

Contextualizing Surveillance Capitalism within a State-Corporate Crime Framework

Franky Yousry
Department of Criminology
University of Ottawa
Ottawa, Canada
fyousry@uottawa.ca

Abstract— After the Cambridge Analytica scandal, many scholars and polls suggested a trust deficit in the digital economy, as well as a public desire for stricter regulation and oversight over Big Tech after two decades of self-regulation and soft-regulation. Under surveillance capitalism, what does regulation actually entail and why has more not been done to protect privacy as a political right?

Keywords— Cambridge Analytica, democracy, mass surveillance, privacy, state-corporate crime

I. INTRODUCTION

The Cambridge Analytica scandal exposed the extent to which surveillance capitalism has transformed personal information into a source of economic and political power. As articulated by privacy scholars, legal scholars, democratic theorists, criminologists, certain politicians, activists and many concerned citizens after the news of Cambridge Analytica broke in 2018—it became apparent that under surveillance capitalism, informational and decisional privacy were and are still being eroded through the privatized online public sphere. Crucial to both individual autonomy and an authentic democracy, is privacy, a right that is not a distinct right or consolidated into a single conception, but a right that overlaps with other rights and of course, human dignity. It has also been argued that privacy is in fact *the* prerequisite for liberal democratic societies [1], [2]. Within the Canadian context, there is a growing recognition that breaches of individual privacy can produce collective or mass harm, for instance, though mass surveillance impacts individuals, it may cause collective harm through large-scale behavioural changes or through widespread lessening of dignity and autonomy [1]–[5]. This ongoing threat to the autonomy and dignity of citizens and democracy has been broadly acknowledged after the Cambridge Analytica scandal with public outcry to both reign in and punish corporations like Meta, and yet from a regulatory standpoint, not much has been addressed. This paper argues that understanding this apparent regulatory failure requires situating surveillance capitalism within a state-corporate crime framework. Rather than viewing privacy violations as isolated instances of corporate misconduct, surveillance capitalism should be understood as a system reproduced through the mutually reinforcing relationship between the State and Big Tech.

II. OF TECHNO-SOCIAL ENGINEERING AND SURVEILLANCE CAPITALISM

The underlying principle of the right to privacy is that of the inviolate person, which refers to the right of the individual to be free or safe from injury or violation. With the underlying principle of the inviolate person, informational privacy involves the degree to which one may control access by others to information about themselves, and whether, once acquired, legal constraints operate to prevent indiscriminate or other unwanted disclosure; while decisional privacy involves the scope of an individual's capacity to make decisions, the degree to which such decisions are adequately informed, and the ability to restrict the government from interfering with decisions. As is the general consensus amongst the literature, privacy essentially serves as a shield against unwanted interference from others whether it be other individuals, corporations or the government [1]–[9]. Furthermore, privacy facilitates independent decision-making, which in turn, facilitates autonomy which is essential to both individual identity and authentic participation within democratic processes.

Despite the importance of privacy as it relates to autonomy and democracy, scholars have articulated that it is difficult to conceptualize how protecting against intrusions to privacy can be legislated. What constitutes legitimate spheres of privacy, what comprises an invasion of privacy, and which countervailing interests may supersede privacy interests—these questions have generated a considerable amount of commentary, but also a profound lack of effective regulatory legislation nonetheless. It is this thread of *countervailing interests that may supersede privacy interests*, that this paper wishes to draw upon using a state-corporate crime framework.

III. SITUATING SURVEILLANCE CAPITALISM WITHIN A STATE-CORPORATE CRIME FRAMEWORK

A. Surveillance Capitalism

In the case of surveillance capitalism as mentioned previously, informational and decisional privacy are being 'disrupted' by corporations. This is because under capitalism, corporations seek to dominate information and decision-making environments in order to pursue their broad economic and political interests [7]–[10]. With the emergence of Big Data logic and infrastructure, surveillance technology and

neoliberal deregulation and privatization, surveillance capitalism emerged as both a logic and means to shape human behaviour and attitudes in order to secure particular economic and political interests of both corporations and the State [7]. It is therefore disingenuous to conflate surveillance capitalism with that of a digital economy that is purely an extension of technology and neoliberalism.

Furthermore, neoliberalism, which has been closely tied to broad ideological notions of the free market, free enterprise, as well as individual liberty and autonomy that requires protection from as well as ‘limited touch’ regulation from the State to sustain and maintain itself does not entirely overlap with the ideological underpinnings of surveillance capitalism. Though surveillance is a key feature of neoliberalism with the maintenance of ‘law and order’ and the protection of private property, surveillance capitalism emphasizes ‘consent’ with regards to contractual arrangements between service providers and service users; though as one might expect there is more power and influence with the corporate and State actors than that held by the individual using the services and these contracts. In order to access ‘free’ services, one must agree to offer their information, and since this information can and is commodified, it represents a new arena of commerce beyond digital markets, it represents an entire economy based around the adoption of extensive commercial surveillance and the erosion of privacy [7].

B. Privacy as a Political Right

Privacy as a political freedom and surveillance capitalism by extension, are phenomenon that are best understood as overlapping in specific contexts rather than abstract and vague. With regards to informational privacy (data privacy) which involves the collection and dissemination of data, technology, and the public expectation of privacy—under surveillance capitalism corporations and increasingly government organizations take data about individuals or groups of individuals and use it to create both risk and psychological profiles of individuals and groups of people, often distributing this data (via sharing or selling) without the individual or groups in question possessing the knowledge of what is happening to their data or how exactly it is being used. As for the relationship between decisional privacy and freedom of expression, surveillance practices can be construed as both a *background* and *active* disruption that can affect: the freedom to make decisions without undue influence; freely think; freely access and read materials; to be able to privately consult with peers; as well the freedom to develop new ideas including those that may be counter-hegemonic in nature. To put it in other words, it is *the inviolability via the process* of the exchange of ideas and the freedom to develop new ideas in relation to others that is in need of protection. Privacy can then be seen as an individual’s power to be in control of the relationships and the exchanges they choose to engage in.

Under surveillance capitalism, the identifiable “chilling effects” indicate that mass surveillance and algorithmic processes through these new technologies: a) deprives the individual of the power to exercise autonomy (through technological engineering and the fear of being surveilled and

discovered online); b) results in hyperpolarization and fragmentation of civil society; and c) facilitates the normalization of surveillance practices that will eventually lead to greater invasions or disruptions to privacy. It can therefore not be overlooked, that these invasions and disruptions to privacy must not be simplified by being solely located within the context of corporate harm, they must also be located within the context of harm by the State.

C. Moving Towards a State-Corporate Crime Framework to Understand Gaps in Privacy Protection Legislation

State-corporate crime provides a useful framework for understanding why meaningful privacy protections have proven difficult to implement. Rather than treating corporations and governments as fundamentally opposed actors, state-corporate crime scholarship emphasizes their mutual dependence in maintaining capitalist markets and facilitating economic growth. The State creates corporations through law, defines the legal boundaries within which they operate, and structures regulatory systems that determine acceptable forms of corporate conduct. Regulation is therefore *productive*. Regulation does not simply restrain markets; it actively *produces the conditions* under which markets function [11], [12]. From this perspective, surveillance capitalism is sustained not merely through corporate behaviour but through regulatory choices that normalize extensive data collection while limiting meaningful constraints upon commercial surveillance [8], [9].

Following the Office of the Privacy Commissioner’s (OPC) Federal Court case against Facebook, Parliament introduced Bill C-11 (2020) and later Bill C-27 (2022) to modernize Canadian privacy law (neither were implemented). In its 2021 submission, the OPC argued that while Bill C-11 promised stronger privacy protections, greater individual control, and harsher penalties for privacy violations, Bill C-11 ultimately prioritized *commercial interests over privacy rights*. According to the OPC, Bill C-11 expanded organizations’ ability to collect, use, and disclose personal information without meaningful consent, reflecting the realities of a data-driven economy rather than challenging the logic of surveillance capitalism.

While the OPC (2021) contended that Parliament continued to frame privacy and economic growth as competing interests, often favouring innovation and commerce, the OPC also rejected the idea that privacy and innovation are inherently incompatible. Instead, it advocated for modernized laws that would permit greater organizational flexibility to process personal information without consent for “responsible innovation” and socially beneficial purposes, including public health, *economic growth*, and improved public policy, while embedding privacy as a fundamental human right. This position, however, appears contradictory.

Although the OPC criticized Bill C-11 for privileging commercial interests, it also endorsed broader exceptions to consent and proposed amendments aimed at sustaining information-based commerce and relying more on corporate responsibility. Ultimately, Bill C-11, Bill C-27 and the OPC’s 2021 report suggested that both Parliament and the OPC

accepted expanded data collection as necessary for economic development, and that corporations should be tasked with ensuring corporate responsibility to offset weak enforcement measures—which serves to reinforce this idea that there is State support for surveillance capitalism, in which economic priorities have and continue to outweigh meaningful privacy protections.

IV. CONCLUSION

The Cambridge Analytica scandal is commonly interpreted as an extreme privacy harm that resulted from corporate misconduct and ended with political consequences. However, by contextualizing surveillance capitalism through a state-corporate crime framework, privacy harms such as Cambridge Analytica are better understood as products of broader political and economic arrangements. Governments do not merely respond to corporate surveillance; through legislation, regulation, and institutional design they actively shape the conditions under which surveillance capitalism operates. The Canadian debate surrounding Bill C-11 (2020) demonstrates that even proposed reforms responding to widespread public concerns surrounding privacy, continue to prioritize the needs of a data-driven economy. Although regulatory institutions criticized aspects of the legislation, they largely accepted the continued expansion of data processing as compatible with democratic governance. Consequently, privacy as a political right remains subordinate to countervailing economic priorities.

In addition, for future research, there is a particular strength in contextualizing surveillance capitalism within a state-corporate crime framework. A state-corporate crime framework successfully shifts the focus of analysis from individual corporate wrongdoing towards the symbiotic institutional relationships between the State and Big Tech. Doing so highlights that contemporary invasions of informational and decisional privacy are not isolated regulatory failures but structural outcomes of a political economy that increasingly depends upon the collection,

circulation, and commercialization of personal information. Understanding how to legislate meaningful privacy protections—and, consequently, understanding why current privacy protections remain inadequate—requires examining not only corporate practices but also the State's role in reproducing and legitimizing mass surveillance and surveillance capitalism.

REFERENCES

- [1] A. Westin, *Privacy and freedom (e-book)*. Ig Publishing, 1967.
- [2] V. Steeves, "Theorizing privacy in a liberal democracy: Canadian jurisprudence, anti-terrorism, and social memory after 9/11," *Theoretical Inquiries*, vol. 20, no. 1, pp. 323–341, 2019.
- [3] Canadian Security Intelligence Service, "Foreign interference threats to Canada's democratic process." CSIS, 2021. [Online]. Available: <https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-threats-to-canada%27s-democratic-process.pdf>
- [4] Office of the Privacy Commissioner of Canada, "Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020." Office of the Privacy Commissioner of Canada, May 11, 2021. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/
- [5] V. Steeves, "Big Data Surveillance: Privacy and Trust Implications," *The Journal of Intelligence, Conflict, and Warfare*, vol. 4, no. 2, 2021.
- [6] D. Solove, "Conceptualizing privacy," *California Law Review*, vol. 90, pp. 1087–1155, 2002.
- [7] D. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven, Connecticut: Yale University Press, 2013.
- [8] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: New York: Public Affairs, 2019.
- [9] M. Andrejevic and K. Gates, "Editorial | Big data surveillance: Introduction," *Surveillance and Society*, vol. 12, no. 2, pp. 186–195, 2014.
- [10] J. Habermas, *The Structural Transformation of the Public Sphere: An Inquiry Into a Category of Bourgeois Society*. in *Studies in Contemporary German Social Thought*. Boston, Massachusetts: Massachusetts Institute of Technology, 1992.
- [11] D. Miller and C. Harkins, "Corporate strategy, corporate capture: food and alcohol industry lobbying and public health," *Critical Social Policy*, vol. 30, no. 4, 2010.
- [12] R. Kramer, R. Michalowski, and D. Kauzlarich, "The origins and development of the concept and theory of State-Corporate crime," *Crime & Delinquency*, vol. 48, pp. 263–282, 2002.