CJC Policy Portal

Searching for Data Privacy Self-Management: Individual Data Control and Canada's Digital Strategy

Jonathan A. Obar
York University

ABSTRACT

The problematic presumption that users can control the vast consent and data-management responsibilities associated with big data is referred to as the fallacy of data privacy self-management. Though untenable, this presumption remains fundamental to Canadian privacy law, exemplified in the individual access principle of the Personal Information Protection and Electronic Documents Act governing commercial data management. This article describes the fallacy, critiques the individual access principle, and introduces potential solutions relevant to Canada's digital strategy.

Keywords *Big data; Consent; Infomediation; PIPEDA; Privacy*

RÉSUMÉ

On peut qualifier d'« illusion de maîtrise sur ses données privées » cette présomption qu'ont les utilisateurs de pouvoir assumer les vastes responsabilités de gestion et de consentement associées aux mégadonnées. Cette présomption, bien qu'elle soit sans fondement, demeure fondamentale dans les lois canadiennes sur la protection de la vie privée. Par exemple, pour la gestion de données commerciales, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) se base sur un principe erroné d'accès individuel. Cet article décrit l'illusion de maîtrise sur ses données personnelles, critique le principe d'accès individuel, et propose des solutions pour améliorer la stratégie numérique canadienne.

Mots Clés *Mégadonnées; Consentement; Infomédiation; LPRPDE; Vie privée*

Jonathan A. Obar, PhD is an Assistant Professor in the Department of Communication Studies at York University. Email: jaobar@yorku.ca .

Canadian Journal of Communication Policy Portal Vol 44 (2019) PP-35–41 http://doi.org/10.22230/cjc.2019v44n2a3503

Introduction

You do not control your digital destiny. You say you want privacy—sometimes. You act as though you want protections—occasionally. But most of the time, you behave as if nothing bad is ever going to happen and ignore the big data deluge that might consume your rights and your dreams.

This is not entirely your fault. You have largely been placed in an impossible scenario, defined by a data privacy self-management fallacy (Obar, 2015; Solove, 2012), whereby governments and industry allow the game to continue without ensuring the rules are fair for all the players.

While the vulnerable are the most likely to be victimized by big data discrimination (Eubanks, 2018; Madden, Gilman, Levy, & Marwick, 2017; Newman, 2014), we are all threatened, even if we believe, incorrectly, that we have "nothing to hide" (Solove, 2007). Financial institutions, border and immigration services, the police, employers, and universities (among many others) may all implement big data-driven eligibility systems to assess whether we are "targets or waste" (Turow, 2012, p. 88). As Canada moves towards a digital strategy, we must ensure that big data processes are legal and just, that our digital footprints and any subsequent analyses are accurate and fair, and that a system is in place affording the opportunity to hold those in power accountable.

One step in this direction involves improving top-down policy approaches to data governance. This article asserts that the individual access principle (principle 9) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's privacy law governing commercial data use, contributes to our inability to protect ourselves in the big data universe (see also Clement & Obar, 2016). Addressing the limitations of this principle would improve Canada's approach to data governance and should therefore be central to Canada's digital strategy. In what follows, the fallacy of data privacy self-management is described. A critique of PIPEDA's individual access principle is presented next. The final section presents a number of recommendations to be considered in the context of a national digital strategy that may help individuals move beyond fallacy.

The fallacy of data privacy self-management

As described in "Big Data and *The Phantom Public*: Walter Lippmann and the Fallacy of Data Privacy Self-Management" (Obar, 2015), an overreliance on an "unattainable ideal" (p. 2) infects the current approach to user control in the big data context. Across and within each sector of the global economy, organizations big and small are involved in big data collection, management, retention, use, and disclosure. Each of these processes is advanced in a nuanced way unique to each entity involved. The questions asked and the answers sought vary. The knowledge and implementations of systems and practices vary. The resources vary. The geographical jurisdictions and resulting legal and ethical boundaries vary. This is to say that the representation of an individual's data, along with its management and use, will vary with each entity involved. An individual user might have a digital dossier with thousands of different entities across the world, each defined by a unique approach. On top of this, all is constantly changing, as new data flows day and night, as new answers build upon old, and as new industry opportunities and insights are incorporated into this "swarming confusion of problems" (Lippmann, quoted in Obar, 2015, p. 2).

The "unattainable ideal" (Lippmann, quoted in Obar, 2015, p. 2) or the fallacy of data privacy self-management, is the suggestion that an individual user could manage and oversee all of this. The number of big data challenges that define the threat mosaic increasingly imposed on the individual is potentially astronomical. An individual alone could never accomplish the amount of work required. The time and resources necessary cannot be realized as individuals live life, go to work, and enjoy family. There is also the challenge of expertise. Even if individuals had access to all of this data and the time to sort through it, and arrived at a long list of potential decisions to make, what then? Furthermore, beyond the challenges associated with reviewing, checking, and critiquing data, what about understanding how these actions could be integrated into the future plans of each individual organization? Or how secondary analyses would impact these decisions? Or analyses based on aggregated and/or anonymized data?

A persistent consent challenge exemplifies the data privacy self-management fallacy and the individual's problematic relationship to big data. The difficulties faced in attempting to navigate terms of service and privacy policies begins this problematic process, which continues through the aforementioned challenges associated with data control. Helen Nissenbaum (2011) describes the consent challenge as presenting a "transparency paradox" (p. 36). When entities involved with big data present individuals too much information in the manifestations of consent processes (e.g., terms of service and privacy policies), research suggests that information overload results (Obar & Oeldorf-Hirsch, 2018; Solove, 2012). The other end of the paradox suggests that not presenting individuals with enough information in consent materials hides the truth from them (Clement & Obar, 2016; Nissenbaum, 2011), making it difficult for individuals to understand big data processes in general, and their connections to those processes in particular.

With far too much to do, users need help. One strategy that may support individuals living in Canada is to address the limitations of Canadian privacy law and question how new approaches might actually deliver data privacy and reputation results.

PIPEDA's individual access principle

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is a federal law in Canada that governs commercial data management. It requires that entities operating in the private sector provide data subjects with certain information about data practices but requires that the individual data subject initiate the review process.

Principle 9 of PIPEDA, the individual access principle, states:

> Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. (Canada, 2000, p. 55)

While the principle does note that "The requested information shall be provided or made available in a form that is generally understandable" (Canada, 2000, p. 56), the necessity that entities involved in data management operate in the best interests of the individual is made less clear by statements such as the following:

> In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual. (Canada, 2000, pp. 55–56)

Thus the law protects individuals by requiring that they: 1) initiate review processes with data managers working at potentially thousands of entities, both seen (e.g., an internet service provider, social network, or bank) and hidden (e.g., data brokers), all over the world, likely in different languages, through interfaces and processes that have yet to be standardized and made user-friendly; 2) deal with the threat mosaic associated with these entities, defined by endless and evolving consent materials and datasets, each one of which is unique to the myriad data managers that deal with individual dossiers; and 3) address the uncertainty associated with the possibility that different entities "may have disclosed information" (Canada, 2000, p. 56).

At what point do we acknowledge the failures of the unattainable?

Moving beyond the first step: Addressing PIPEDA's individual access principle

Access is certainly an important first step toward data privacy self-management. Without the opportunity of access, individuals would have no method for even beginning the oversight process. Similarly, access to detailed and useful consent materials is also an essential first step; without the opportunity to review and learn from these materials, the truth would certainly be hidden.

What remains is a question of delivery. Once information is made available and access is given, how can an individual engage to reify privacy and reputation protections in the big data context? At the moment, PIPEDA does not provide an answer to these questions. No other Canadian law or regulation appears to provide an answer to these questions.

For this reason, the Office of the Privacy Commissioner of Canada (OPC, 2018) recently conducted a consent consultation, and has proposed a variety of "guidelines for obtaining meaningful consent" (para. 1). Among them is the need for clearer and less complex consent materials. Interactive, customizable, and dynamic consent processes are encouraged, as they move individuals away from static PDFs placed at the margins of sites or apps, which are rarely accessed and less often read. While many of these ideas suggest practices that might be improvements, none of them address the challenge of the evolving mosaic of materials, or the tangential nature of consent processes to online behaviours (Obar & Oeldorf-Hirsch, 2018). Furthermore, these suggestions only address the consent aspect of the self-management fallacy, not data management concerns.

Others argue for options that seemingly remove users from the oversight process. This includes calls for data managers to become information fiduciaries. As Jack Balkin (2016) notes,

> [a]n information fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the

> information they obtain in the course of the relationship … that means, in particular, that professionals have duties to use the information they obtain about their clients for the client's benefit and not to use the information to the client's disadvantage. (p. 1209)

This approach, which suggests that entities such as Google, Facebook, or a data broker have fiduciary responsibilities, aims to deliver privacy and reputation protections by requiring certain standards of practice, or as the OPC (2017) describes, calls for limitations on data practice. Advancing the fiduciary model is important, and acknowledges that platforms currently are, in the most practical sense, the most likely entity to deliver protections (DeNardis & Hackl, 2015). That being said, relying exclusively on a fiduciary model ignores the individual natures and stories of data publics and threatens the realization of data justice.

While all of these options ought to be tested, another recommendation to consider is the role of infomediation. With the aim of producing an advantageous principal-agent relationship (see Jensen & Meckling, 1976), an infomediary (e.g., agent) could be an individual or an organization that a user (e.g., principal) works with to achieve a measure of data privacy self-management. In a variety of parallel and historical contexts, much has been written about the benefits (and drawbacks) of these forms of delegation, and how they address information asymmetries, time management challenges, and demand for positive outcomes (e.g., Hawkins, Lake, Nielson, & Tierney, 2006; Jensen & Meckling, 1976; Snider, 2005). Similar to the lawyer who helps an individual navigate a legal scenario in the face of a complex legal system and the accountant who helps an individual interpret the tax code and realize a positive financial outcome through the analysis of financial data, for-profit and nonprofit infomediation might offer a form of delegation that could actually achieve privacy and reputation deliverables. For users who do not have the time or expertise to engage with consent materials, or the skill or the ability to manage their data, perhaps entities that specialize in these areas could help them make modest gains in terms of informed consent and data protection. Companies offering identity theft protection and dark-web scans are already beginning to offer these services. With funding and research support from the Canadian government, along with a vision for how Canadians ought to delegate their data privacy self-management, advances might be made that would ensure some protections.

Beginning to answer the question of how infomediation might work effectively involves the analysis of parallel and historical contexts (Obar, 2019). Though imperfect, the legal aid system, for example, provides a variety of principal-agent relationships that help support communities in need. This example highlights how government support systems can develop policy that produces advantageous divisions of labour through a distributive justice approach (see Obar & Schejter, 2019). As noted previously, current research suggests that members of marginalized communities are the most vulnerable to forms of big data discrimination. As a result, policy efforts should emphasize more equitable approaches in this context to ensure that those most likely to be victimized are the first to receive support. Again, figuring out how to do this well, or as well as possible, should involve assessments in contexts where this sort of work is already happening. Work on trauma-informed lawyering, for example, which has

connections to the legal aid system, is a context that big data infomediation efforts should learn from (e.g. Kraemer, & Patten, 2014).

One might ask: do we not have enough organizations to deal with? Why add a few more as infomediaries? One answer to this question is that one of the benefits of the principal-agent relationship is that the infomediary should actually reduce the number of organizations to manage by dealing with many of the data management entities on a user's behalf. Another answer relates to network and data sovereignty (see Clement, 2018; Obar & Clement, 2013; Scassa, 2018). One of the challenges raised with big data is the prevalence of international internet transmissions and, as a result, the internationalization of big data systems. If infomediaries operate in Canada, they can be subject to Canadian law and, thus, are more easily held accountable. Perhaps infomediaries might have to register with the government to facilitate services. Perhaps they might have to undergo periodic audits to ensure compliance. The central point here is that we need to do more to ensure "Canadian law governs Canadian data" (Obar & McPhail, 2018, p. 56).

As Canada moves towards a digital strategy, we should not discard the individual access principle but rather acknowledge and identify its limitations. Providing access to our big data via consent materials and data management opportunities is essential, but our efforts must not end there. Certainly the international nature of the big data boom amplifies the complexity of the challenge, but small victories at home with the hope of eventually expanding abroad might help Canadians realize a semblance of control in a world increasingly defined by ones and zeroes.

References

Balkin, Jack M. (2016). Information fiduciaries and the First Amendment. *UC Davis Law Review, 49*(4), 1183–1234.

Canada. (2000). *Personal Information Protection and Electronic Documents Act. S.C. 2000, c. 5.* URL: https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf [May 9, 2019].

Clement, Andrew. (2018, March 26). *Canadian network sovereignty: A strategy for twenty-first-century national infrastructure building.* Waterloo, ON: Centre for International Governance Innovation. URL: https://www.cigionline.org/articles/canadian-network-sovereignty [April 19, 2019].

Clement, Andrew, & Obar, Jonathan A. (2016). Keeping internet users in the know or in the dark: An analysis of the data privacy transparency of Canadian internet carriers. *Journal of Information Policy, 6*(1), 294–331.

DeNardis, Laura, & Hackl, Andrea M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770.

Eubanks, Virginia. (2018). *Automating inequality: How high-tech tools profile, police and punish the poor.* New York, NY: St. Martin's Press.

Hawkins, Darren G., Lake, David A., Nielson, Daniel L., & Tierney, Michael J. (Eds.). (2006). *Delegation and agency in international organizations.* New York, NY: Cambridge University Press.

Jensen, Michael C., & Meckling, William H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360.

Kraemer, Talia, & Patten, Eliza. (2014). Establishing a trauma-informed lawyer-client relationship (part one). *Child Law Practice*, *33*(10), 197–202.

Lippmann, Walter. (2009). *The phantom public.* New Brunswick, NJ: Transaction Publishers. (Original work published in 1927).

Madden, Mary, Gilman, Michele, Levy, Karen, & Marwick, Alice. (2017). Privacy, poverty, and Big Data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review, 95*(1), 53–125.

Newman, Nathan. (2014). *How big data enables economic harm to consumers, especially to low-income and other vulnerable sectors of the population.* URL: https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf [April 19, 2019].

Nissenbaum, Helen. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Obar, Jonathan A. (2015). Big data and the phantom public: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society, 2*(2), 1–16.

Obar, Jonathan A. (2019). *Big data and the phantom public revisited: The infomediary and "knowing publics."* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3387578 [May 13, 2019].

Obar, Jonathan A., & Clement, Andrew. (2013). Internet surveillance and boomerang routing: A call for Canadian network sovereignty. *TEM 2013: Proceedings of the Technology & Emerging Media Track-Annual Conference of the Canadian Communication Association.*

Obar, Jonathan, & McPhail, Brenda. (2018). *Preventing Big Data discrimination in Canada: Addressing design, consent and sovereignty challenges.* Waterloo, ON: Centre for International Governance Innovation. URL: https://www.cigionline.org/articles/preventing-big-data-discrimination-canada-addressing-design-consent-and-sovereignty [April 19, 2019].

Obar, Jonathan A., & Oeldorf-Hirsch, Anne. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1–20.

Obar, Jonathan A., & Schejter, Amit. M. (2019). *Distributional data justice: Shifting policy to address digital discrimination in vulnerable communities.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3374891 [April 19, 2019].

Office of the Privacy Commissioner of Canada. (2017). *Report on consent.* URL: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617 [May 9, 2019].

Office of the Privacy Commissioner of Canada. (2018). *Guidelines for obtaining meaningful consent.* URL: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ [April 19, 2019].

Scassa, Teresa. (2018, March 5). *Considerations for Canada's national data strategy.* Waterloo, ON: Centre for International Governance Innovation. URL: https://www.cigionline.org/articles/considerations-canadas-national-data-strategy [April 19, 2019].

Snider, J.H. (2005). *Speak softly and carry a big stick: How local TV broadcasters exert political power.* New York, NY: iUniverse.

Solove, Daniel J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, *44*(4), 745–772.

Solove, Daniel J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*, 1880–1903.

Turow, Joseph. (2012). *The daily you: How the new advertising industry is defining your identity and your worth.* New Haven, CT: Yale University Press.