IRIE
International Review of Information Ethics Vol. 28 (06/2020)

Jill Clayton, Scott Sibbald

Privacy and Ethics Are Fundamental to Tech Development: A Privacy Regulator's Perspective

Abstract:

For years, privacy regulators have said that privacy is good for business. Strong privacy management programs and accountability mechanisms build trust with consumers. In the public sector, privacy regulators have seen massive information sharing projects fail when public input or consultation, or independent oversight is not considered. After a sequence of events in 2018, society as a whole began asking questions about what is being done with personal information and questioned whether it is in our best interests. This presentation made at the University of Alberta's Kule Institute's event on "AI, Ethics and Society" in May 2019 provides an overview of the shifts that have taken place and how privacy regulators internationally have incorporated discussions about ethical assessments, in addition to traditional privacy impact assessments, as a way to guide current and future tech developments involving personal information in a way that is legal, fair and just.

Keywords:

Big Data, Ethics, Personal Information, Private Sector, Privacy, Public Sector Regulation

Outline:

Author(s):

Jill Clayton:

- Office of the Information and Privacy Commissioner of Alberta, #410, 9925 - 109 Street, Edmonton, Alberta, Canada, T5K 2J8
- ☎ +1 780-422-6860, ✉ jclayton@oipc.ab.ca, 💻 www.oipc.ab.ca

Scott Sibblad:

- Office of the Information and Privacy Commissioner of Alberta, #410, 9925 - 109 Street, Edmonton, Alberta, Canada, T5K 2J8
- ☎ +1 780-422-6860, ✉ ssibbald@oipc.ab.ca, 💻 www.oipc.ab.ca

ISSN 1614-1687

1. Introduction

For years, privacy regulators have said that privacy is good for business. Strong privacy management programs and accountability mechanisms build trust with consumers. The response to such pronouncements was often muted. Privacy was seen as a barrier – not a driver – of business outcomes. Privacy in this context refers to information privacy or data protection. These conversations are shifting.

The above issues are not limited to the private sector. In the public sector, trust is equally important, particularly in democratic societies, when massive information sharing projects are undertaken. Opaqueness regularly leads to project failures (Perrin et al.).

Society is recognizing how integral privacy and ethics are to current and future tech development, and the business world and policymakers are responding and adapting to those expectations. These shifts are unsurprising given the sequence of events in 2018 that made it a watershed year for privacy regulation.

2. 2018: A Watershed Year for Privacy Regulation

In 2018, the curtain was lifted on a number of big data initiatives that made people sit up and take notice – and made many feel uncomfortable. Society as a whole began asking questions about what is being done with personal information and questioned whether it is in our best interests. Phrases like algorithmic transparency, information sharing, individualized marketing, targeted advertising, political profiling and voter manipulation became popular topics of discussion. These were issues many of us in this room had been talking about for years that suddenly became part of mainstream discourse.

First and foremost, the Facebook-Cambridge Analytica-AggregateIQ scandal shifted discussions about how we in democratic societies expect our personal information to be handled (Wu). The opaqueness of Uber's personal information practices was exposed. It took more than a year for Uber to notify millions of people that a malicious actor had access to their personal information (Newcomer). The Equifax breach showed that regardless of size or how many sensitive data sets a company may collect on hundreds of millions of people, it can have significant shortcomings in privacy and security practices (Office of the Privacy).

Such events can completely destroy the reputation of a company to the point of shuttering its doors, as was the case with Cambridge Analytica (Watkins and Sutton). These matters have also prompted discussions about companies that are "too big to fail". Policymakers in several countries are contemplating how to break up big tech (Dayen). Some CEOs are now advocating for further regulation (Zuckerberg). These concerns are not limited to the private sector.

For example, in the public sector, Statistics Canada's plan to collect the personal banking data of 500,000 Canadians was exposed (Russell and Akin). The plan was forged without public input or consultation, which diminished trust and halted the project. Smart cities made countless headlines, thanks in large part to the Waterfront Toronto and Sidewalk Labs project, and its public-private partnership to develop a data-driven neighbourhood (Wylie). Much of the backlash around this project has centred on data governance, ethics, trust and public consultation (Allen). Additionally, efforts to advance predictive analytics in policing (Kent) and child welfare (Hurley) have accelerated in recent years which raise myriad privacy and ethical questions.

Last year also saw a complete revamp in privacy regulation with the European Union's *General Data Protection Regulation* (GDPR) coming into force. GDPR requires businesses handling or processing the personal data of European citizens to be accountable for how data is managed; it requires notification of privacy and security incidents; and it introduces stringent penalties for non-compliance, among other legal obligations. These changes have a global impact.

Thanks to the conversations these and other cases have instigated, tech developments involving personal information are being reviewed to ensure compliance with privacy laws and regulations, and to ensure that they uphold individual autonomy, human rights, and are actually working to solve the problems they are intending fix.

3. What Do We Do Now?

Now that we've finally reached this watershed moment for privacy, the question becomes, "What do we do now?" First, multidisciplinary and cross-sectoral events such as the one today are a good start. Recognizing and understanding the different approaches and interests on these topics is useful. These discussions help us recognize where the gaps exist in current regulations. In Canada, that means seriously considering whether our laws are adequate to drive innovation in an ethical and thoughtful manner.

In Alberta, the first law was established nearly 25 years ago. The *Freedom of Information and Protection of Privacy Act* came into force in 1995, followed by the *Health Information Act* (HIA) in 2001, and the *Personal Information Protection Act* (PIPA) in 2004.

These laws establish access and privacy rights for all of us, and set a framework for how public, health and private sector organizations handle and safeguard both personal and health information.

There are variations in each law. For example, completing privacy impact assessments is required only under HIA, while reporting privacy breaches is required by both HIA and PIPA. Essentially, the laws establish the framework for privacy protection, and my office is the oversight body working to ensure compliance with these laws.

At one time, Alberta's laws, particularly PIPA, were considered very strong and certain aspects were recognized globally. These laws are now in need of modernization, particularly in light of GDPR and other global developments.

3.1. Privacy Management Programs

In the absence of more stringent regulations, back in 2012, my office collaborated with the Office of the Information and Privacy Commissioner for British Columbia and the Office of the Privacy Commissioner of Canada to issue a guidance document entitled "Getting Accountability Right with a Privacy Management Program". This document recognizes that organizations often struggle to understand how to build privacy into their practices (Office of the Information).

Under GDPR, one of the data protection principles is accountability. This is what we were thinking about when we issued the accountability guidance in 2012. The principles of accountability in the guidance document are now enshrined in GDPR.

Accountability in a privacy context means accepting responsibility for personal information protection. This is accomplished by a strong privacy management program that includes organizational commitment, program controls, and ongoing assessment and revision.

Like IT governance programs, effective privacy management takes careful planning across disciplines and job functions within an organization. It also takes considerable training and education to get the message across that privacy is everyone's responsibility.

The explosion of information sharing, data analytics and machine learning in all sectors have exposed gaps in traditional tools to address and mitigate privacy risks.

3.2. Beyond Privacy Impact Assessments: Ethics in Big Data Initiatives

In 2017, my office hosted a Data Privacy Day event in Edmonton that focused on artificial intelligence, machine learning, and ethical considerations for tech developments. Presenters were from the Alberta Machine Intelligence Institute, Google Canada and the Information Accountability Foundation (IAF).

We heard what artificial intelligence and its practical applications in the tech sector. We also talked about an ethical assessment framework project that IAF conducted in Canada meant to assist organizations in determining whether a project involving personal information is legal, fair and just.

For several years, there has been increasing recognition that privacy impact assessments, which have been used for more than two decades, do not contemplate all the human rights issues posed by many big data projects.

Based on this realization, IAF worked with Canadian companies involved in big data projects to develop the "Canadian Assessment Framework: Big Data Assessment for Canadian Private Sector Organizations Project" (Information Accountability). The framework is meant to assist organizations to determine and assess the rights and interests that may be impacted by personal information collection, use and disclosure in data-driven activities.

More recently, in October 2018, the International Conference of Data Protection and Privacy Commissioners met in Brussels and passed several resolutions that deal with tech development and big data issues. The theme of this annual data protection conference was digital ethics.

One of the resolutions passed at the conference was a declaration on privacy and ethics in artificial intelligence (International Conference). That is, ensuring that artificial intelligence and machine learning-based systems respect privacy rights and laws, and are legal, fair and just in their applications.

The international resolution recognizes that artificial intelligence systems have incredible potential and are being used for innovations in a variety of disciplines, often without any privacy implications, such as in industrial systems. But there are other considerations, especially privacy and human rights implications when massive personal data sets make decisions about or for individuals.

The conference endorsed principles for ethical assessments based on:

- Fairness for individuals and groups, such as ensuring that AI systems remain consistent with their original purposes
- Accountability for all relevant stakeholders, such as establishing governance processes or setting up independent ethics committees or oversight
- Transparency, such as promotion of algorithmic transparency and the auditability of systems
- Ethics by design, such as assessing and documenting the expected impacts on individuals and society at the beginning of an artificial intelligence project
- Empowerment of the individual by providing individuals with a way to exercise their individual rights
- Mitigating unlawful biases or discriminatory practices by investing in research to discover technical ways to identify, address and diminish biases

The resolution also emphasizes the need for trust, and the need for international standards and approaches to ensure human rights, human dignity and information privacy are components of artificial intelligence technologies that involve the use of personal information.

Most recently, the European Commission issued "Ethics Guidelines for Trustworthy AI", which includes a pilot assessment framework (European Commission).

The guidelines are based on principles similar to those outlined in the documents referenced above. They also strongly encourage interdisciplinary convergence of professionals in data privacy, cybersecurity and artificial intelligence to determine whether certain projects build trust for consumers and citizens.

The European Commission's guidance goes a step further than the documents referenced above in that the paper discusses how to balance certain tensions that exist between these principles.

For example, the paper discusses artificial intelligence for predictive policing, saying it "may help to reduce crime, but in ways that entail surveillance activities that impinge on individual liberty and privacy." The paper argues that an assessment of such projects should look at whether "overall benefits… substantially exceed foreseeable individual risks". For predictive policing, does the principle of preventing harm significantly outweigh the principle of human autonomy – or vice versa? These are the types of questions that should be asked when planning many tech projects.

Specific to artificial intelligence and machine learning, the guidelines contemplate "predictions". From a privacy perspective, the principle of accuracy of personal information is considered. In an artificial intelligence context, the paper notes that "accuracy pertains to an AI system's ability to make correct judgments, for example to correctly classify information into the proper categories, or its ability to make correct predictions, recommendations, or decisions based on data or models". Coupled with the principle of human autonomy and the unpredictability of the human experience, the paper notes, "A high level of accuracy is especially crucial in situations where the AI system affects human lives".

There are other assessment tools at various stages of development, including one from the United Nations Global Pulse in partnership with the International Association of Privacy Professionals.

They collaborated on a paper entitled "Building Ethics into Privacy Frameworks for Big Data and AI". I had the honour of speaking at a conference about this work in New York in May 2017, with many international aid organizations and private sector businesses.

The purpose of this work is in part to leverage the tried and true method of privacy impact assessments, but to incorporate ethics considerations into the decision-making framework. There are many challenges with this work, but the white paper was a step in the right direction for contemplating big data projects in humanitarian aid contexts.

4. Conclusion

In summary, as we contemplate how to go forward, both the public and the private sector should be mindful of the basics of strong privacy management programs and accountability mechanisms. Privacy needs to be valued as a fundamental or quasi-constitutional human right. It must become recognized that ethical considerations are paramount as all sectors continue to innovate with the use of personal information. Strong and effective regulatory schemes need to be put into place to ensure benefits are achieved and risks are mitigated – with proper independent oversight. Finally, privacy regulators need to keep an open mind to differing viewpoints to determine how best to proceed.

5. References

Allen, Kate, "AI pioneer urges Toronto to back ethical use of artificial intelligence", *Toronto Star*, April 11, 2019. Retrieved from https://www.thestar.com/news/gta/2019/04/11/ai-pioneer-urges-toronto-to-back-ethical-use-of-artificial-intelligence.html.

Dayen, David, "How to Think About Breaking Up Big Tech", *The Intercept*, April 1, 2019. Retrieved from https://theintercept.com/2019/04/01/elizabeth-warren-tech-regulation-2020/.

European Commission, "Ethics guidelines for trustworthy AI", April 8, 2019. Retrieved from https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

Hurley, Dan, "Can an Algorithm Tell When Kids Are in Danger?", *The New York Times Magazine*, January 2, 2018. Retrieved from https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html.

The Information Accountability Foundation, "Canadian Assessment Framework: Big Data Assessment for Canada Private Sector Organizations Project", February 26, 2017. Retrieved from http://informationaccountability.org/wp-content/uploads/Canadian-Assessment-Framework-final-28-feb.pdf.

International Conference of Data Protection and Privacy Commissioner, "Declaration on Ethics and Data Protection in Artificial Intelligence", October 2018. Retrieved from https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.

Kent, Fletcher, "Edmonton police seek public's help to pay for high-tech crime-fighting centre", *Global News*, February 5, 2018. Retrieved from https://globalnews.ca/news/4007696/edmonton-police-high-tech-crime-fighting-centre/.

Newcomer, Eric, "Uber Paid Hackers to Delete Stolen Data on 57 Million People", *Bloomberg*, November 21, 2017. Retrieved from https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.

Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia, "Getting Accountability Right with a Privacy Management Framework", April 2012. Retrieved from https://www.oipc.ab.ca/media/383671/guide_getting_accountability_with_privacy_program_apr2012.pdf.

Office of the Privacy Commissioner of Canada, "Privacy Commissioner finds Equifax safeguards 'unacceptable' and will monitor company for six years following major data breach", April 9, 2019. Retrieved from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_190409/.

Perrin, Stephanie, Barrigar, Jennifer and Gellman, Robert. "Government Information Sharing: Is Data Going Out of the Silos, Into the Mines?", *An Independent Research Report Commissioned by the Office of the Information and Privacy Commissioner of Alberta*, January 2015. Retrieved from https://www.oipc.ab.ca/media/387468/report_government_information_sharing_jan2015.pdf.

Russell, Andrew and Akin, David, "Stats Canada requesting banking information of 500,000 Canadians without their knowledge", *Global News*, October 26, 2018. Retrieved from https://globalnews.ca/news/4599953/exclusive-stats-canada-requesting-banking-information-of-500000-canadians-without-their-knowledge/.

Watkins, Eli and Sutton, Joe, "Cambridge Analytica files for bankruptcy", *CNN Politics*, May 18, 2018. Retrieved from https://www.cnn.com/2018/05/18/politics/cambridge-analytica-bankruptcy/index.html.

Wu, Tim, "How Capitalism Betrayed Privacy", *New York Times*, April 10, 2019. Retrieved from https://www.nytimes.com/2019/04/10/opinion/sunday/privacy-capitalism.html.

Wylie, Bianca, "Sidewalk Toronto: Here's the Business Model Framework", *Medium*, June 7, 2018. Retrieved from https://medium.com/@biancawylie/sidewalk-toronto-waterfront-toronto-digital-strategy-advisory-panel-meeting-1-before-6a158971eb65.

Zuckerberg, Mark, "The Internet needs new rules. Let's start in these four areas." *The Washington Post*, March 30, 2019. Retrieved from https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/.