Privacy, Power, and the Public Good: Balancing Surveillance and Liberty

October 10, 2025

Word Count: 1479

I. Introduction

"[T]he essence of a menacing surveillance state, be it the NSA or the Stasi or Big Brother or the Panopticon, is the knowledge that one can be watched at any time by unseen authorities." [1]

- *Glenn Greenwald*

In modern states, governments increasingly deploy surveillance tools, including, but not limited to, CCTV cameras, biometric databases, and central bank digital currencies (CBDCs). They do so under the banner of public safety and security. While these technologies promise to protect the public, they also carry the danger of eroding privacy, therefore allowing intrusive oversight of citizen's beliefs, associations, and daily routines.[2] Thus, public safety and the individual's privacy sit in tension. A liberal democracy cannot allow unchecked surveillance lest it overthrows the very freedoms it seeks to defend; but some intrusions may be justified in rare, exceptional circumstances.[3] This essay argues that privacy is the cornerstone of individual freedom in a democratic society and that government interference should be tightly limited to proportionate circumstances involving clear threats to public safety. It first examines the value of privacy, then evaluates the circumstances under which government interference may be justified, and finally proposes policy measures.

II. The Value and Importance of Privacy in a Free Society

---

[1] Greenwald, Glenn. 2014. *No Place to Hide*. Metropolitan Books.

[2] Stanford Encyclopedia of Philosophy. 2023. "Privacy." *Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/entries/privacy/

[3] Boynton, Sean. 2025. "Could the police get your online data without a warrant? What Liberals propose." *Global news.* https://globalnews.ca/news/11466300/bill-c2-strong-borders-act-internet-privacy-concerns/

Protecting privacy requires more than the simple idea that "nobody's watching." It rests on deeper philosophical foundations that reveal why privacy is essential to human freedom and dignity. One key aspect is autonomy - the "space to think." Privacy provides individuals with room to reflect, experiment, and grow intellectually or morally without a constant fear of judgement.[4] If every thought, gesture, or association is subject to scrutiny, then self-censorship becomes increasingly prevalent. Privacy allows us the breathing room to develop beliefs and identities, which is especially important for minority or unpopular views. Additionally, privacy embodies dignity and respect by recognizing each individual's right to set boundaries against intrusion. As Alan Westin explains in *Privacy and Freedom,* it is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[5] Without the space to think, speak, associate, and develop identities outside state scrutiny, individual liberty cannot truly flourish. Westin's four "states" of privacy - solitude, intimacy, anonymity, and reserve - highlight the varied ways in which personal control and boundaries preserve individual integrity.[5] Beyond the individual, privacy is also vital to democracy. As Michel Foucault's concept of the Panopticon shows, the mere possibility of being watched disciplines citizens into conformity, erodes spontaneity, and reshapes norms.[6] When state monitoring becomes routine, people may refrain from dissent or unconventional behaviour, qualities essential for democratic life.[7] A practical value of privacy is

---

[4] Sætra, Henrik. 2022. "The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security." *Technology in Society* 68 (101854)

[5] Westin, Alan. 1967. *Privacy and Freedom.* Atheneum.

[6] Foucault, Michel. 1975. *Discipline & Punish: The Birth of the Prison.* Pantheon Books.

[7] Manheim, Karl and Lyric Kaplan. 2019. "Artificial Intelligence: Risks to Privacy and Democracy." 21 Yale J.L. & Tech. 106

that it limits state or other agents' power to abuse information or make errors; data leaks, profiling mistakes, or shifting political environments may expose citizens to harm.[8] Finally, the "nothing to hide" argument - "if you have nothing to hide, why fear surveillance?" - is widely rejected by privacy theorists, because it ignores how even innocuous data, in aggregate, can be used harmfully (e.g., discrimination).[2] Thus, privacy is not about hiding wrongdoing but about preserving autonomy, pluralism, and protection from a concentrated power.

In a free society, privacy is not a luxury or secondary concern - it is a cornerstone of liberty.[4] Without private spaces, the foundations of political discourse, cultural diversity, and dissent fall. When citizens fear that their day to day life is being monitored, they may avoid organizing, protesting, or speaking critically, thereby undermining the very essence of democracy. Privacy also protects pluralism by shielding minority groups and dissenting voices from the scrutiny and influence of the majority. Equally important, it nurtures self-development by allowing individuals to explore beliefs, form relationships, and experiment with identity free from the judgement or coercion from others. In this sense, privacy is not merely a personal right but a structural precondition for freedom itself.[9] A truly free society must always ensure that surveillance remains the exception and that privacy remains the standard.

III. Government Interference and Policy Proposals

[8] Rayhan, Rajan and Shahana Rayhan . 2023. "AI and Human Rights: Balancing Innovation and Privacy in the Digital Age." DOI: 10.13140/RG.2.2.35394.56001

[9] Dufresne, Philippe. 2023. "Protecting privacy in a digital age." *Office of the Privacy Commisioner of Canada.* https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/sp-d_20231127/

Government interference with privacy should be rare, tightly controlled, and justified only under exceptional circumstances. The 2019 case involving the Royal Canadian Mounted Police (RCMP) revealed how they had used the facial-recognition software *Clearview AI* without prior authorization or transparency. The software scraped billions of photos from social media to match faces for policing purposes. The *Office of the Privacy Commissioner of Canada* found that this violated federal privacy law because individuals had not consented to the use of their images, nor were they aware of how the data were collected or stored.[10] This case demonstrated how quickly emerging technologies can outpace existing privacy protection, increasing the risk of misuse and undermining public trust. It underscores the urgent need for strong safeguards and accountability measures. Because privacy is foundational to freedom, any state intrusion must meet strict standards of necessity, transparency, and oversight. The government may only intervene when pursuing a legitimate aim - such as countering terrorism, serious crime, or financial fraud - and only in response to a specific, demonstrable threat.[7] Intrusions must use the least invasive means available; if a targeted warrant or human investigation can achieve the goal, broad surveillance or data harvesting is unjustified. Moreover, the scale and duration of any surveillance must stay proportional to the threat, with strong design limits to minimize data collection, retention, and use. Algorithms should be transparent and auditable to prevent hidden bias or abuse.[8] To prevent overreach, all surveillance powers should include sunset clauses, and individuals affected must have avenues for recourse and redress.[11] In line with Canadian privacy law and the Office of the Privacy Commissioner, such measures ensure that any state action

---

[10]Office of the Privacy Commissioner of Canada. 2021. “Police use of Facial Recognition Technology in Canada and the way forward.” *Office of the Privacy Commissioner of Canada.* Police use of Facial Recognition Technology in Canada and the way forward - Office of the Privacy Commissioner of Canada

[11] Lauenroth, Benjamin. 2025. “The Critical Nature of Sunset Provisions in National Security Legislation.” *The Georgetown Law Journal.* Vol. 113:885.

taken in the name of security remains transparent, temporary, and accountable to democratic principles.

Building on these principles, a fair and accountable surveillance regime must integrate privacy protections at every stage of both policy development and technology implementation. First, Privacy Impact Assessments (PIAs) should be mandatory before using new systems such as facial recognition, or central bank digital currencies (CBDCs).[9] These assessments should also be made publicly available and open to feedback, evaluating risks to privacy, discrimination, data handling, and retention.[7] Access to mass data, such as from CCTV footage or financial records, should generally be restricted to de-identified or aggregated information. Only when there is a specific, warrant-approved reason should identifiable data be accessed.[3] Strong data governance should ensure that information collected for one purpose (for example, crime prevention) cannot be repurposed for another (such as political monitoring) without new authorization. An independent oversight body, composed of judicial and technical experts, should continuously inspect surveillance programs, publish reports, and investigate complaints. Additionally, to maintain public transparency while respecting operational secrecy, governments should regularly disclose the number and types of warrants, surveillance requests, and data usage.[8] Finally, all surveillance authorities should include sunset and renewal provisions, which automatically expire after a set term - typically three to five years - unless renewed through parliamentary review with clear evidence of effectiveness and proportionality.[11] Together, these policies would uphold privacy as a democratic safeguard while ensuring that necessary surveillance remains lawful, limited, and transparent.

IV. Addressing objections and counterarguments

To understand the importance of strong privacy protections, it is helpful to consider and address common objections especially in an era of rapid technological change. Some argue that "security must trump privacy" - that during crises, surveillance should take precedence.[4] Yet if privacy is continually suspended in the name of safety, emergency powers risk becoming permanent, giving the state unchecked authority. The default must always be privacy, with surveillance justified only as an exception. Others claim "we have nothing to hide," but this overlooks how aggregated, seemingly harmless data can expose personal beliefs, and political leanings, thus discouraging personal expression and dissent. Another objection holds that modern technology demands new trade-offs, implying that privacy must yield to innovation.[4] In reality, the proper response is not to abandon rights but to strengthen governance - through transparency, accountability, and oversight. As Michel Foucault cautioned, surveillance's greatest danger lies in its subtle normalization, as people internalize control.[6] Finally, some argue that restrictions on surveillance allow criminals to evade detection, yet mass monitoring often produces vast quantities of irrelevant data while undermining public trust.[12] Focused, warrant-based investigations are more effective and less intrusive. In short, none of these objections justify weakening privacy; rather, they underscore the need to balance safety with freedom through targeted, transparent, and proportionate measures.[2]

V. Conclusion

[12] Almeida, Denise, Konstantin Shmarko, and Elizabeth Lomas. 2021. "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks." AI and Ethics 2:377–387.

Privacy is not a niche or sentimental concern; it is integral to autonomy, innovation, and democratic vitality. In a free society, individuals must retain control over which aspects of their lives are exposed and to whom. Governments may sometimes justifiable interfere, but only under strict conditions: clear threat, necessity, oversight, transparency, and checks against abuse. Hence the proper balance is to start with privacy as the default, and permit government penetration only when it satisfies precise rules and accountability. The enduring lesson from theory, law, and history is clear: protecting privacy is what safeguards citizens from state overreach and makes genuine freedom possible.

Bibliography

Almeida, Denise, Konstantin Shmarko, and Elizabeth Lomas. 2021. “The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks.” AI and Ethics 2:377–387.

Boynton, Sean. 2025. “Could the police get your online data without a warrant? What Liberals propose.” *Global news.* https://globalnews.ca/news/11466300/bill-c2-strong-borders-act-internet-privacy-concerns/

Dufresne, Philippe. 2023. “Protecting privacy in a digital age.” *Office of the Privacy Commisioner of Canada.* https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/sp-d_20231127/

Foucault, Michel. 1975. *Discipline & Punish: The Birth of the Prison.* Pantheon Books.

Greenwald, Glenn. 2014. *No Place to Hide*. Metropolitan Books.

Lauenroth, Benjamin. 2025. “The Critical Nature of Sunset Provisions in National Security Legislation.” *The Georgetown Law Journal.* Vol. 113:885.

Manheim, Karl and Lyric Kaplan. 2019. “Artificial Intelligence: Risks to Privacy and Democracy.” 21 Yale J.L. & Tech. 106

Office of the Privacy Commissioner of Canada. 2021. “Police use of Facial Recognition Technology in Canada and the way forward.” *Office of the Privacy Commissioner of Canada.* Police use of Facial Recognition Technology in Canada and the way forward - Office of the Privacy Commissioner of Canada

Rayhan, Rajan and Shahana Rayhan . 2023. “AI and Human Rights: Balancing Innovation and Privacy in the Digital Age.” DOI: 10.13140/RG.2.2.35394.56001

Sætra, Henrik. 2022. “The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security.” *Technology in Society* 68 (101854)

Stanford Encyclopedia of Philosophy. 2023. “Privacy.” *Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/entries/privacy/

Westin, Alan. 1967. *Privacy and Freedom.* Atheneum.