer data rights, stricter accountability requirements, and mechanisms for redress. However, these frameworks face limitations in enforcement and are often unable to address the global, transnational nature of data flows. In many regions, particularly in the Global South, privacy protections remain minimal or fragmented, creating a patchwork of governance that favours dominant platforms. The growing complexity of algorithmic systems and the asymmetry of power between users and digital corporations further complicate the regulatory landscape. To address these challenges, there is a clear need for reforms that focus on strengthening user rights and increasing transparency in data processing and algorithmic decision-making. Consent must be reimagined as a dynamic and ongoing process rather than a one-time event, supported by simplified interfaces and continuous user control. Greater algorithmic transparency is also essential, requiring platforms to disclose how decisions are made and what data is utilized in those processes. In addition, global cooperation in data governance must be expanded, moving toward international frameworks that uphold universal privacy standards while respecting local contexts. Efforts to promote digital literacy are equally vital, as informed users are better equipped to assert their rights and challenge harmful practices. Finally, encouraging the development of privacy-respecting technologies and ethical platform alternatives can provide users with real choices and help recalibrate the power dynamics of the digital ecosystem. Navigating the intersecting concerns of surveillance, control, and consent demands an integrated approach that blends legal, institutional, and cultural responses. A shift toward accountable, user-centric governance is not only necessary for protecting privacy but also fundamental to sustaining democratic values and human dignity in the digital age.

References

- Citron, D.K. and Pasquale, F., 2014. *The scored society: Due process for automated predictions*. Washington Law Review, 89(1), pp.1–33.
- EU, R., 2016. 679 of the European parliament and of the council (General Data Protection Regulation). *Official Journal of the European Union*, pp.1-88.
- Iwuanyanwu, C.C., 2023. *Facebook Artificial Intelligence Algorithm: Users' Awareness and Response to Data Privacy Issues*. Robert Morris University.
- Gorwa, R., 2019. *The platform governance triangle: conceptualising the informal regulation of online content*. *Internet Policy Review* 8, 2 (June 2019) [online]
- Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M. and Narayanan, A., 2019. Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on human-computer interaction*, 3(CSCW), pp.1-32.
- Pariser, E., 2011. *The filter bubble: What the Internet is hiding from you*. penguin UK.
- Pasquale, F., 2015. *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Sadowski, J., 2019. When data is capital: Datafication, accumulation, and extraction. *Big data & society*, 6(1), p.2053951718820549.

- Schneier, B., 2015. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.
- Solove, D.J., 2013. Introduction: Privacy self-management and the consent dilemma. *Harvard law review*, 126(7), pp.1880-1903.
- Tufekci, Z., 2015. Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Tech. LJ*, 13, p.203.
- Van Dijck, J., Poell, T. and De Waal, M., 2018. *The platform society: Public values in a connective world*. Oxford university press.
- Zuboff, S., 2019. The age of surveillance capitalism: The fight for a human future at the new frontier of power, edn. *PublicAffairs*, New York.
- Illman, E. and Temple, P., 2019. California consumer privacy act. *The Business Lawyer*, 75(1), pp.1637-1646.
- Jia K, Chen S. Global digital governance: paradigm shift and an analytical framework. *Global Public Policy and Governance*. 2022 Sep;2(3):283-305.