Framing the Right to Digital Privacy

The issue of personal data ownership increasingly requires special attention on the part of legislators, especially with the acceleration of digitization due to the COVID-19 pandemic. Digitization is central to any modern state, since it is a new market that redefines the boundaries of privacy by extracting data from individuals' behaviours in an increasingly intrusive manner. In his report tabled in December 2019, the Privacy Commissioner of Canada identifies the critical need in Canada to modernize the *Privacy Act* (The Privacy Commissioner of Canada, 2019). The Commissioner outlines **the need for a framework** based on individuals' right to privacy and on obligations, whereas the current model is based more on codes of conduct that involve few obligations.

The European Union has been at the forefront of this issue with the adoption in 2016 of the *General Data Protection Regulation* (GDPR). The main purpose of this legislation is to provide individuals with rights to their personal data (Voigt and Von Dem Bussche, 2017). As a result, a citizen of the European Union may now request access to all their personal data collected by a company and may also request that their data be destroyed. This regulation therefore establishes an individual's right to the data they produce during online behaviour, which restores their ability to define the portion of their privacy that cannot be exploited by external actors. It is important to establish in Canada a legal framework to protect the rights of individuals to data resulting from their online behaviour that is comprehensive and complete, in order to protect and inform citizens about the reality of this new economy.

To fully understand this issue, we first need to address two opposing visions. On the one hand, the issue of personal data is seen as a new win-win market: The data "extractor" profits from the sale of data produced through user activity. The "buyer" can use this information to direct its products to potential users and can also change its product based on user behaviour. The "user" benefits from an enriched and customized experience without having to pay for it (Romanosky and Acquisti, 2009). However, this perspective is highly idealized and does not take the underlying economic relationship into account. In fact, the user has neither power nor influence in this market (Carrière-Swallow and Haksar,

2019). Although the user is the source of the exploited resource, they are at the mercy of undue influences seeking to modify their behaviour to the benefit of "buyers." (Zuboff, 2019). Thus, although the individual is the very source of this new economy, they do not derive any direct benefit from the exchange, and their agentivity is reduced.

The second perspective emphasizes the individual and their right to privacy. However, the issue of privacy in a digital context is complex and requires consideration. What can be considered private on the Internet? We can start by defining 'private' as opposed to 'public,' namely, what is common, exposed and shared with others. What is private would therefore be what is hidden, confidential and secret. We can also define 'private' from an individual point of view by confirming our "private life" through a right to choose our life rather than being controlled or alienated (González Fuster, 2014). This perspective emphasizes the importance of the possibility of having a closed space to keep information for ourselves and of being able to choose our own actions and our own life. In an increasingly digital world, it is important to create a personal space for individuals so that they have a private realm where they govern themselves and everything related to them.

The problem identified by the Privacy Commissioner of Canada is therefore central to equalizing these two visions. We need to strike a balance between an individual's right to privacy on the Internet and developing the digital economy. The solution of adopting a framework for individual rights would make it possible to regulate this economic sector and protect the individual's agentivity over the exploitation of the product of their behaviours, while allowing businesses to grow this sector. In developing this framework, it is important to focus on individuals, their protection and their integration into this new economy (Crabtree et al., 2016). To resolve issues of trust arising from scandals in which personal data are used without prior consent, the legislative framework needs to re-enable individuals by guaranteeing them power over the use of their data. It is equally important to address information asymmetry, where companies take advantage of their resources and privileged information, and individuals do not have the means to stand up to them.

To address the problem of agentivity, one must first ensure a basis of right to personal data, which can take the form of a "veto" where each individual can decide how their data is used. In addition, integrating nudges into this framework would guide the behaviour of both individuals and businesses without putting in place too many restrictive obligations. Indeed, a nudge, or decision node, is a type of choice architecture that guides an individual's choices in order to predictably change their behaviour without obliging them to do so (Bazerman and Tenbrunsel, 2013). It is about focusing on the structure of an individual's choice environment to encourage certain behaviours using behavioural psychology instruments (Bégin, 2014). The framework could therefore change the default option for user permission to collect personal data so that this permission is not granted by default. This change to choice architecture would mean that individuals, rather than having to make an effort to protect their privacy, could have that protection by default.

Similarly, digital consent forms need to be redesigned. These forms are too long and require technical and legal knowledge that most individuals do not have (Carolan, 2016; Perrault and Nazione, 2016). The consent arising from these forms is therefore based on asymmetric information that puts individuals in a position of dependence on businesses from the outset. Reversing the burden of consent first requires that companies restore some equality of information by making consent forms easy to understand (Perrault and McCullock, 2019). Second, we need to regulate what businesses are allowed to include in these forms to avoid problematic elements from being included. Dividing the form by theme (e.g. a form for individual/business rights/responsibilities) would allow individuals to better understand the implications of their consent.

One criticism this solution must address relates to the very idea of the new digital economy, which entails an increasing commodification of privacy (Zuboff, 2019; Elvy, 2017). Regulating and ensuring a certain amount of freedom for businesses legitimizes the exploitation of a portion of the personal sphere, which used to be considered sacred. The result is an ideological shift where the new normal is ready to be challenged once again to increase exploitation even further. In response to this

criticism we can say that establishing a framework for individual digital rights, similar to adopting a charter of human rights, allows a certain ideological fixation of what is “sacred” and establishes a conception of digital privacy in the very social contract of our society. Explicitly stating and defending the rights of individuals allows us to identify and punish deviant behaviours in order to avoid insidious exploitation where individuals are left to fend for themselves.

Bibliography

Bazerman, M.H., and Tenbrunsel, A.E. 2013. *Blind Spots*. Princeton University Press.

Bégin, L. (2014). "Design institutionnel et intervention éthique." in E. Rude-Antoine and M. Piévic (dir.), *Un état des lieux de la recherche et de l'enseignement en éthique* (pp. 91-101), L'Harmattan.

Carolan, E. (2016). "The continuing problems with online consent under the EU's emerging data protection principles." *Computer Law & Security Review*. 32, 3: 462-473.

Carrière-Swallow, Y., and Haksar, V. (2019). "The Economics and Implications of Data: An Integrated Perspective." *Departmental papers 19/16*. International Monetary Fund. https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596

Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Mortier, R. and Haddadi, H. (2016) "Enabling the new economic actor: data protection, the digital economy, and the Databox." *Personal and Ubiquitous Computing* 20, pp. 947-957.

Elvy, S.A. (2017) "Paying for privacy and the personal data economy." *Columbia Law Review* 117,6: 1369-1459.

González Fuster, G. (2014). "The Emergence of Personal Data Protection as a Fundamental Right of the EU." *Issues in Privacy and Data Protection* 16. (Switzerland) Springer International Publishing.

Office of the Privacy Commissioner of Canada (2019). *Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy.* https://www.priv.gc.ca/media/5076/ar_201819_eng.pdf

Perrault, E.K., and Nazione, S.A. 2016. "Informed Consent—Uninformed Participants: Shortcomings of Online Social Science Consent Forms and Recommendations for Improvement." *Journal of Empirical Research on Human Research Ethics* 11, 3: 274-280.

Perrault, E.K., McCullock, S.P. 2019. "Concise Consent Forms Appreciated—Still Not Comprehended: Applying Revised Common Rule Guidelines in Online Studies." *Journal of Empirical Research on Human Research Ethics* 14, 4: 299-306.

Romanosky, S., and Acquisti, A. (2009). "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." *Berkeley Technology Law Journal* 24, 3: 1061-1101.

Voigt, P., and von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer, 2006.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.