VIRTUAL ECHO CHAMBERS – REGULATION FOR FUTURE PRIVACY INTERESTS IN CANADA

By: Harman Singh

<u>*Abstract:*</u>

This paper will critically examine the phenomenon of digital echo chambers as a structural harm emerging from algorithmic profiling and personalization practices, with a focus on Canadian privacy laws. Drawing upon the work of scholars such as Ignacio Cofone, Sandra Wachter, and Brent Mittelstadt, the paper argues that privacy in the digital era is not merely a matter of data control, but one of informational autonomy and democratic resilience. Algorithmic curation as rooted in opaque inferential logics, construct and reinforces online environments that isolate users within ideologically homogenous content, eroding their capacity for independent thought process. Echo chambers not only shape individual behavior but also amplify polarization and exclusion thus posing a direct threat to cohesion and discourse.

The paper conducts a comparative analysis of existing legal frameworks, specifically the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Privacy Act, revealing shortcomings in addressing algorithmically induced harms. PIPEDA's consent-based architecture fails to account for inferential data and curatorial logic, while the Privacy Act's focus on state use of information overlooks the democratic implications of public-sector content personalization. Drawing lessons from Article 22 GDPR, which provides procedural safeguards against automated decision-making, the paper proposes a dual-track regulatory approach. This model calls for strengthening individual rights over inferences while enabling state intervention in cases of algorithmic manipulation that threaten national security, social harmony, election integrity or sovereignty of the nation as a whole.

Ultimately, this paper advocates for a redefinition of privacy as civic and constitutional condition, which is integral not only for personal liberty but also to safeguarding Canada's multicultural democracy. In doing so, it calls for an evolution in privacy governance from individualistic data rights to structurally attuned frameworks that address the informational architectures shaping a collective life in the age of AI.

Keywords: Algorithmic Profiling, Echo Chambers, Canadian Privacy Law, Inferential Harm, Democratic Integrity

1. INTRODUCTION

Privacy is no longer a matter of secrecy or control, but of autonomy and power. As Cofone argues in *The Privacy Fallacy*, contemporary privacy harms are often indirect, systemic, and structurally embedded within algorithmic infrastructures that escape traditional legal scrutiny. These harms do not arise from isolated data breaches or overt surveillance anymore, but also from the subtle manipulation of informational environments where algorithms, curated content, and profiling techniques jointly distort user agency. Echo chambers are among the most insidious outcomes of this architecture, built not by coercion but by design[1].

Information, opinions, and beliefs that reinforce a person's existing views with little or no exposure to contradictory perspectives often end up creating information cocoons (well known as echo chambers). Echo chambers result from the intentional or algorithmic curation of content that aligns with users' preferences, leading to informational isolation. Cass Sunstein emphasized that echo chambers are problematic not merely because they limit diversity, but because they intensify group

[1] Ignacio N Cofone, *The Privacy Fallacy: Harm and Power in the Information Economy* (Cambridge: Cambridge University Press, 2024), ch 6, "Pervasive Data Harms"

polarization, a process whereby members of a like-minded group tend to adopt more extreme positions after discussing an issue. This becomes particularly dangerous in democratic contexts, where disagreement and diversity of opinion are essential to the deliberative process. In such chambers, people become less tolerant of dissent, more certain of their own righteousness, and more suspicious of outsiders.[2]

When combined with algorithmic profiling based on attributes like race, religion, gender, or political orientation, echo chambers can give rise to digital segregation, a condition in which individuals matching any of the pre mentioned descriptive profile are systematically presented with personalized content, including news, ads, and opportunities, that entrenches and perpetuates existing social inequalities. For example, a teenager living in a lower-middle-class immigrant neighborhood who regularly interacts with content portraying other racial groups negatively may be algorithmically grouped into a profile that receives more and more hateful material while being excluded from educational or developmental resources, thereby amplifying a preexisting disparity and bias at the same time. Likewise, men while scrolling passively are targeted with a steady stream of misogynistic content, while women are algorithmically nudged toward self-validating material under the guise of empowerment, such as Instagram reels promoting curated ideals of self-love- both reinforcing limiting and often harmful gender norms.

Similarly, Wachter and Mittelstadt, in *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*[3], highlight that algorithmic inferences produced by opaque AI systems expose a major loophole in even the most advanced data protection frameworks

[2] Cass R Sunstein, *Republic: Divided Democracy in the Age of Social Media* (Princeton: Princeton University Press, 2017) at 5 [*Daily Me*, ch 1]

[3] Sandra Wachter & Brent Mittelstadt, “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI” (2019) 2019:2 *Colum Bus L Rev* 494 at 506–513

worldwide. Meanwhile Article 22 of the GDPR (considered to be one of the best data protection laws worldwide) protects individuals from harm caused by fully automated decision-making, this protection is also limited to decisions that produce legal effects or similarly significant consequences with caveats to the protection offered being enshrined in the Paragraph 2 of the Article itself[4]. As such, the autonomy-eroding impact of echo chambers often falls outside its scope. Profiling systems, the authors argue, are inherently curatorial i.e., they can create internal representations of individuals based on metadata, behavioral patterns, and associations, and use these profiles to influence future actions. In echo chambers, such inferences become self-fulfilling prophecies, reinforcing pre-existing biases and trapping individuals in digitally constructed realities. This idea of Echo chamber is further verified by Meta's own disclosures as mandated under Principle 2 of PIPEDA ("Identifying Purpose"), which outline how user data is collected and utilized to shape content delivery in Canada. Meta states that decisions about what to display to users are based on various types of information, including[5]:

- User profile details,
- Activity both within and outside Meta's platforms
- Content users engage with or produce
- Inferences drawn about user interests
- Data related to friends, followers, and other connections

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, [2016] OJ, L 119/1 [General Data Protection Regulation], art 22(1): "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

[5] Meta Platforms, Inc, *Facebook Privacy Policy: How We Show Ads* (2024), online: Facebook https://www.facebook.com/privacy/policy?subpage=2.subpage.2-HowWeShowAds

Thus, curating information that aligns with inferred preferences, thereby shape a users' online experiences and perspectives at the end of the day.

This intersection of algorithmic inferences and curatorial logic brings to light the inadequacies of traditional privacy laws in addressing the structural harms caused by digital echo chambers. In Canada, the current regulatory frameworks PIPEDA and Privacy Act, have yet to fully grapple with the normative and epistemic consequences of algorithmic environments. These laws continue to conceptualize privacy primarily in terms of individual consent and data collection, with insufficient attention to the collective harms of information curation and automated inference. The rising use of AI tools to personalize not only content but also behavior and thought challenges the existing three-part test (reasonable expectation of privacy, threshold of harm, and proportionality of interference) demanding a redefinition of privacy itself not as a static right to seclusion, but as a dynamic condition for democratic agency and informed self-determination. Moving forward, the paper will examine the limitations of Canadian data protection laws in the context of algorithmically reinforced echo chambers, while proposing a regulatory model that foregrounds autonomy and civic resilience in the AI-driven public sphere.

2. PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA), which was enacted to regulate the private sector's use of personal information in commercial activities is premised on the principles of meaningful consent and transparency. Yet, as digital environments evolved due to embed artificial intelligence (AI) and algorithmic decision-making, the Act's underlying assumptions particularly the individualistic model of privacy and the procedural notion of consent have been increasingly tested. Nowhere is this tension more evident than in the context of algorithmically reinforced echo chambers, where personal data are not merely collected and used, but transformed into inferred profiles that shape individuals' digital realities. These realities are predictive and manipulative, yet they often evade regulatory oversight due to the non-tangible nature of the harm.

PIPEDA still continues to rest on the idea that privacy protection is primarily secured through informed consent. However, this model collapsed in the face of AI systems that operate on massive, opaque datasets and draw complex inferences beyond user comprehension.[6] AI systems infer personality traits, political affiliations, emotional states, and moreover all this without explicit disclosure or consent to do the same. Users are thus exposed to personalized experiences that subtly reinforce prior beliefs, trap them within echo chambers, and narrow the range of ideas and discourses they are exposed to.

PIPEDA's focus on the collection of identifiable personal information fails to account for inferential data that are predictive and relational in nature ignoring the collective implications of algorithmic curation, which affect not just individuals but also the public sphere itself. Although, the right to access one's personal information and to know how it is being used is recognized under Section 8 of PIPEDA, yet this right falls short of ensuring algorithmic transparency. As Kirsten R. Goodwin argues, Canadian privacy law does not yet provide for a robust right to explanation comparable and falls short even to Article 22 of the GDPR.[7] In the case of automated decision-making that does not produce "significant legal effects," PIPEDA does not guarantee that individuals are told why they were targeted with specific content or how their behavioral data

[6] Teresa Scassa, "Privacy Law and Artificial Intelligence: Through an Equity Lens" (2021) 20:1 *Can JL & Tech* 1 at 12–13

[7] Kirsten R Goodwin, "Algorithmic Decision-Making and the Right to Explanation" (2018) 55:2 *Ottawa L Rev* 263 at 278–81

contributed to the personalization process. This regulatory shortfall is particularly concerning in the context of echo chambers, where individuals are often unaware that their information environment is being shaped by inferred traits in absence of a legal mechanism to demand meaningful explanations of algorithmic inferences and content delivery logic.

In his critique of Canadian privacy law, Michael Geist also emphasized that PIPEDA's consent-based model is outdated, especially in contexts involving automated decision-making. The proposed Consumer Privacy Protection Act (CPPA) under Bill C-27[8] aims to update PIPEDA by introducing rights to mobility, algorithmic transparency, and stronger enforcement mechanisms, but even this proposal was criticized for failing to impose duties regarding collective and contextual harms like content induced radicalization.

Moreover, PIPEDA currently does not address the responsibility of Big Tech platforms to design against manipulation or promote epistemic diversity. It treats users as data subjects and not as civic agents, capable of contributing to and shaping public discourse. This perspective is essential if privacy is to be understood not just as a shield from harm, but as a condition for democratic self-determination. In sum, although PIPEDA may have served as a foundational privacy statute for private sector in Canada but was ill-prepared for the algorithmic age, particularly in regulating environments that engineer echo chambers through automated profiling and inference. The statute's reliance on consent, lack of enforceable explanation rights, and narrow focus on identifiable information leave individuals and democratic institutions vulnerable to curatorial manipulation.

[8] Currently under review before Standing Committee on Industry and Technology, House of Commons.

To counteract the epistemic harms of algorithmic profiling and echo chambers, Sandra Wachter and Brent Mittelstadt proposed a right to reasonable inferences, arguing that privacy laws must extend beyond the collection of data to include the logic by which that data is interpreted and deployed.[9] They argue that individuals should have the legal ability to challenge harmful inferences, especially when they are used to shape opportunities, content exposure, and social perception, all of which are central to the formation of echo chambers. PIPEDA, however, lacks such safeguards, as it does not recognize inference as a distinct site of harm.

In contrast, Article 22 of the GDPR placed at a better pedestal than PIPEDA offers a more rights-based model by prohibiting individuals from being subject to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects.[10] Crucially, paragraph 3 of Article 22 mandates the right to human intervention in such cases, ensuring that users can contest decisions made by algorithms and request explanations. Even more significantly, paragraph 4 provides that such automated processing must include measures to safeguard data subjects' rights, freedoms, and legitimate interests, including mechanisms to reduce bias and discrimination on the basis of identity. By embedding accountability into the design and execution of profiling systems, Article 22 may serve as a template. Adopting similar provisions can be beneficial to mitigate the personalization feedback loops that trap individuals in echo chambers, restoring social media more of as an informational agency and humans as decision makers on the basis of the information presented with their free will and understanding.

[9] Wachter, supra note 3 at 531

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data [2016] OJ, L 119/1 at art 22(1) [GDPR]

3. Privacy Act

Privacy Act, a quasi-constitutional statute, governs the collection, use, disclosure, retention, and protection of personal information by federal public bodies. As government services continue to digitize, this shift offers significant potential for enhancing how Canadians interact with state institutions thus creating a more efficient, coordinated, and responsive public service delivery in a welfare state. According to Department of Justice[11], one key rationale behind such data collection is to gain "a better sense of public needs," thereby enabling more informed decision-making and tailored services. However, this very logic that data is to be used to curate public interactions raises important questions about whether such personalization might contribute to echo chamber-like effects within the public sector. In this context, the state-driven curation of services could fall within the broader scope of echo chamber regulation, warranting enhanced privacy safeguards to ensure democratic neutrality, diversity of access, and the protection of informational autonomy, all this while state fulfilling its welfare duties.

In light of these shortcomings, it is imperative that Canada adopts a government-led approach to regulating algorithmic echo chambers, one that places the sovereign interest of the nation and the safety of its citizens at the forefront. While models like the GDPR may offer valuable insights especially in terms of individual rights protections, algorithmic transparency, and bias mitigation mechanisms under Article 22 but they must not be transplanted wholesale into the Canadian legal context. Instead, they should serve as lessons for reform, adapted to Canada's unique legal, political, multicultural and democratic culture.

[11] Canada, Department of Justice, *Modernizing Canada's Privacy Act: Consultation Paper* (Ottawa: Department of Justice, 2021) at 3

The recent Consultation Paper on the Modernization of Canada's Privacy Act explicitly recognized that digital technologies present risks beyond individual privacy, including national security, law enforcement, and democratic integrity.[12] The paper acknowledged that information privacy today intersects with public safety, noting that a modernized framework must enable data use "for law enforcement, national security, and regulatory purposes" while upholding public trust.[13] This acknowledgement offers a legislative foundation to regulate algorithmic profiling not merely for its impact on consent or data protection but for its broader implications on social cohesion, extremism, and public order, the issues deeply implicated in the rise of digital echo chambers. A growing body of international and domestic evidence shows that profiling and curatorial content can escalate social unrest in domestic jurisdictions for Canada. For instance, platforms operating in Canada have been used to amplify foreign narratives, polarizing communities and enabling digital radicalization through recommendation engines that reward engagement over truth.

An illustrative case of narrative distortion emerged following the 2024 Brampton Temple incident[14], where Indian national media and political figures from the ruling Indian establishment characterized the event primarily as a religiously motivated attack meanwhile disregarding its more accurate framing as a localized conflict between two Canada based groups. This reductive portrayal, disseminated widely through both traditional media and digital platforms, inflamed communal sentiments and misrepresented the Canadian socio-political context, by prioritizing a singular communal lens over the complexity of domestic dynamics. Such external narratives, when

[12] Ibid at 5

[13] Ibid at 14

[14] CBC News, "3 Men Charged After Violent Protests Outside GTA Hindu Temple, Sikh Gurdwara," *CBC News* (3 November 2024), online: https://www.cbc.ca/news/canada/toronto/temple-brampton-alleged-violent-altercation-protest-peel-police-1.7372541; Anirudh Bhattacharyya, "Organiser of Khalistani Protest That Attacked Hindus at Canada Temple Arrested," *Hindustan Times* (10 November 2024), online: https://www.hindustantimes.com/india-news/canada-hindu-temple-attack-fresh-arrest-made-amid-fear-of-more-clashes-101731207882567.html.

reinforced through algorithmic amplification, contributed to the erosion of social cohesion and deepened divisions within Canada's multicultural society. This episode underscores the vulnerability of Canadian public discourse to foreign-curated, polarized content, and the urgent need for regulatory frameworks that protect informational integrity in a globally networked environment. In this regard, echo chambers do not merely affect cognitive diversity or autonomy, rather, they pose a direct challenge to the state's responsibility to maintain peace and democratic legitimacy. Canada could reimagine privacy regulation not just as a means of protecting individuals, but as a strategic instrument of governance in such cases. Echo chambers, fueled by profiling must be treated as infrastructure with potential national consequences and not simply private sector missteps. This would empower the state to restrict algorithmic personalization that demonstrably contributes to polarization or the erosion of public trust in democratic institutions.

To achieve this, the Privacy Act could be modernized to include clear provisions that authorize proactive content governance, particularly in cases involving threats to national security, inter-ethnic harmony, or election integrity. While the Consultation Paper hesitated to define the precise boundaries of algorithmic regulation, it opens the door to such reforms by proposing a broader definition of personal information that includes inferred and relational data.[15] This shift could also allow regulators to move beyond traditional consent-based models toward a risk-based accountability framework, which aligns more closely with Canadian constitutional values than a blind adoption of GDPR-like mechanisms.

Moreover, by emphasizing the public interest as a guiding principle in the use and disclosure of personal information,[16] the Canadian model could be future-proofed against both domestic

[15] Ibid, Pg 11–13
[16] Ibid 7

manipulation and foreign influence operations. This aligns with the Charter obligation under Section 7 to protect the life, liberty, and security of the person, interests that are deeply entwined with digital autonomy in today's world.[17]

In conclusion, the Canadian state must act not merely as a referee between users and platforms, but as a sovereign actor, as far as protecting democratic values and ensuring public order is concerned. GDPR's Article 22 and similar models offer procedural tools worth integrating, particularly the guarantee of human intervention and safeguards against algorithmic bias. However, their adoption must be filtered through the lens of Canadian sovereignty, emphasizing contextual adaptation rather than normative transplant. In a fractured multipolar world, with rising geopolitical tensions and information warfare, the regulation of data curation and echo chambers must be driven not only just by individual rights, but also by the imperatives of nationhood, public safety, and democratic integrity.

4. Conclusion

The growing entrenchment of echo chambers within Canada's digital lives illustrates that privacy is no longer merely about control over personal information, but a structural condition shaping democratic participation and national cohesion. While much attention has rightly been placed on private-sector regulation through PIPEDA and forthcoming reforms under the CPPA, the public sector requires a categorically distinct regulatory approach. The Privacy Act, unlike its private counterpart, governs state-held data and thus intersects directly with sovereign responsibilities

[17] Canadian Charter of Rights and Freedoms, s 7, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11

including national security, law enforcement, and public trust. Treating both domains under a singular or harmonized privacy model would be conceptually flawed and strategically naive.

As this paper has demonstrated, public institutions not only manage data but increasingly curate services, communication, and even citizen-state interactions using the same data. This practice of curation by state, while administratively efficient, risks inadvertently reproducing the same algorithmic biases and echo chamber effects attributed to corporate platforms. However, public-sector data use carries broader implications not just for individual autonomy but for the legitimacy of state action itself for protection of sovereign interests and performance of welfare duties it is bound to uphold.

The Consultation Paper on the Modernization of the Privacy Act rightly emphasized the need to balance data innovation with democratic safeguards, advocating a risk-based accountability framework rather than consent-centric models typical of private-sector regulation. International models like the GDPR, while helpful in conceptualizing algorithmic accountability, cannot be adopted wholesale in Canada. Instead, Canadian privacy governance must prioritize sovereignty, constitutional rights (notably section 7 of the Charter), and multicultural cohesion, especially in light of foreign influence campaigns and manipulated narratives as evidenced by the Brampton Temple incident and its communal misrepresentation.

Ultimately, echo chambers in the public sector are not merely a matter of information, rather, they constitute a democratic and constitutional challenge, given their impact on public discourse and the amplification of biases that may already exist in historical data, shaping the narratives, services, and decisions. A reformed Privacy Act must acknowledge this duality and move beyond informational silos towards an integrated yet differentiated governance model, the one that reinforces Canada's unique constitutional culture and fortifies its democratic future.