Algorithmic Harm and Justice: Evaluating the Algorithmic Ecology Toolkit through CARE and Indigenous Sovereignty

Miranda G Woodland

Athabasca University

MAIS752: Critical Computations

Michael Lithgow

November 11, 2024

Algorithmic Harm and Justice: Evaluating the Algorithmic Ecology Toolkit through CARE and Indigenous Sovereignty

In June 2024, Georgia State University assistant professor of law, Jeffrey L. Vagle, and deputy director of the American Civil Liberties Union's National Security Project, Patrick Toomey, were interviewed by *Wired Magazine* and expressed concerns over the potential misuse of surveillance powers under a second Trump administration, suggesting that national security could be used as a loophole to justify invasive monitoring (Benson, 2024). The *Wired* article highlights the possibility of increased government surveillance on political opponents, activists, and marginalized communities to suppress free expression and privacy rights. Within weeks of the article, the International Association of Privacy Professionals published an article explaining why it is unlikely that Canada will make amendments to its privacy laws before the 2025 Federal Election (LaCasse, 2024). This raises concerns about the likelihood that Canada will follow the United States' lead in terms of moving politically right and whether similar surveillance concerns will arise given the lack of transparency of current surveillance and no additional legislation for the foreseeable future.

Using the example of the Royal Canadian Mounted Police's (RCMP) use of Clearview AI facial recognition technology, this paper considers surveillance concerns through the lens of the Algorithmic Ecology Tool, arguing that while the tool is effective in promoting community resistance to algorithmic systems, it requires enhancement in addressing Indigenous data sovereignty and further integration of the CARE principles to achieve a more inclusive and equitable data governance framework.

Background: The Algorithmic Ecology Tool

The Algorithmic Ecology Tool is a framework and organizing tool developed by the Stop LAPD Spying Coalition to analyze and resist harmful policing algorithms, particularly focusing on the predictive policing technology PredPol (Stop LAPD Spying Coalition and Free Radicals, 2020). It emphasizes understanding the multiple actors and ideologies behind algorithms rather than viewing them in isolation, and highlights the intersection of race, poverty, and policing in marginalized communities. The

framework is designed to decentre the algorithm itself and instead focuses on the various actors involved in its development, implementation, and impact (2020).

By way of example, I will apply the Algorithmic Ecology Toolkit to the RCMP's use of Clearview AI, a facial recognition system that has faced criticism for its privacy violations and potential for misuse (Office of the Privacy Commissioner of Canada *et al.*, 2021; Kelly, 2022). The toolkit not only deconstructs the RCMP's reliance on FRT but also identifies opportunities for community resistance and policy reform. While not as artistic as the template provided by Free Radicals (see Appendix), Table 1 provides an overview of the key considerations emphasized by the toolkit.

Table 1 Application of the Algorithmic Ecology Toolkit using the findings from the Privacy Commissioner of Canada and the Standing Committee on Access to Information, Privacy and Ethics regarding the RCMP's use of Facial Recognition Technology.

LAYER	KEY QUESTIONS	FINDINGS
COMMUNITY IMPACT	• Who is targeted, and how does FRT impact them? • What harms or risks arise?	○ Disproportionate surveillance of marginalized groups, including Indigenous and racialized communities. ○ Risk of false positives, wrongful identification, and reputational damage.
OPERATIONALIZATION	• How are RCMP operations structured around FRT? • What data sources are used?	○ Use of Clearview AI's database, which collects images without consent. ○ Limited transparency in deployment and monitoring of FRT.
INSTITUTIONAL ROLE	• Which institutions support or regulate this technology? • How does RCMP comply with legal frameworks?	○ RCMP's practices conflict with privacy laws (PIPEDA), failing to ensure consent for data use. ○ Insufficient oversight mechanisms.
IDEOLOGICAL UNDERPINNINGS	• What narratives justify FRT? • How does this align with societal goals?	○ FRT framed as essential for public safety and crime prevention, reflecting a trend of technological solutionism.

		○ Reinforces power imbalances under the guise of security.
OPPORTUNITIES FOR RESISTANCE	• How can communities and policymakers respond?	○ Increased transparency through public disclosures. ○ Community involvement in decision-making. ○ Regulatory reforms, including moratoriums and stricter oversight.

In this case, I was able to use the findings of the two privacy reports (Office of the Privacy Commissioner of Canada *et al.*, 2021; Kelly, 2022), creating a retrospective rather than proactive analysis. However, this example serves as a practical illustration of the toolkit's potential to empower marginalized communities and foster accountability in the deployment of surveillance technologies.

Evaluation of The Algorithmic Ecology Toolkit Based on CARE Principles

The CARE principles, developed by the International Indigenous Data Sovereignty Interest Group, complement the FAIR data principles, which focus on making data Findable, Accessible, Interoperable, and Reusable. However, "The FAIR principles do not mention or address the specific concerns of Indigenous Peoples in relation to Indigenous Data" (Walter *et al.*, 2021, p. 151) such as the historical and ongoing power imbalances related to data collection, use, and ownership.

On the other hand, the CARE Principles are grounded in Indigenous worldviews and aim to empower Indigenous Peoples by ensuring they have control over their data: "Indigenous data governance refers to formal mechanisms, which can assert Indigenous data interests in relation to the when, how and why of how data are accessed and used, ensuring Indigenous data practices reflect Indigenous priorities, values, culture, and diversity" (Walter *et al.*, 2021, p. 150). These mechanisms are meant to guide external stakeholders in their interactions with Indigenous data and to promote ethical and responsible data practices.

The Algorithmic Ecology Toolkit shares common ground with the CARE Principles by emphasizing community empowerment, challenging power imbalances, and seeking to minimize the

harm caused by algorithms. However, the toolkit's primary focus is on resistance and dismantling existing systems (Brand and Sander, 2020), while the CARE principles encourage a broader approach that includes promoting collective benefits, Indigenous data sovereignty, and responsible data practices.

The Toolkit underscores the imperative of identifying and addressing the detrimental impacts of algorithms on marginalized communities, resonating with the principle of collective benefit. This principle involves "ensuring data use leads to equitable outcomes, improved governance, and inclusive development for Indigenous communities" (Walter et al., 2021, p. 152). By mapping the network of actors and interests within an algorithm's ecosystem, the toolkit enables communities to advocate for more equitable outcomes. While its primary focus remains on resisting and dismantling harmful systems, the toolkit does not explicitly prioritize fostering innovation or promoting positive development within these ecosystems.

In providing communities with the means to understand and challenge algorithmic influences, the toolkit enhances their authority to control data usage and decision-making processes. This empowerment supports greater autonomy over how data is applied in contexts that directly impact their lives. However, it does not extend to addressing broader issues of data ownership or suggesting new governance structures. Its focus remains on disrupting existing systems rather than proposing comprehensive frameworks for alternative, community-led governance models.

The toolkit also draws attention to the responsibility of various stakeholders - funders, developers, and implementers - who play pivotal roles in shaping algorithmic systems. This approach encourages users to interrogate the power dynamics and ideological biases underpinning these technologies, fostering a critical reflection on ethical obligations. As Walter et al. (2021) argue, "There needs to be the joint development of principles and protocols around the governance and stewardship of Indigenous data that are formally applicable to those who currently hold those data and those who would choose to analyse it" (p. 149). Yet, despite this recognition, the toolkit offers limited guidance on building positive relationships with communities or enhancing their data capabilities, which could further empower marginalized groups.

Rooted in an abolitionist framework, the toolkit places ethical considerations at the forefront, emphasizing the need to minimize harm caused by algorithmic systems. By exposing the vested interests and ideologies embedded within these technologies, it challenges prevailing narratives of technological objectivity and neutrality. This ethical stance not only underscores the moral imperative to resist and dismantle harmful systems but also highlights the responsibility to confront injustices perpetuated by algorithmic processes.

The Algorithmic Ecology Toolkit and the Principles of Fairness, Safety, and Diversity

The principles of fairness, safety, and diversity intersect with the CARE Principles by providing complementary frameworks for evaluating and improving data systems. Both sets of principles aim to address power imbalances and promote justice but focus on different aspects of the data ecosystem.

The principle of fairness emphasizes the need for data systems to treat all individuals equitably, avoiding biases and discriminatory practices that could disproportionately impact marginalized communities. This notion of fairness aligns closely with the CARE principle of collective benefit, which argues that the advantages of data systems should be accessible to entire communities rather than privileged groups alone. As Krupiy (2020) observes, “The attention on how to embed fairness into the decision-making procedure of a technical system side-lines the discussion of how the employment of AI decision-making processes impacts on achieving social goals” (Krupiy, 2020, p. 2). For instance, AI-driven policing tools, such as facial recognition, demand fairness in avoiding the undue targeting of marginalized groups, while collective benefit further emphasizes equitable distribution, ensuring that historically marginalized groups also derive value from these systems. Together, these principles advocate for data practices that actively challenge systemic inequalities, fostering a more just society.

Safety, in this context, involves minimizing risks and harms associated with data systems, thereby protecting communities from misuse or exploitation. This focus on safety is intrinsically linked to the concept of authority to control, which advocates for communities having the ability “to determine the means of collection, access, analysis, interpretation, management, dissemination and re-use of data pertaining to the Indigenous Peoples from whom it has been derived, or to whom it relates” (Walter *et al.*,

2021, p. 146). The deployment of Clearview AI by the RCMP exemplifies safety concerns, especially for Indigenous and racialized communities disproportionately affected by surveillance. According to the Office of the Privacy Commissioner of Canada et al. (2021), "The mass collection of images and creation of biometric facial recognition arrays by Clearview... represents the mass identification and surveillance of individuals by a private entity... creating the risk of significant harm to those individuals, the vast majority of whom have never been and will never be implicated in a crime" (Office of the Privacy Commissioner of Canada *et al.*, 2021, p. 2). By asserting authority over their data, communities could challenge harmful practices and reduce exposure to potential harm, as both safety and authority to control advocate for governance mechanisms that empower communities to protect their data and well-being.

Diversity, which calls for the inclusion of varied perspectives—especially those of marginalized communities—ensures that data systems accurately reflect the complexity of human experiences. This principle complements the CARE principle of responsibility, emphasizing the ethical obligations of those involved in designing, funding, and implementing data systems. Ensuring diverse input in data tool development fosters cultural sensitivity and inclusivity. Mohamed, Png, and Isaac (2020) assert that "AI must actively seek diverse epistemologies and prioritize the perspectives of historically marginalized groups... necessitating a multiplicity of intellectual frameworks to ensure AI aligns with ethical imperatives, centering those most affected by its deployment" (Mohamed, Png and Isaac, 2020, p. 660). The RCMP's use of facial recognition technologies, for example, frequently overlooks the lived experiences of marginalized groups, exacerbating existing inequalities. The principle of responsibility within the CARE framework reinforces the importance of including diverse voices at the heart of data system design and governance, thereby fostering accountability and trust.

Both the CARE principle of ethics and the ethical considerations inherent in fairness, safety, and diversity stress the importance of prioritizing human dignity and justice within data systems. Stark et al. (2021) argue that "The governance of AI systems, particularly through values statements and high-level principles, tends to focus on transparency and technical fixes but often lacks a deeper engagement with the political economy and ethical obligations of justice" (Stark, Greene and Hoffmann, 2021, p. 263). The

frameworks discussed herein challenge the frequently unquestioned narratives of neutrality and objectivity in technology. For instance, the RCMP's reliance on Clearview AI embeds specific values that prioritize state security over individual rights. Ethical scrutiny reveals these biases, advocating for systems that are not only transparent but also just and equitable. Embedding ethical considerations at every stage of development enables data systems to resist perpetuating harm and instead serve as tools that contribute to societal well-being.

Integrating Indigenous Data Sovereignty into the Algorithmic Ecology Toolkit

Currently, the Algorithmic Ecology Toolkit provides a powerful framework for deconstructing the harm caused by algorithmic systems and identifying opportunities for resistance. However, it has limited engagement with Indigenous worldviews and data practices, leaving significant gaps in its ability to address unique challenges faced by Indigenous communities. Indigenous Data Sovereignty (IDS) frameworks offer a way to bridge these gaps by emphasizing the control, governance, and application of data in ways that respect Indigenous self-determination and cultural values (Walter *et al.*, 2021). Incorporating IDS into the toolkit would enhance its capacity to account for the historical and ongoing impacts of colonialism embedded in algorithmic systems and provide a more comprehensive roadmap for dismantling these harms.

Indigenous Data Sovereignty frameworks highlight the importance of collective rights over data, challenging the dominant individual-centric paradigms of data governance (Walter *et al.*, 2021, p. 145). Integrating IDS into the Algorithmic Ecology Toolkit would involve not only analyzing how algorithms impact Indigenous communities, but also ensuring that data collection, storage, and analysis are governed by Indigenous protocols. This could prevent exploitative practices and ensure that data-driven technologies respect Indigenous sovereignty and contribute to community well-being (Walter, 2021).

Moreover, Indigenous Protocols for AI, such as those outlined by Lewis (2020), provide practical guidelines for embedding Indigenous knowledge systems into technological design. These protocols advocate the development of AI systems that align with Indigenous principles, including relationality, reciprocity, and respect for the land (Lewis, 2020). By adopting these protocols, the Algorithmic Ecology

Toolkit can extend its analysis beyond resisting harm to include the proactive design of algorithmic systems that uphold Indigenous epistemologies. This shift would enable the toolkit to not only dismantle harmful systems, but also promote the creation of technologies that support Indigenous resilience and cultural revitalization.

It is important to note that neither privacy report referenced in this paper included representatives from Indigenous communities in their consultations while at the same time it is noted that "For domestic law enforcement images, the highest false positive rates were for Indigenous peoples" (Kelly, 2022, p. 14). By incorporating Indigenous Data Sovereignty, the Algorithmic Ecology Toolkit could evolve into a more holistic framework that not only critiques existing systems, but also supports the development of alternative, community-driven technologies. This integration would ensure that the toolkit remains relevant and effective in addressing the complex challenges of algorithmic harm, particularly in the context of Indigenous communities' struggles for data justice and sovereignty.

Conclusion

This paper has demonstrated the utility and limitations of the Algorithmic Ecology Toolkit in evaluating the Royal Canadian Mounted Police's (RCMP) use of facial recognition technology. While the toolkit offers a powerful framework for resisting harmful algorithmic systems, it requires further integration of CARE principles and Indigenous Data Sovereignty frameworks to achieve its full potential in a Canadian context.

As Canada is facing increasing pressure to address privacy and surveillance concerns, the importance of integrating community-driven frameworks into data governance has become increasingly urgent. By incorporating Indigenous knowledge systems and governance practices, the Algorithmic Ecology Toolkit could move beyond critiquing harmful technologies to actively shaping equitable and culturally respectful data ecosystems. This evolution is crucial not only for safeguarding the rights of marginalized communities but also for fostering a broader societal commitment to justice and accountability in the digital age.

References

Benson, T. (2024) 'How Donald Trump Could Weaponize US Surveillance in a Second Term', *Wired*, 3 June. Available at: https://www.wired.com/story/trump-second-term-surveillance-state/.

Brand, J. and Sander, I. (2020) 'The Algorithmic Ecology Tool: An Abolitionist Tool for Organising Against Algorithms', in *Critical data literacy tools for advancing data justice: A guidebook*. Digital Justice Lab, p. 6.

Kelly, P. (2022) *FACIAL RECOGNITION TECHNOLOGY AND THE GROWING POWER OF ARTIFICIAL INTELLIGENCE: Report of the Standing Committee on Access to Information, Privacy and Ethics*. House of Commons.

Krupiy, T. (Tanya) (2020) 'A vulnerability analysis: Theorising the impact of artificial intelligence decision-making processes on individuals, society and human diversity from a social justice perspective', *Computer Law & Security Review*, 38, p. 105429. Available at: https://doi.org/10.1016/j.clsr.2020.105429.

LaCasse, A. (2024) *Ahead of 2025 federal election, will Canada pass Bill C-27?*, *International Association of Privacy Professionals*. Available at: https://iapp.org/news/a/ahead-of-2025-federal-election-will-canada-pass-bill-c-27- (Accessed: 9 November 2024).

Lewis, J.E. (ed.) (2020) 'Indigenous Protocol and Artificial Intelligence Position Paper'. Concordia University Library. Available at: https://doi.org/10.11573/SPECTRUM.LIBRARY.CONCORDIA.CA.00986506.

Mohamed, S., Png, M.-T. and Isaac, W. (2020) 'Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence', *Philosophy & Technology*, 33(4), pp. 659–684. Available at: https://doi.org/10.1007/s13347-020-00405-8.

Office of the Privacy Commissioner of Canada *et al.* (2021) *PIPEDA Findings #2021-001: Joint investigation of Clearview AI, Inc.* Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

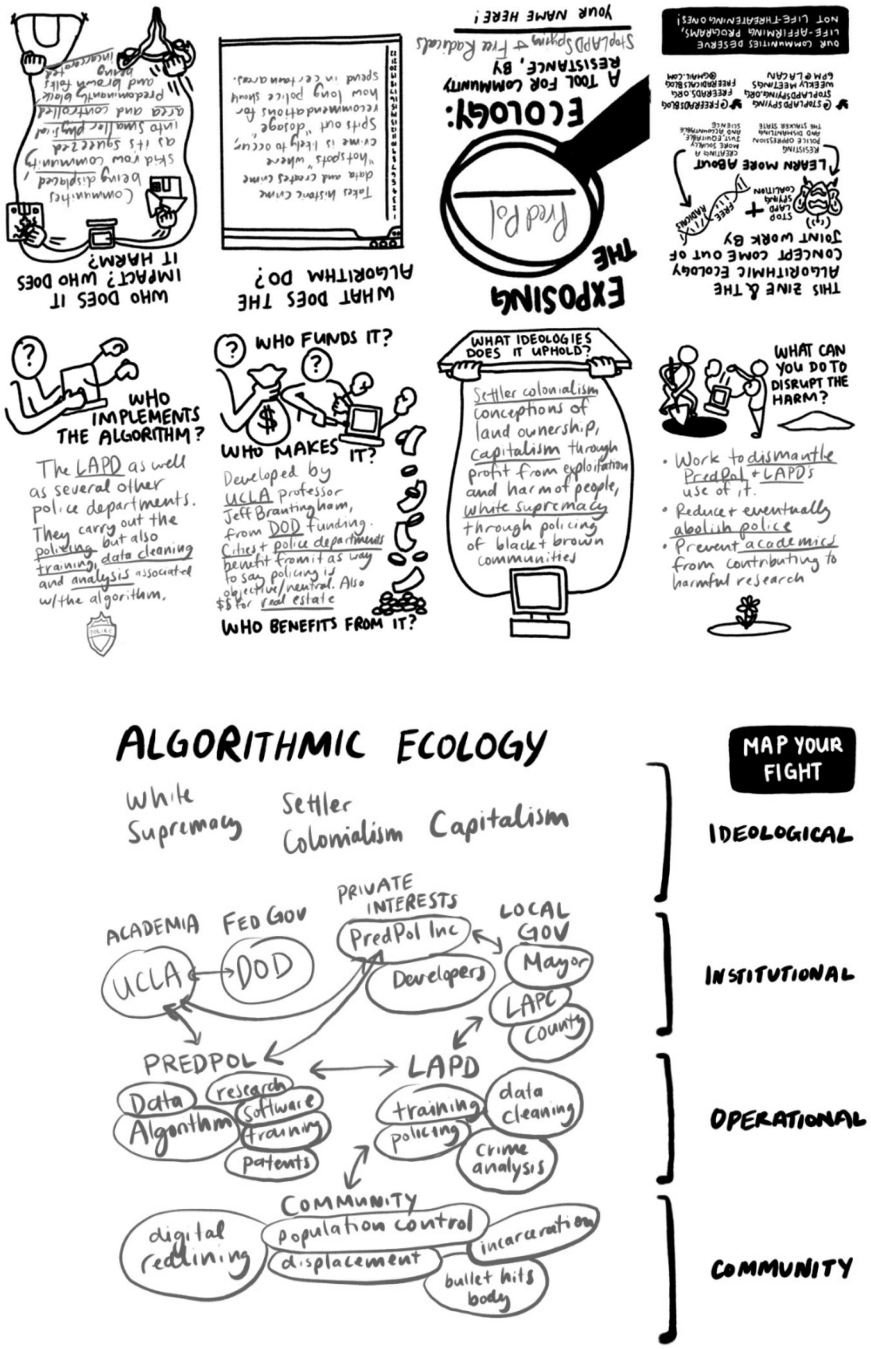
Stark, L., Greene, D. and Hoffmann, A.L. (2021) 'Critical Perspectives on Governance Mechanisms for AI/ML Systems', in J. Roberge and M. Castelle (eds) *The Cultural Life of Machine Learning*. Cham: Springer International Publishing, pp. 257–280. Available at: https://doi.org/10.1007/978-3-030-56286-1_9.

Stop LAPD Spying Coalition and Free Radicals (2020) 'The Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms', *Free Rads*, 2 March. Available at: https://freerads.org/2020/03/02/the-algorithmic-ecology-an-abolitionist-tool-for-organizing-against-algorithms/.

Walter, M. *et al.* (2021) 'Indigenous Data Sovereignty in the Era of Big Data and Open Data', *Australian Journal of Social Issues*, 56(2), pp. 143–156. Available at: https://doi.org/10.1002/ajs4.141.

Appendix

Figure 1 The Algorithmic Ecology Framework using PredPol as an Example. Downloaded from Free Radicals: https://freerads.org/wp-content/uploads/2020/03/AE_Zine_PredPol-2.pdf



(Stop LAPD Spying Coalition and Free Radicals, 2020)