Digital Authoritarianism: A Case for Policy Supporting Data Unions

Carissa Hubbard, Justin Myers and Reagan Roopnarine

Issue

Transnational corporations and authoritarian regimes are exploiting personal data to surveil, harass and control populations worldwide in ways that directly undermine Canada's foreign policy objectives related to prosperity, security, democracy and human rights.

Background

According to a 2022 survey by Statistics Canada, 95 percent of Canadians aged 15 and older use the Internet (Statistics Canada 2023). With nearly the entire Canadian population online, it is paramount that the Canadian government enact policies that protect them in the digital realm. This goal aligns with the mandate of the Minister of Innovation, Science and Industry, who has been tasked with shaping global responses to emerging digital technologies and strengthening privacy protections domestically (Trudeau 2021). However, privacy is only one of the many rights under threat in the current global policy regime; labour rights, property rights and moral rights are also being impinged.

Data collection can be beneficial for users of online platforms as it can spark digital innovation and present specific, relevant information for individuals using the services (Moiso and Minerva 2012). However, the current system disproportionately benefits the companies that collect data, resulting in concerns relating to data privacy, unpaid labour, ownership and sovereignty (Zuboff 2015). This current data model suggests that users' access to and use of services such as Google, Facebook and Amazon are free because of the data that they produce (Arrieta-Ibarra et al. 2018). Under surveillance capitalism, data has become a new form of currency (Moiso and Minerva 2012). Specifically, user data is collected, packaged and then analyzed and sold as "big data" by data brokers to companies interested in targeted advertising (Zuboff 2015). This shift towards big data has transformed the Internet into an advertising "real estate market," as advertisers seek access to the data that will most successfully predict customers' purchasing habits (Papadimitropoulos 2021). This has only compounded with the so-called "Internet of Things" — the ubiquitous collection of data gathered from sources including doorbells, fridges cars and watches, among other devices (Langley et al. 2021). No piece of data is considered inconsequential or irrelevant. For example, web searches, text messages, social media likes and comments, mouse movements and user location are routinely collected (Zuboff 2015). These collection processes remain very opaque to data producers, resulting in concerns that data is being misused, as there are currently very few legitimate mechanisms to control where one's data ends up (ibid.).

The deepening of this system has been exacerbated by an international data sharing regime that for years has operated on the presumption that international transfers of personal data should be considered safe and permitted until proven otherwise (Jurcys, Compagnucci and Fenwick 2022). Based primarily on questions of privacy and corporate rights to data, this regime misses significant issues.

However, in some jurisdictions, data governance and protection of personal information have been rising priorities. Key developments include the European Union's general data protection regulation in 2016, California's

similar California Consumer Privacy Act in 2018 and the Schrems II decision made by the Court of Justice of the European Union in 2022. All are significant steps towards protecting the producers of data, who are often the users of online services.

Canada has followed suit and is looking to implement a number of changes to its data governance regime with Bill C-27, The Digital Charter Implementation Act. This bill aims to repeal and supplement specific sections of the current legal framework protecting personal data, the Personal Information Protection and Electronic Documents Act (PIPEDA). Currently under review by the Standing Committee on Industry and Technology, if Bill C-27 passes, Canadians will see a three-fold update. First, the bill will repeal part one of PIPEDA and replace it with the Consumer Privacy Protection Act. Second, the bill will create a Personal Information and Data Protection Tribunal with the power to impose significant fines for organizations that do not comply with the Consumer Privacy Protection Act. Finally, the bill will enact the Artificial Data Intelligence Act to regulate AI in the Canadian Marketplace (Charland, Savoie and van den Berg 2021).

One of the most notable changes introduced by Bill C-27 is the updated definition of "personal information." Under PIPEDA, personal information is defined as data that can identify an individual directly or indirectly, using reasonably available information (ibid. 2000). This definition presents a gap; if information is altered to the extent that its source cannot be traced, it can be used without consent from the individual it came from. Bill C-27 addresses this gap by introducing and distinguishing between the terms "Anonymize" and "De-identify." Anonymization, as defined in the bill, involves permanently modifying personal information to ensure no individual can be identified. Neither Bill C-27 nor PIPEDA offers protections for anonymized data, suggesting that if data is untraceable, it is no longer linked to the person who produced it. Conversely, de-identification involves modifying personal information to prevent direct identification, although a risk of traceability remains. Unlike its predecessor, Bill C-27 accounts for this risk, extending its protection to data in the de-identified category. However, Bill C-27 forgoes issues of labour, ownership and other human rights, instead focusing mostly on privacy and personal information.

Bill C-27's recognition of the risk attached with de-identified data aligns with a growing body of literature that rejects anonymization as a possibility in the current data extraction landscape. Early contributors to this literature include Michael Zimmer, who warned of the fragility of presumed privacy in his 2010 paper on the ethics of research using data from Facebook. Zimmer speaks to a 2008 case study in which a group of researchers accidentally released profile data from the media platform "despite good faithed efforts to protect the privacy of the subjects" (Zimmer 2010, 318). In his analysis, Zimmer found "considerable conceptual gaps in the understanding of the privacy implications of research in social networking spaces" as a whole (ibid., 323). A more recent study found that 99.98 percent of Americans could be re-identified in any data set using just 15 demographic attributes such as age, gender and marital status (Rocher, Hendrickx and Montjoye 2019). These findings question the assurances given by digital media firms regarding the protection of users' personal data, building on Zimmer's concern that current anonymization standards do not sufficiently guarantee privacy.

Therefore, despite Canada's recent attempts to better incorporate and manage data under federal regulations, these could be made more robust to better protect data producers. Currently, data is considered a commodity, merely the by-product of online consumption (Arrieta-Ibarra et al. 2018). In the Internet of Things where data is endlessly gathered from a multitude of sources, people are generating profits for large corporations and advertisers daily. Recent scholarship and activism on the issue suggests that this should be considered a form of uncompensated labour (ibid.).

In recent years, support has been growing for data intermediaries: a new suite of technologies that enable users to pool their data in a secure and trusted virtual space and allow their data to be bundled and sold to organizations only if the individuals have provided explicit consent (Carovano and Finck 2023). Data unions, a category of data intermediaries, can provide financial compensation for data provided and/or allow for new contracts or "terms of service" to be collectively negotiated between users and platforms, giving individuals more input over what they are agreeing to (Smichowski 2019). Data unions can also help to reduce the illegibility of data labour — a person's online activity that is unknowingly captured (Li et al. 2023). Although in some instances users may be aware that their data is being collected (rendering it legible), they may be unaware of the specific way their data is being used (ibid.). Empowering data unions in Canadian legislation would help to mitigate these key issues, as increasing individual Canadians' capacity to manage their data would help lower threats to sovereignty due to data mismanagement.

Protection of personal data must be balanced with international trade considerations. International trade agreements encourage openness of cross-border data flows and minimize restrictions on international data sharing to reduce the burden on businesses that operate internationally. International agreements such as the Comprehensive and Progressive Agreement on Trans-Pacific Partnership require parties to allow cross-border data flows between businesses. However, some restrictions are permitted if they are used to pursue public policy goals (Gao 2023).

Protecting personal data within the bounds of international agreements has been a rising priority among many of Canada's allies and international partners over the last several decades. The 2005 Asia-Pacific Economic Coperations's Privacy Framework and 2013 Organisation for Economic Co-operation and Development's privacy guidelines are two examples of international agreements that create frameworks for the international transfer of data and include requirements to ensure protection (ibid.). The World Economic Forum's (WEF's) "Rethinking Personal Data" has recognized that technological growth and data flows are "outstripping the ability to effectively govern on a global basis" and has called for a restructuring of the way that society views personal data (WEF 2014, 3). New tools for managing data, such as data unions, will allow consumers to reconsider and redevelop these relationships through the union.

Canada should look to the European Union as an example of progressive innovation in the field of international data governance. The EU 2016 General Data Protection Regulation, drawing from the earlier 1995 Data Protection Directive, contains a sweeping prohibition on cross-border data flows unless strict conditions are met (Jurcys, Compagnucci and Fenwick 2022). This approach of ensuring that other countries have sufficient means to protect the data of citizens is known as the adequacy approach and has since become a best practice for negotiating the terms of international data trade.

The European Union's latest innovation in data governance is the 2022 Data Governance Act, which seeks to incentivize voluntary data sharing and establish trust in data markets. To do this, the Data Governance Act establishes a regulatory framework to govern data intermediaries (Carovano and Finck 2023). The Digital Governance Act imposes 15 conditions on data intermediation services that aim to build trust and foster competition (von Ditfurth and Lienemann 2022). Data intermediaries must be neutral parties to the transaction and cannot use the data they manage for their own benefit. They also cannot make the price for their data intermediation services conditional on the use of other services that they offer, must take measures to ensure that the data they process is interoperable with other data intermediaries, and must monitor their transactions for unlawful transfers (ibid.).

The EU Data Governance Act aims to help data intermediaries such as data unions overcome their most significant hurdles: their unknown status as an emerging technology and the resulting lack of consumer trust. In early stages of growth, the benefit that a data union can offer its users is tied to the size of its user base — larger datasets containing more users and a wider range of data are worth far more than smaller datasets of limited scope. Conversely, a data union's user base will be proportional to the benefit, financial or otherwise, that it can offer new users. Heeding the WEF's message that data sharing and trade is rapidly outpacing governance, Canada should take a proactive approach to ensure that data unions do not become trapped in preliminary stages of development, struggling to build trust and gain users.

Failure to follow the example of the European Union and provide meaningful legislation regarding data protection could result in Canada falling further behind in keeping up with the rapid advancements in digital technology, being sidelined as an innovative player on the global stage and failing to protect citizens domestically. However, if Canada is to take the initial steps forwarded as recommendations, this could make room for more conceptual changes in the future. Empowering data intermediaries and providing Canadians with viable alternatives to better protect their data lays the foundation for revisiting the legal definition of data, potentially viewing it as labour rather than a commodity.

Recommendations

Canada should empower data union start-ups and initiatives by providing multifaceted funding incubators that include financial packages, training workshops and networking/mentoring opportunities. This should be spearheaded by the Minister of Innovation, Science and Industry, pursuant to his mandate to "ensure fair competition in the online marketplace" (Trudeau 2021). Innovative proposals for data intermediary companies should be rewarded with these benefits to help provide Canadians with legitimate alternative choices in relation to the data that they are continuously producing.

Canada should introduce legislation that will regulate and support the growth of data intermediaries by implementing regulatory requirements that data intermediaries must follow, and creating a certification process for those that demonstrate an ability to meet high standards of integrity. Giving federal certification to intermediaries that satisfy requirements for neutrality and transaction monitoring such as those seen in the Data Governance Act will allow successful intermediaries to build consumer trust and develop at a more rapid pace, while making it easier for consumers to know who to trust with their data.

Canada should remove the categorization of anonymized data in Bill C-27. Bill C-27 distinguishes between anonymized and de-identified data, offering protection based on the traceability of the information. Aside from the growing evidence that data can never be truly anonymized, data producers should not lose autonomy over the information they generate online merely because it has been altered to prevent traceability. By failing to protect data that has been decoupled from its producer, Bill C-27 perpetuates the current model of data governance and reinforces a system of data authoritarianism. Protecting all data, regardless of its traceability status, empowers data producers (the average Canadian) to retain control over their information.

About the Authors

Carissa Hubbard is a student in the University of Waterloo's Master's of Arts in Global Governance program, based at the Balsillie School of International Affairs.

Justin Myers is a student in the University of Waterloo's Master's of Arts in Global Governance program, based at the Balsillie School of International Affairs.

Reagan Roopnarine is a student in the University of Waterloo's Master's of Arts in Global Governance program, based at the Balsillie School of International Affairs.

Acknowledgements

The authors would like to thank Dr. Jeremy Hunsinger for his guidance and mentorship throughout the course of the fellowship program.

Works Cited

Arrieta-Ibarra, Imanol, Leonard Goff, Diego Jiménez-Hernández, Jaron Lanier and E. Glen Weyl. 2018. "Should We Treat Data as Labor? Moving beyond 'Free.'" AEA Papers and Proceedings: 38-42. doi:0.1257/pandp.20181003.

Carovano, Gabriele and Michèle Finck. 2023."Regulating Data Intermediaries: The Impact of the Data Governance Act on the EU's Data Economy." Computer Law & Security Review, 10830, 50.September. doi:10.1016/j.clsr.2023.105830.

Charland, Sabrina, Alexandra Savoie and Ryan van den Berg. 2021. "Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make Consequential and Related Amendments to other Acts." 1st Sess, 44th Parliament of Canada. https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

Gao, Henry. 2023. "Data Sovereignty and Trade Agreements: Three Digital Kingdoms." In Data Sovereignty from the Digital Silk Road to the Return of the State, edited by Anupam Chandler and Haochen Sun, 213– 39. New York, NY: Oxford University Press.

Jurcys, Paulius, Marcelo Corrales Compagnucci and Mark Fenwick. 2022. "The Future of International Data Transfers: Managing Legal Risk with a 'User-Held' Data Model." Computer Law & Security Review, 105691, 46. September. doi:10.1016/j.clsr.2022.105691.

Langley, David J., Jenny van Doorn, Irene C.L Ng, Stefan Stieglitz, Alexander Lazovik and Albert Boonstra. 2021. "The Internet of Everything: Smart Things and their Impact on Business Models." Journal of Business Research 122: 853–63. doi:10.1016/j.jbusres.2019.12.035.

Li, Hanlin, Stevie Chancellor, Nicholas Vincent and Brent Hecht. 2023. "The Dimensions of Data Labor: A Road Map for Researchers, Activists, and Policymakers to Empower Data Producers." 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23), June 12–15, 2023: 1151-1161. doi:10.1145/3593013.3594070.

Moiso, Corrado and Roberto Minerva. 2012. "Towards a User-Centric Personal Data Ecosystem: The Role of the Bank of Individuals' Data." 16th International Conference on Intelligence in the Next Generation: 202–-9. doi:10.1109/ICIN.2012.6376027.

Statistics Canada. 2023. "Canadian Internet Use Survey, 2022." Statistics Canada.

www150.statcan.gc.ca/n1/daily-quotidien/230720/dq230720b-eng.htm.

Trudeau, Justin. 2021. "Minister of Innovation, Science and Industry Mandate Letter." Office of the Prime Minister. www.pm.gc.ca/en/mandate-letters/2021/12/16/minister-innovation-science-and-industry-mandate-letter.

Papadimitropoulos, Evangelos. 2021. "Platform Capitalism, Platform Cooperativism, and the Commons." Rethinking Marxism: A Journal of Economics, Culture & Society 33 (2): 246–62. doi:10.1080/08935696.2021.1893108

Parliament of Canada. 2000.The Personal Information Protection and Electronic Documents Act (PIPEDA). https://laws-lois.justice.gc.ca/eng/acts/p-8.6/.

Rocher, Luc, Julien M. Hendrickx and Yves-Alexandre de Montjoye. 2019. "Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models." Nature Communications 10 (3069): 1–9. doi:10.1038/s41467-019-10933-3.

Smichowski, Bruno Carballa. 2019. "Alternative Data Governance Models: Moving Beyond One-Size Fits-All Solutions." Intereconomics Review of European Economic Policy 54 (4): 222–27. doi:10.1007/s10272-019-0828-x.

von Ditfurth, Lukas and Gregor Lienemann. 2022. "The Data Governance Act: – Promoting or Restricting Data Intermediaries?" Competition and Regulation in Network Industries 23, no. 4 November 19.: 270–95. doi:10.1177/17835917221141324.

WEF. 2014. "Rethinking Personal Data: A New Lens for Strengthening Trust." Cologny/Geneva, Switzerland: WEF. www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf.

Zimmer, Michael. 2010. "But the Data is Already Public: On the Ethics of Research in Facebook." Ethics and Information Technology 12 (4): 313–25. doi:10.1007/s10676-010-9227-5.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." Journal of Information Technology 30 (1): 75–89. doi:10.1057/jit.2015.5.