Surveillance Capitalism: How Your Data Becomes the Product

Nemanja Milanovic

DASC 205S

Old Dominion University

04/26/2025

Surveillance Capitalism: How Your Data Becomes the Product

Surveillance capitalism is a new economic logic that regards human experience as free raw material for industrial practices of extracting, predicting, and selling (Quan-Haase 2015). Harvard professor Shoshana Zuboff first identified this emerging form of capitalism when she identified it as a system by which companies collect and commodify personal data to predict and modify human behavior to make a profit (Zuboff 2022). In digital technologies, just about every aspect of daily life has been integrated with the collection, and the monetization of personal data has been sped up. Today, business models of major technology corporations are centered around extracting behavioral data, which is then processed through advanced algorithms in behavioral prediction products sold in behavioral futures markets. This paper describes the operation of surveillance capitalism, its implications for privacy and autonomy, the power dynamics between data collectors and users, and the regulatory responses from such an emerging phenomenon.

The Mechanics of Surveillance Capitalism

Fundamental operations of surveillance capitalism are the collective effort of systematical collection, analysis, and monetizing personal data at a scale never seen before. Google's discovery that the 'data exhaust' from user searches (previously thought of as waste material) could be predicted to inform user behavior and, in turn, improve targeted advertising was at the founding of what has become known as surveillance capitalism (Zuboff 2022). This discovery is the business model that would dominate internet platforms, which exempt an ostensibly free service in exchange for being able to extract behavioral data from users. All are adopted by Facebook, Amazon, Microsoft, and many other technology companies, with what these scholars call 'information capitalism,' where data collection is the main form of capital production (Landwehr, Borning, and Wulf 2021). The collection methods have become more sophisticated, including

direct online interaction and geolocation tracking, voice commands, biomarker data, and emotional status based on facial expressions or typing patterns.

Once personal data is collected, advanced machine learning algorithms process the data to create prediction products (Quan-Haase 2015). The products offered in these behavioral futures markets are expected to be bought by the user. Hence, these products are suspected by the product creators in their attempt to anticipate the user's preferences, behaviors, and decisions to purchase. As a result, the economic incentives in this model will drive them to collect more and more intrusive types of data and employ more sophisticated prediction techniques. Ironically, the inversion of this scenario of traditional capitalism, where companies sell products to consumers based on their supply, surveillance capitalism redefines the scenario, as the consumer's data becomes the product, and the consumer body is the object of behavioral modulation. This is a massive shift from markets based on consuming goods and services to markets based on extracting and commodifying personal information and predicting human behavior.

Privacy Implications and Consent Mechanics

The surveillance capitalist framework fundamentally challenges traditional privacy and well-informed consent ideas. Notices and consents, the current approach to privacy protection based primarily upon, have, by and large, been found to be fundamentally inadequate to the task of addressing pervasive data collection (Wong, Chong, and Aspegren 2023). Users who appear to have agreed to terms of service and privacy policies remain unaware of how far and why data collection extends. Surveys have shown that most Americans do not read privacy policies and that privacy policies are never read. However, even when users try to interact with the privacy policies, they are made purposely obscure by intricately worded, overly long, and frequently changed legal language provided by the companies that write them.

In digital environments, the ability to reduce the information asymmetry for data collectors and the user undermines knowledge of consent. There is nothing accidental about this asymmetry; this is a feature of surveillance capitalism that keeps information flowing and gives the sense of user choice and control (Tang, Li, and Fantus, 2023). When put in the face of modern data collection systems' complexity, scale, and opacity, the idea of privacy self-management—where data is expected to be dealt with by people making their read under-informed conditions—falls flat. In addition, when aggregated and analyzed, seemingly innocuous data points may reveal highly sensitive personal information about individuals that they never explicitly shared, which privacy scholars term as an aggregation problem in privacy protection. This problem highlights that users understand that the data is collected but cannot foresee the results of data analysis at scale.

Power Dynamics and Social Inequality

By reaffirming and reinforcing existing social inequality and asymmetrical power relations between the data collectors and the data subjects, surveillance capitalism renders people's movements into highly surveillable capital that can be exploited much more by the capital accumulators for their advantage. Today, dominant positions in the market have been taken by major technology platforms that dominate the digital infrastructure through which most online activity now occurs (Quan-Haase 2015). By concentrating such power into their hands, these companies can unilaterally set the terms of engagement, leaving users with total either/or comprehensive data collection or no services for playing a vital social and economic role in contemporary society. As a result, some scholars have called this dynamic 'instrumentation power,' in which the surveillance capitalists may work on a large scale by strategically using data-informed insights.

Surveillance technologies cannot produce more social biases than already exist in society since they increase existing biases. The automated decision systems used in surveillance capitalism algorithms demonstrate discriminatory behavior against minority groups and lead to increased detrimental effects against them. Any domain shows how these systems obtain historical biases from training data, which they use to develop feedback loops that aggravate social inequalities. The extended data collection and restricted opt-out options faced by economically disabled groups make experts describe their situation as "privacy poverty" because privacy privileges only elite groups. According to Tang, Li, and Fantus (2023) privacy problems do not exist, and they are listed as a philosophical issue slated to address overall social fairness principles and equity considerations.

Regulatory Responses and Future Directions

Wall Street Journal reported that Wall Street Journal declared surveillance capitalism as the leading cause behind new regulatory frameworks requiring restricted data collection methods. The General Data Protection Regulation (GDPR) is the most extensive European Union legislation determining personal information disclosure limits in 2018 (Labadie and Legner 2022). The regulatory framework supports three crucial areas, which mandate (1) target-driven restrictions (2) limited data processing, and (3) requires consent authorizations. In 2018, the United States introduced CCPA as legislation, which extends limited security measures to surveillance capitalism's data handling practices in a manner comparable to the GDPR framework of the European Union (Wong, Chong, and Aspegren 2023). The authors believe these policies represent strong beginnings yet lack provision for correcting the fundamental power inequalities in surveillance capitalism systems.

The reform of business models with intensive data extraction must be an essential regulatory requirement. Data collection entities should have fiduciary duties, while interoperability standards must become mandatory, with companies being required to dismantle specific platforms to decrease market power dominance. Research by Kumar and Singh (2022) shows that several systems have initiated new positive paths through technological methods that combine data reduction strategies, privacy technology components, and decentralized structural solutions. The solution to surveillance capitalism requires a systemic legal, technical, and social framework that will shape the future of surveillance capitalism through combined legislative and technological advancement and societal redefinition of data rights. The fundamental political issue regarding human freedom in our digital era dictates technological development standards.

Conclusion

Operating under surveillance capitalism, data-gathering methods for business monetization have produced a new handling practice in this present-day society. Safety capitalists build new economic systems by taking data records through processing to turn them into predictive tools that respect no previous privacy standards without user consent. The deliberate manipulation of data during this data-handling process leads to the generation of digital power inequalities that pose fundamental problems with respect to self-determinacy and social fairness in digital spaces. GDPR and CCPA must be supplemented with extended evaluations of data rights, business approaches, and user technology relationships to be even fit to measure additional growth. Surveillance capitalism will govern social and economic relationships between people in the coming decades primarily because people's data and the costs associated with personal data collection continue to shape these relationships.

Bibliography

Kumar, Mandeep, and Amritpal Singh. 2022. "Probabilistic Data Structures in Smart City: Survey, Applications, Challenges, and Research Directions." *Journal of Ambient Intelligence and Smart Environments* 14(4):229–84. doi: https://doi.org/10.3233/ais-220101.

Labadie, Clément, and Christine Legner. 2022. "Building Data Management Capabilities to Address Data Protection Regulations: Learning from EU-GDPR." *Journal of Information Technology* 38(1):16–44. doi: https://doi.org/10.1177/02683962221141456.

Landwehr, Marvin, Alan Borning, and Volker Wulf. 2021. "Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure." *Information, Communication & Society* 26(1):1–16. https://doi.org/10.1080/1369118X.2021.2014548

Quan-Haase, Anabel. 2015. "Technology & Society : Social Networks, Power, and Inequality : Quan-Haase, Anabel, Author : Free Download, Borrow, and Streaming : Internet Archive." *Internet Archive*. Retrieved April 26, 2025 (https://archive.org/details/technologysociet0000quan_t4g1).

Tang, Lu, Jinxu Li, and Sophia Fantus. 2023. "Medical Artificial Intelligence Ethics: A Systematic Review of Empirical Studies." *Digital Health* 9. doi: https://doi.org/10.1177/20552076231186064.

Wong, Richmond Y., Andrew Chong, and R. Cooper Aspegren. 2023. "Privacy Legislation as Business Risks: How GDPR and CCPA Are Represented in Technology Companies' Investment Risk Disclosures." *Proceedings of the ACM on Human-Computer Interaction* 7(CSCW1):1–26. doi: https://doi.org/10.1145/3579515.

Zuboff, Shoshana. 2022. "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization." *Organization Theory* 3(4). doi: https://doi.org/10.1177/26317877221129290.