Title: Lines We Should Not Cross: Privacy, Surveillance, and Canada's Digital Charter

Word Count: 1,379

Date: October 26, 2025

Introduction

From CCTV cameras on public streets to biometric border checks and AI based predictive policing, governments now collect and analyze citizen data on a scale unimaginable a generation ago.[1] Canadian officials justify these technologies as necessary to ensure public safety in an era of digital threats, terrorism, and cybercrime. Yet each advance in surveillance carries an implicit cost: the erosion of privacy. In Canada, this tension has taken legislative form in the federal government's Digital Charter Implementation Act (Bill C-27), which seeks to modernize privacy law while enabling responsible data use.

Privacy is valuable because it safeguards autonomy and democratic equality, the ability of citizens to live without undue scrutiny or manipulation. While the Canadian government's Digital Charter promises both protection and innovation, it also normalizes an expanding state presence in citizens' digital lives. Drawing on Alan Westin's theory of privacy as informational control and John Stuart Mill's harm principle, this essay contends that privacy must function as a constitutional boundary that limits surveillance power. True balance between safety and privacy requires surveillance to be lawful, necessary, and proportionate, with independent oversight to prevent the transformation of "safety" into pretextual control.[2]

Body Paragraph 1: The Value of Privacy, Westin's Informational Control and Human Autonomy.

[1] "Privacy." *Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Stanford University, 19 Oct. 2023, https://plato.stanford.edu/entries/privacy/.
[2] "Privacy." *Routledge Encyclopedia of Philosophy*, Taylor & Francis, https://www.rep.routledge.com/articles/thematic/privacy/v-1.

Privacy is valuable not because citizens have something to hide, but because they have something to be, independent, reflective selves capable of free moral judgment.[3] Alan Westin's seminal work Privacy and Freedom (1967) defines privacy as "the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others."[4] For Westin, control over personal data is not merely procedural, it is the essence of autonomy. In a democracy, autonomy underpins all other freedoms: freedom of conscience, expression, and association.[5]

Without privacy, citizens internalize surveillance, moderating behaviour to conform with social expectations. Michel Foucault's panopticon metaphor captures this phenomenon: people who believe they are watched begin to police themselves.[6] This subtle form of coercion undermines freedom even in the absence of overt state violence. In Canada, where Section 8 of the Charter of Rights and Freedoms guarantees protection against "unreasonable search or seizure," privacy stands as the legal manifestation of this autonomy.

Yet recent initiatives like Toronto's proposed Sidewalk Labs "smart city" project show how digital technologies can bypass these protections.[7] The project aimed to collect extensive urban data, from movement patterns to waste disposal habits, through embedded sensors and connected infrastructure. Although marketed as a model of urban efficiency, critics, including former

---

[3] Bélanger, France, and Robert E. Crossler. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly*, vol. 35, no. 4, 2011, pp. 1017–41. *JSTOR*, https://doi.org/10.2307/41409971. Accessed 27 Oct. 2025.
[4] Reynolds, Osborne M. *Administrative Law Review*, vol. 22, no. 1, 1969, pp. 101–06. *JSTOR*, http://www.jstor.org/stable/40708684. Accessed 27 Oct. 2025.
[5] "Internet Research Ethics." *Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Stanford University, 13 July 2025, https://plato.stanford.edu/entries/ethics-internet-research/.
"Surveillance Ethics." *Internet Encyclopedia of Philosophy*, http://iep.utm.edu/surv-eth/.
[6] Office of the Privacy Commissioner of Canada. *"Protecting Privacy in a Digital Age."* Speech/Statement, 27 Nov. 2023, https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/sp-d_20231127/.
[7] "Sidewalk Toronto: The Vision Behind Google's Failed City." *Tomorrow.city*, https://www.tomorrow.city/sidewalk-toronto-the-vision-behind-googles-failed-city/.

Ontario Privacy Commissioner Ann Cavoukian, warned that such pervasive surveillance would create a "city of constant observation," eroding individuals' ability to act freely in public. Cavoukian ultimately resigned from the project over its refusal to guarantee data anonymization at the source. When data collection becomes passive and continuous, as in smart cities, smartphones, and biometric IDs, individuals lose the practical ability to exercise control.[8] Privacy thus becomes not just a personal concern but a structural condition for freedom. Its value lies in ensuring that citizens remain subjects of their choices, not objects of state data systems.

Body Paragraph 2: Privacy and Freedom in the Context of Canada's Digital Charter.

In response to these technological shifts, the Canadian government introduced the Digital Charter Implementation Act (Bill C-27) in 2022.[9] Its key component, the Consumer Privacy Protection Act (CPPA), promises to give Canadians "greater control and transparency when companies handle their personal information."[10] On the surface, the Digital Charter recognizes Westin's principle of informational control by codifying rights of consent, data portability, and deletion. Yet, embedded within the same legislative ecosystem are parallel measures that expand state surveillance capacity in the name of safety, such as digital ID initiatives, cross border data

---

[8] Lange, Christian. "The Nobel Peace Prize 1921 – Nobel Lecture." *The Nobel Peace Prize*, NobelPrize.org, https://www.nobelprize.org/prizes/peace/1921/lange/lecture/.

[9] Innovation, Science and Economic Development Canada. *"Bill Summary: Digital Charter Implementation Act, 2020."* Government of Canada, https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020.

[10] Innovation, Science and Economic Development Canada. *"Consumer Privacy Protection Act (CPPA)."* Government of Canada, https://ised-isde.canada.ca/site/innovation-better-canada/en/consumer-privacy-protection-act

sharing agreements, and AI based security analytics funded under Public Safety Canada's Cybersecurity Strategy.

This duality reveals a fundamental paradox: as Canada strengthens citizens' individual rights to data protection, it simultaneously enlarges the institutional apparatus of surveillance.[11] In 2023, for instance, federal and provincial governments began piloting Digital IDs, systems intended to streamline access to healthcare and financial services. However, privacy advocates such as the Canadian Civil Liberties Association (CCLA) warn that these IDs could enable centralized tracking of citizens' transactions and movements.[12] The absence of strict "purpose limitation" clauses means that data gathered for identification could later be used for law enforcement or commercial profiling.

Mill's harm principle provides a useful lens here. He argues that liberty may only be restricted to prevent harm to others, not to promote efficiency or convenience. Yet the Digital Charter's language of "innovation" and "trust" risks expanding state power beyond Mill's limit, treating privacy as a variable to be optimized rather than a right to be respected. This danger is evident in the RCMP's use of Clearview AI's facial recognition technology, which collected over three billion images from the internet without consent, claiming it would improve public safety.[13] In 2021, the Office of the Privacy Commissioner found this practice unlawful, ruling that the RCMP had violated federal privacy law despite its "security" justification.[14] The case reveals

---

[11] "Privacy." *Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Stanford University, 19 Oct. 2023, https://plato.stanford.edu/entries/privacy/.
[12] Innovation, Science and Economic Development Canada. *"Consumer Privacy Protection Act (CPPA)."* Government of Canada, https://ised-isde.canada.ca/site/innovation-better-canada/en/consumer-privacy-protection-act
[13] "RCMP Used Facial-Recognition Tech Without Proper Legal Safeguards, Documents Show." *CBC News*, https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5479673
[14] HR Law Canada. "Federal Court Strikes RCMP Class Action over Alleged Privacy Breach." *HR Law Canada*, 12 May 2025, https://hrlawcanada.com/2025/05/federal-court-strikes-rcmp-class-action-over-alleged-privacy-breach/

how easily privacy protections can be reframed as barriers to innovation and policing efficiency.[15] Thus, while the Charter reflects good intentions, its implementation blurs the line between protection and penetration. A genuinely free society must treat privacy as a constitutional constraint on surveillance, not as an adjustable parameter within it.

Body Paragraph 3: Finding the Proper Balance.

To reconcile privacy and public safety, Canada must operationalize three normative principles: lawfulness, necessity, and proportionality. These standards, derived from international human rights jurisprudence and privacy theory, offer a structured test for legitimate surveillance.

First, lawfulness demands that any intrusion be grounded in clear, publicly accessible legislation, not secret ministerial directives. This ensures democratic oversight and predictability. Second, necessity requires the government to demonstrate that no less intrusive means could achieve the same security objective.[16] Finally, proportionality insists that the benefits to public safety must outweigh the costs to individual rights. As legal scholar Lisa Austin notes, "privacy's erosion in the name of efficiency often reflects administrative convenience rather than true necessity."

Canada's experience with cell site simulators (IMSI catchers) illustrates the need for these principles.[17] In 2017, a CBC investigation revealed that the RCMP and local police forces had quietly deployed these devices, which mimic cellphone towers to intercept signals and identify

---

[15] Stevens, Yuan, and Ana Brandusescu. *"Weak Privacy, Weak Procurement: The State of Facial Recognition in Canada."* Centre for Media, Technology & Democracy, 6 Apr. 2021, https://www.mediatechdemocracy.com/all-work/weak-privacy-weak-procurement-the-state-of-facial-recognition-in-canada.

[16] Office of the Privacy Commissioner of Canada. *"Protecting Privacy in a Digital Age."* Speech/Statement, 27 Nov. 2023, https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/sp-d_20231127/.

[17] Office of the Privacy Commissioner of Canada. *"OPC Investigation into the RCMP's Use of Facial Recognition Technology."* 16 Aug. 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170816_rcmp/.

users, without judicial warrants or public disclosure. The Privacy Commissioner later condemned the practice, stating that it violated the expectations of privacy guaranteed under Section 8 of the Charter. The lack of transparency and legal clarity showed a failure of both lawfulness and proportionality: surveillance justified in the name of public safety had drifted into secrecy.

Applying these principles to Canada's Digital Charter suggests several policy reforms. (1) Create an independent Data Protection Commissioner with authority to audit government surveillance programs, not only private sector breaches. (2) Mandate public impact assessments before deploying technologies such as predictive policing or facial recognition, similar to the EU's GDPR Article 35 requirements. (3) Enshrine data minimization and purpose limitation into federal law, ensuring that information collected for identification cannot be reused for unrelated surveillance. (4) Require judicial warrants for any government access to citizen biometric or financial data under digital ID systems.

These measures would translate theoretical respect for autonomy into enforceable safeguards. By adopting them, Canada could preserve both public trust and public safety, proving that democratic societies can govern technology without surrendering to it. Surveillance should serve as a shield against danger, not a window into citizens' lives.

Conclusion

Privacy is not an obstacle to public safety; it is its precondition. Without privacy, citizens lose the autonomy to think, dissent, and participate freely in democracy, eroding the very trust that security relies on. The Digital Charter Implementation Act represents a pivotal moment in Canada's struggle to define that balance. Its promise of "control and transparency" reflects

genuine progress, yet its permissive stance toward data integration risks institutionalizing surveillance as normal governance.[18]

Drawing on Westin's conception of informational control and Mill's harm principle, this essay has argued that privacy must act as a constitutional boundary, not a negotiable policy choice. Governments may interfere with privacy only when the intrusion is lawful, necessary, and proportionate, and only with independent oversight.[19] The proper balance between privacy and public safety, then, is not a midpoint between two competing values but a hierarchy: safety should never come at the expense of freedom's foundation. In an age where surveillance is easy and freedom is fragile, the test of democracy will be how firmly Canada chooses to draw that line.

[18] Justice Canada. *Canadian Charter of Rights and Freedoms / Charte canadienne des droits et libertés.* Government of Canada, Department of Justice, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/.
[19] Justice Canada. *Canadian Charter of Rights and Freedoms / Charte canadienne des droits et libertés.* Government of Canada, Department of Justice, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/.

Bibliography

Justice Canada. *Canadian Charter of Rights and Freedoms / Charte canadienne des droits et libertés.* Government of Canada, Department of Justice, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/.

Stevens, Yuan, and Ana Brandusescu. *"Weak Privacy, Weak Procurement: The State of Facial Recognition in Canada."* Centre for Media, Technology & Democracy, 6 Apr. 2021, https://www.mediatechdemocracy.com/all-work/weak-privacy-weak-procurement-the-state-of-facial-recognition-in-canada.

Lange, Christian. "The Nobel Peace Prize 1921 – Nobel Lecture." *The Nobel Peace Prize*, NobelPrize.org, https://www.nobelprize.org/prizes/peace/1921/lange/lecture/.

Innovation, Science and Economic Development Canada. *"Bill Summary: Digital Charter Implementation Act, 2020."* Government of Canada, https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020.

Office of the Privacy Commissioner of Canada. *"Protecting Privacy in a Digital Age."* Speech/Statement, 27 Nov. 2023, https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/sp-d_20231127/.

Innovation, Science and Economic Development Canada. *"Consumer Privacy Protection Act (CPPA)."* Government of Canada, https://ised-isde.canada.ca/site/innovation-better-canada/en/consumer-privacy-protection-act

"Privacy." *Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Stanford University, 19 Oct. 2023, https://plato.stanford.edu/entries/privacy/.

"Internet Research Ethics." *Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Stanford University, 13 July 2025, https://plato.stanford.edu/entries/ethics-internet-research/.

"Privacy." *Routledge Encyclopedia of Philosophy*, Taylor & Francis, https://www.rep.routledge.com/articles/thematic/privacy/v-1.

Office of the Privacy Commissioner of Canada. *"OPC Investigation into the RCMP's Use of Facial Recognition Technology."* 16 Aug. 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170816_rcmp/.

"Surveillance Ethics." *Internet Encyclopedia of Philosophy*, http://iep.utm.edu/surv-eth/.

Bélanger, France, and Robert E. Crossler. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly*, vol. 35, no. 4, 2011, pp. 1017–41. *JSTOR*, https://doi.org/10.2307/41409971. Accessed 27 Oct. 2025.

Reynolds, Osborne M. *Administrative Law Review*, vol. 22, no. 1, 1969, pp. 101–06. *JSTOR*, http://www.jstor.org/stable/40708684. Accessed 27 Oct. 2025.

"Sidewalk Toronto: The Vision Behind Google's Failed City." *Tomorrow.city*, https://www.tomorrow.city/sidewalk-toronto-the-vision-behind-googles-failed-city/.

"RCMP Used Facial-Recognition Tech Without Proper Legal Safeguards, Documents Show." *CBC News*, https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5479673

HR Law Canada. "Federal Court Strikes RCMP Class Action over Alleged Privacy Breach." *HR Law Canada*, 12 May 2025, https://hrlawcanada.com/2025/05/federal-court-strikes-rcmp-class-action-over-alleged-privacy-breach/