Effective Data Protection Enforcement: An empirical look through the Canadian Experience

By Chantal Bernier,
National Practice Leader, Privacy and Cyber-security, Dentons Canada LLP
former Assistant and Interim Privacy Commissioner of Canada

The objective of this paper is to identify the key assets and limitations for effective data protection enforcement through the Canadian experience, as a case study. The question arises as Canada embarks on the projected modernisation of its privacy legislative framework addressing, as a pivotal issue, enforcement powers.

Technological developments put pressure on all privacy frameworks. Canada, however, faces specific challenges: (i) its adequacy status with Europe comes under review no later than 2020, according to Article 45.3 of the GDPR forcing the question as to whether it meets a higher standard of enforcement measures; (ii) its choice in 2000 of an ombuds model for its Data Protection Authority (DPA), the Office of the Privacy Commissioner of Canada (OPC), is now called "toothless" in the face of fining powers granted to its counterparts; and (iii) significant data breaches have shaken Canadians' trust in the ability of the current enforcement process in Canada to keep organizations compliant.

Last May, the Government of Canada issued a Digital Charter stating the Principles that will guide modernization.[1] Principle 10 reads:

> "10. Strong Enforcement and Real Accountability:
>
> There will be clear, meaningful penalties for violations of the laws and regulations that support these principles."

The *Digital Charter in Action: A Plan by Canadians for Canadians* announces that:

> "The Government will also examine a number of options to strengthen the enforcement powers of the [Office of the Privacy] Commissioner, and to increase his ability to collaborate with other key enforcement bodies on matters that pertain to privacy, competition and the broader data economy."[2]

This constitutes a departure from the policy choice of an ombuds model that has prevailed until now in Canada on two points: enforcement powers are deemed insufficient to be effective and the distinct, exclusive enforcement mechanisms among regulators do not address the multi disciplinarity of data protection.

In 2000, the idea was that the:

> "Ombuds model was particularly well suited to the first phase of regulating industry, where there was considerable concern about the impact of regulation on commercial enterprise."[3]

---

[1] https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

[2] https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html at page 26.

[3] France Houle and Lorne Sossin Powers and Functions of the Ombudsman in the Personal Information Protection and Electronic Documents Act: An Effectiveness Study, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2010/pipeda_h_s/

Effective Data Protection Enforcement: An empirical look through the Canadian Experience

Why a change of tack when the Office of the Privacy Commissioner of Canada (OPC) has been remarkably effective in bringing both private and public sector organisations to change their practices to improve privacy protection? The answer rests in the growing power imbalance between individuals and the organizations that hold their data, whether state or business. The seemingly infinite capacity to collect and analyze personal information in complex, invisible ways requires, more than ever, the possibility for individuals to have their claim to privacy leveraged and mediated by a commensurately strong data protection authority.

In this context, effective data protection enforcement is a matter of mediated accountability, meaning through a regulator with the powers and the resources to hold organisations accountable for compliance with their obligations to individuals. That is the case with any industry where users are not in a position to protect themselves from significant risk. So oversight mechanisms step in. Analogies take us to food inspection, airline safety or drug approval as other examples where technical challenges to assess risk exceed individual capacity and therefore require what can be called "mediated accountability".

Key assets and limitations of effective data protection enforcement in this context can be assessed by viewing the strengths and weaknesses of the Office of the Privacy Commissioner of Canada. We will use the Canadian experience as a case study.

I. Key assets for effective data protection enforcement

#1: An independent DPA

Canada and the European Union, as well as the 12 States that have received EU adequacy status, take the view that an effective DPA is corollary to the protection of privacy as a fundamental right. Respect for privacy, as the condition for the fulfillment of all rights and freedoms, is a defining value of a democratic society. As such, its protection must be entrusted to an independent guardian, situated above the political fray and vested with all the necessary resources to fulfil its mandate. The European *General Data Protection Regulation* (GDPR) makes it a specific criterion to assess adequacy of a national data protection regime to safely transfer personal data from the EU across borders:

> "When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
>
> (…)
>
> the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States."[4]

In confirming Canada's adequacy in 2006, the European Commission considered the fact that

> "…Canadian legislation provides for appropriate institutional mechanisms, such as an independent supervisory authority with appropriate powers and appropriate recourse before the courts in case of violations of privacy."[5]

---

[4] Article 45.2(b) *General Data Protection Regulation*

[5] The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act, at page 6 https://ec.europa.eu/transparency/regdoc/rep/2/2006/EN/2-2006-1520-EN-1-1.Pdf

What makes the OPC independent? First, it reports to Parliament, not to a Minister. Consequently, it escapes political direction. Second, the Commissioner is appointed for a period of 7 years, a comfortable tenure that provides latitude to take action. Thirdly, the Commissioner can only be removed for cause, after recommendation from Parliament. It has happened once where the Privacy Commissioner was found to have mismanaged public funds. Of course, the Commissioner is appointed by the Prime Minister, which allows a political choice, but the appointment is subject to the approval of Parliament and, once appointed, the Commissioner has a solid tenure to act freely.

Privacy policy is developed by the Department of Justice (DoJ), with respect to public sector privacy legislation, and by the Department of Innovation, Science and Economic Development (ISED) for private sector privacy legislation. It is enforced by the OPC through investigations and guidance in relation to the private sector and, in addition to investigations and guidance, through review of Privacy Impact Assessments and audits, at discretion, in relation to the public sector.

The OPC reports annually to Parliament on its investigations, naming respondent government departments but keeping the name of respondent companies confidential except where the Commissioner considers it in the public interest to name the company. The annual report is widely covered in the press so Canadians have visibility into all the privacy issues and violations occurring every year.

This takes us to the second key element of effective data protection enforcement as observed through the Canadian experience.

#2: Public support

When we celebrated the coming into force of the private sector privacy legislation in Mexico, in September 2010, Artemi Rallo Lombarte, then head of the Spanish DPA, had this resounding advice for his Mexican colleagues: your greatest, most critical, support is that of Mexican citizens.

This is very obvious with the OPC. Canadians' attachment to privacy and confidence in the OPC mean organizations comply, if not in agreement, at least for fear of being named in an investigation and suffering reputational damage. Canadian media knows how trustworthy OPC positions are for the quality of the research behind them and give them full airing. This creates an invincible solidarity between the Canadian DPA and the citizens it is tasked to protect. It requires sustained, proactive outreach to address topical issues and answer frequently asked questions.

#3: Sufficient Human and Financial Resources

The OPC's resources are voted in Parliament to the level necessary to fulfill its mandate and its staff is composed of public servants, hired on merit, professional and non-partisan, subject to strict conflict of interest rules. When Canada adopted mandatory breach notification, Parliament voted to increase the OPC's budget to correspond to the increase in workload.

The fields of expertise of DPA staff are also relevant. While lawyers and policy analysts have always been pillars of DPAs, it became clear about ten years ago that no DPA could function without technologists. It is one of the most challenging fields to recruit in considering market demand. Yet, technologists are essential in providing the DPA the necessary visibility into current data processing, on behalf of users. In the early 2000s, the OPC created a technology group that has grown since then and consolidated its importance.

#4: Relevance

For the first time in many years, the OPC has suffered a credibility loss and that experience highlights the key importance of relevance in effective data protection enforcement.

The OPC took the position that Canada's private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) prohibits cross-border data flows without consent when, contrary to the Québec and Alberta private sector privacy legislation, it contains no reference whatsoever to cross border transfers. In fact, the Canadian legislator has been careful not to create any such restriction, in spite of the fact that PIPEDA was adopted to obtain adequacy with Europe and *that Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*[6], in force at the time, restricted cross-border data transfers. Canada's economy is far too integrated with that of the United States to make such restriction feasible or desirable. Moreover, the Government of Canada has just signed trade agreements where it specifically commits to not adopting any data localization requirements.

The OPC's position was denounced, resoundingly and unanimously, as an error of law. ISED clarified in its *Digital Charter in Action: A Plan by Canadians, for Canadians* Canada's ongoing commitment to "support bilateral and multilateral commitments relating to the cross-border transfer of information, as well as commitments, which seek to prevent data localization requirements." The OPC eventually withdrew, reverting back to the position prevailing until then that cross border data transfers should be made known to users, as material to data management, but are not subject to express consent under Canadian law.

The debate has significantly undermined the credibility of the OPC, raising questions about its legal rigour, its awareness of relevant policy and its understanding of commercial realities. The fact that it misinterpreted PIPEDA, that it took a position practically inoperative in an economy largely integrated with that of the U.S., therefore largely tributary of cross border data flows, put the OPC at odds with commercial reality. Its position lacked relevance.

Richard Thomas, former U.K. Information Commissioner, has articulated an approach for relevance of the DPA through the concept of "Smart Data Protection". The model he proposes is tailored to the coming challenges of DPAs to stay relevant through an approach based on the following principles:

- Compliance is most solidly ensured when the rules correspond to recognized value systems.
- The rules are followed when there is a sense they have been made fairly.
- Trust in the regulator and therefore ongoing compliance rises where the rules are applied fairly.

More specifically, these observations lead to this vision for the effective DPAs of the future. DPAs should:

- Build on data holders' own interest in compliance (citizen and customer trust, loyalty and ongoing patronage) and proceed with partnerships, advice and support towards compliance rather than punishment that may only lead to circumventing the rules;
- Solidly substantiate their positions and conclusions with all factual evidence and robust legal analysis to maintain their own accountability and credibility;
- Ensure their staff skills and expertise cover the reality of privacy risks and compliance challenges. This may include lawyers, technologists, anthropologists, sociologists and political scientists as well as investigators

---

[6] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*

- Cooperate strategically with other DPAs to leverage their skills, expertise and resources to optimize outcomes;
- Create or take advantage of dialogue forums to remain cognizant of operational challenges in privacy protection and stay relevant in their interpretation of the law, as well as in choosing their priorities of intervention;
- Focus their areas of intervention to the highest risks and impact to cope with the proliferation of privacy risks in an expanding context of collection, use and sharing of personal information even if it has to be at the expense of low priority issues;
- Keep enforcement measures:
    - proportionate not only to the fault but also to the gain that was made in violating privacy to make privacy compliance the winning proposition;
    - Consistent to ensure fairness; and
    - Taking due diligence into account to administer sanctions as the case may be.

In short, Smart Data Protection means being strategic with respect to priorities of actions on the basis of risk, tailoring the DPA expertise to those priorities, engaging data holders from their own interest in compliance and enforcing the law taking into account proper diligence.

#5: Proportionate fines

This key element works both ways: fines must correspond to the level of profit companies gain from using personal data but must not exceed the level of responsibility of the organization. For example, a breach is not necessarily the result of negligence on the part of an organization. Consequently, the mere fact of a breach should not necessarily lead to a fine. Still, it must be as costly to misuse personal data as it is profitable to use it.

Fines must also be scalable, as in the GDPR, where they may be applied as a percentage of annual turnover. They must also include the power to name, in the public interest, as an incentive for investigated companies to cooperate with the DPA. It has been the secret of the OPC. Without powers to fine or to order measures, the OPC has caused tech giants to change their practices worldwide with the publication of its reports of findings naming the respondent company.

#6: Specific review powers for intrusive regimes

In relation to the state, some public interest imperatives, such as public safety, imply significant privacy intrusion. To address these elevated privacy risks, in addition to its general mandate, the OPC has been legislatively mandated to exercise close oversight. It is the case of the operations of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Canada's financial intelligence unit. The OPC is required to review, every two years, how it *"protects information it receives or collects under this Act and shall, within three months after the review, submit a report on those measures to the Speaker of the Senate and the Speaker of the House of Commons"*. This specific mandate reflects the level of intrusion, albeit justified, of financial intelligence gathering.

The OPC is also legislatively mandated to sit as a member of the National DNA Data Bank Advisory Committee under the Regulations of the *DNA Identification Act*. The duties of the Advisory Committee consist in advising the Commissioner of the Royal Canadian Mounted Police (RCMP) on any matter related to the establishment and operation of the national DNA data bank. Again, the specific mandate of the OPC in this regard serves to increase privacy protection in a context of high risk.

7: International cooperation

There are now several examples where efficiencies have been gained through joint or coordinated investigations between national DPAs as far apart geographically as Australia and Canada. The framework for international cooperation, adopted on October 22nd in Tirana, Albania at the 41st International Conference of Data Protection and Privacy Commissioners, moves the markers further in creating an infrastructure for cooperation between DPAs: the objective is to work "towards a global regulatory environment" through "enhanced information exchange", "focusing on key areas, as well as issuing template Memorandums of Understanding".[7]

The investigation of Globe24h is one that shows how international cooperation between DPAs may be the only way for effective data protection enforcement in certain circumstances. Globe24h came to the attention of the OPC, and other DPAs, in 2014 when numerous complainants alleged that the site was republishing legal decisions containing personal data on its website Globe24h.com, allowing this information to be indexed by search engines. When asked to delete it, Globe24h would charge up to €200 for each deletion. Confronted by the DPAs, Globe24h essentially thumbed its nose saying it was based in Rumania and therefore outside of the DPAs jurisdiction. A Memorandum of Understanding with Romania to allow cooperation with the Romanian DPA led to the closure of Globe24h.

#8: Prevention tools

Canada's public sector privacy legislation and internal government directives include what may be regarded as prevention tools: privacy impact assessments and discretionary reviews of compliance.

Through Treasury Board Directive, privacy impact assessments (PIAs), the equivalent to data protection impact assessments (DPIAs) in Article 35 of the GDPR, are made mandatory for "*new or substantially modified programs and activities involving the creation, collection and handling of personal information"*[8] by a federal public institution. This allows privacy integration from inception. The institution identifies the privacy risks created by an initiative and the related mitigation measures. Review by the OPC allows an independent, objective look to assess the legitimacy of the initiative, as well as the privacy mitigation exercise. The OPC may make recommendations where it can be improved or recommend cancellation of an initiative where no legitimacy can be demonstrated for the use of personal information. That was the case in 2009 when the Public Service Commission (PSC) submitted to the OPC's review a PIA for a program that would monitor the Internet and social networks for signs of potentially inappropriate political activity by public servants and potentially creating a database about the political opinions or activities of public servants. The projected program did not survive the PIA review. It was both abandoned and denounced by the PSC as an unendorsed initiative. The OPC had played a prevention role in protecting privacy.

Under section 37 of the *Privacy Act*, the OPC may "*carry out investigations in respect of personal information under the control of government institutions to ensure compliance"*.[9] The OPC has the power to audit, at its discretion, government departments' privacy practices. This power has been exercised as the legal basis for audit work in relation to public institutions that have a high volume and/or sensitive personal data. The 2009 *Audit of the Passenger Protect Program of Transport Canada*, which includes what is commonly called the "No fly list" is a case in point.

All these assets have made the OPC highly effective, even in an ombuds role. Commercial and technological realities, however, are challenging the sustainability of that enforcement approach.

---

[7] Press release, International News, International Data Protection Commissioners plan greater enforcement cooperation, 23 October 2019

[8] Directive on Privacy Impact Assessment, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308

[9] Section 37, *Privacy Act*

II. Key limitations to effective data protection enforcement

#1: Power imbalance with the data holders

The OPC's independence, professionalism and the power to name are no longer sufficient to hold tech giants accountable for their seemingly impenetrable and vast use of personal data:

The OPC has the power to investigate but without any financial consequence except perhaps some investments to correct reputational damage. The equation that misuse of personal information should be as costly as its use is profitable is not realized. Yet, no enforcement can be effective when violation of the law is still more advantageous than compliance. In a data-driven economy, fines are the logical response to violation of data protection laws.

Rebalancing power between the DPAs and the organizations processing data requires scalable fines as established in the GDPR. The mathematical equation should lead to making compliance the more profitable option.

Checks and balance in favour of organizations are also missing. The OPC may apply to the Federal Court of Canada, with the consent of the complainant if the investigation was not initiated by the OPC, to obtain an order for the organization to correct its privacy practices. The organizations, however, do not have such remedy to challenge the OPC's findings.[10] Any increase in the powers of the OPC will have to be accompanied by an increase in the remedies available to organizations.

#2: Lack of prevention tools for the private sector

The OPC's enforcement vantage point with the public sector through mandatory PIAs is not reflected in PIPEDA. Modeling Article 35 of the GDPR on DPIAs, however, would introduce an important prevention tool. Reviewing the construction of Article 35 points to key elements of success of DPIAs or PIAs as prevention tools: DPIAs are mandatory only where privacy risks are high therefore allowing scalability; the kind of processing operations that would require a DPIA is made public by the data protection authority, which increases accountability; while organizations have flexibility on how to perform the DPIAs as most relevant to them, some key requirements provide a certain level of clarity on basic expectations.

The introduction by the ICO of a "Sandbox service" also appears as a prevention tool. The stated purpose is to provide ICO expertise and advice to organisations who are innovating in a direction that may entail new uses of personal data. The key progress of the Sandbox notion is that it overcomes the scruple of DPAs of appearing to provide advance judgment and placing themselves in a situation of conflict of interest having advised a company that could eventually be the object of an investigation. Creating a "safe space" for organizations to innovate and assess privacy risks with the regulator creates a partnership for compliance that is highly promising.

#3: Lack of connection to the private sector

The OPC's recent and unprecedented credibility setback generated by its position on cross border data flows showed its disconnect with commercial realities. In addition to the error of law that privacy lawyers substantiated, industry was dumbfounded by the OPC's lack of understanding of the operational implications of requesting express consent for cross border data flows when the majority of the personal data is stored in the U.S., either through business affiliates or cloud storage. It may be understandable that public servants not be entirely alive to the operational challenges of the private sector. This situation, however, also calls for systematic consultation with the private sector. This could take the form of, advisory panels to the data protection authority bringing together representatives from industry who are not subject to the

[10] Section 25 PIPEDA and section 72 *Privacy Act*

jurisdiction of the OPC to avoid conflicts of interests or broad consultations where all business is broadly invited to participate.

#4: Siloed mandates

The increasingly obvious crosswalks between privacy law, competition law and consumer protection beg for some rationalization of regulatory jurisdiction and the ability to coordinate enforcement. In tandem with the issuance of the Digital Charter, the then Minister of ISED wrote to the Competition Bureau Commissioner describing Canada's plans to address multi-disciplinarity in legitimacy of data processing. On procedure, the Minister raises the question as to whether *"the ease of data accumulation in the digital environment requires new tools or mechanisms to avoid abuse"* and on norms he echoes the concern as to *"whether traditional tests of harm still apply in an era of algorithms and digital advertising"*.[11] The overlap of privacy and competitiveness is also addressed further in the letter stating that *"The growing accumulation of data has rightly raised a desire for heightened transparency and control for citizens in the use, processing, and portability of their information."* In parallel, as mentioned earlier, the Action Plan to the Digital Charter proposes to provide the OPC with the ability to cooperate with other regulators. The same preoccupation motivates the 41st International Conference of Data Protection and Privacy Commissioners "Resolution to support and facilitate regulatory cooperation between data protection authorities and consumer protection and competition authorities to achieve clear and consistently high standards of data protection in the Digital Economy."[12]

Conclusion

The strain on the Canadian ombuds model for data protection enforcement is indicative of a worldwide phenomenon: data processing has become so broad and complex as to exceed the capacities of traditional enforcement approaches. The data holders are so powerful as to be increasingly difficult to rein in and data use has become so profitable that it drives the whole economy, calling for concerted action between regulators. This points to a path forward of fines that are proportionate to profits, DPAs that are well resourced, and concerted approaches among regulators to address data processing issues in relation to every relevant facet.

Success of the Canadian model, however, also shows a path forward for effective data protection enforcement: compliance through partnership between DPAs and data holders to identify relevant solutions, visibility of privacy investigations of public interest to maintain accountability, powers commensurate to risk and comfortable independence.

As privacy risks increase, the commensurate power of the DPA to leverage and mediate the fundamental right to privacy is corollary to its fulfillment.

CANADA

Chantal Bernier
Counsel, Ottawa
D+1 613 783 9684
chantal.bernier@dentons.com

Kirsten Thompson
Partner, Toronto
D+1 416 863-4362

UK

Nick Graham
Partner, London
D+44 20 7320 6907
nick.graham@dentons.com

Simon Elliott
Partner, London
D +44 20 7246 7423

USA

Todd D. Daubert
Partner, Washington, DC
D+1 202 408 6458
todd.daubert@dentons.com

[11] 2019-05-21 Letter from Minister of Innovation, Science and Economic Development to the Commissioner of Competition at https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04464.html
[12] Op. cit at note 7

Effective Data Protection Enforcement: An empirical look through the Canadian Experience

kirsten.thompson@dentons.com simon.elliott@dentons.com