Department of Justice Canada
Ministère de la Justice Canada

PRIVACY ACT MODERNIZATION: A DISCUSSION PAPER

4. A modern and effective compliance framework with enhanced enforcement mechanisms

A technical engagement with experts on the future of the *Privacy Act*, Canada's federal public sector privacy law.

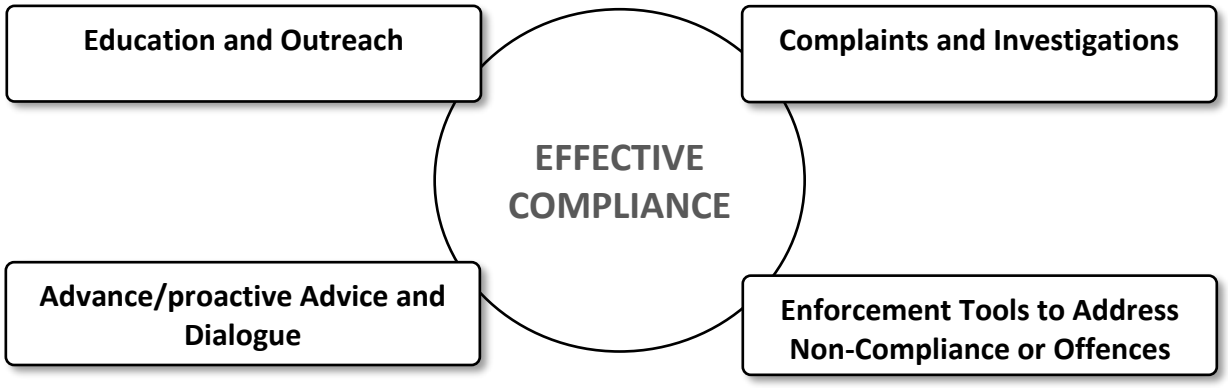
This discussion paper is being sent to expert stakeholders for their views and feedback on technical and legal considerations to consider in modernizing the *Privacy Act*. This targeted technical engagement will help the Government of Canada refine potential proposals for changes to the *Privacy Act*.

Canada

An enhanced compliance framework

There is a great deal of public discourse about the need for privacy rights to be backed by strong legal recourse and remedies. Our increasing awareness of the value of personal information and the individual, social and economic risks that can result from poor privacy protection clearly point in that direction. At the same time, privacy issues often flow from systems breakdowns, human error and ill-informed internal practices, not malevolent intent. There is therefore an equally important role for effective and systematized compliance supports to assist government institutions to prevent compliance issues from arising in the first place.

As Innovation, Science and Economic Development Canada ("ISED") has noted in *Strengthening Privacy for the Digital Age*, an effective Privacy Commissioner can be supported by a compliance framework that brings together four main elements:[1]



In the public sector context, it is also important to appropriately leverage the strengths and roles of the various institutional actors involved.

The Office of the Privacy Commissioner ("OPC") oversees compliance with the *Privacy Act.* The Commissioner interprets and applies the provisions of the Act. He determines what the Act requires of institutions, identifies compliance issues and makes recommendations as to what measures a government institution should take to bring itself into compliance.

As designated Minister for much of the Act, the President of the Treasury Board also supports government institutions to implement strong privacy management measures. The President is responsible for the provision of directives and guidelines concerning the operations of the Act and its regulations. The President has exercised this authority to publish a range of guidance documents and directives that support government institutions to comply with the requirements of the Act and implement a range of best practices. Treasury Board Secretariat also provides tools and advice to government institutions more generally.

In reviewing the ways in which the *Privacy Act* might be modernized to support enhanced compliance, a key question is how to most effectively leverage the strengths and specific roles of each of these institutional actors. For example, what tools can be given to the OPC to make the most of its expertise and most effectively protect individuals' privacy rights in its capacity overseeing compliance with the *Privacy Act* in the public sector? And how can the Treasury Board Secretariat best implement its mandate to establish policies

[1] See, for example, the discussion of the four functions of a data (privacy) protection authority – leader, police officer, complaint handler, authoriser – by the Centre for Information Policy Leadership in its White Paper, "Regulating for Results: Strategies and Priorities for Leadership and Engagement" at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf

and common standards for operational practices and provide tools to government institutions for use in the *Privacy Act* context?

This discussion paper is divided into two parts. The first raises questions about an enhanced "compliance framework" that could be set out in the *Privacy Act.* The term "compliance framework" is intended to describe a broad spectrum of measures structured to support and advance compliance with legal obligations under the Act. The second portion of the paper focuses specifically on policy considerations related to the Privacy Commissioner's request for enhanced enforcement powers – a new tool set that could be added at the end of this spectrum for rare scenarios in which binding adjudicative powers may be required.

In many instances, the considerations raised in this discussion paper mirror those that ISED has put forward for discussion in the private sector context in Strengthening Privacy for a Digital Age. This reflects that fact that many components of an effective compliance and enforcement regime will be relevant to both private sector organizations and public sector institutions. Appropriate alignments in Canada's federal privacy framework could ensure that the ways in which privacy compliance is supported and overseen take the perspective of the individual as a starting point, promote greater efficiency within the Office of the Privacy Commissioner and ensure fairness in expectations across sectors. At the same time, there will be some instances in which public sector-specific approaches will be more appropriate in light of key contextual differences, such as the differing accountability structures, institutional players and roles, and relationships with individuals at play. We would invite reflection upon the circumstances in which the public sector context may warrant unique approaches to privacy compliance and enforcement throughout this discussion paper.

A. *Privacy Act* compliance framework: a spectrum of compliance supports

Education and outreach

From a compliance perspective, a key goal will be supporting government institutions to effectively mitigate privacy risks, both at the beginning, and throughout the life cycle, of a program or activity.

The Privacy Commissioner has noted that "the Office lacks an explicit legislative authority to work proactively on outreach and education efforts tied to public sector issues. This is in comparison to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), where we have done extensive work for over a decade."[2] The Commissioner has recommended that he "be given express authority under the *Privacy Act* to conduct, on his own initiative, research and studies on issues of public importance" and "engage in public education and awareness activities. This would align his mandate with respect to research and education with his current mandate under PIPEDA and otherwise advance the purposes of the *Privacy Act*."[3] The Privacy Commissioner's submissions before the House of Commons' Standing Committee on Access to Information, Privacy and Ethics ("ETHI Committee") during its most recent study on *Privacy Act* reform echoed this position and were supported by most witnesses.

Including an express public education mandate in the Act could support the Privacy Commissioner to educate members of the public about their rights under the Act. It could also support the Privacy Commissioner to proactively communicate to government institutions his interpretations and expectations about the requirements of the Act. It would complement the current authority to undertake studies referred by the Minister of Justice.

Q.4(a): Should the Privacy Commissioner have an explicit mandate for education and outreach in relation to the public sector and if so, what should it include?

[2] https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/
[3] https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/

Advance/proactive advice and dialogue

i. Privacy impact assessments

Currently, the Treasury Board of Canada Secretariat and the Privacy Commissioner support government institutions to prevent and mitigate privacy risks through the privacy impact assessment (PIA) process.

A PIA is an analytical tool that aims to identify, assess, and resolve privacy implications of government programs before a new or substantially modified program or activity involving personal information is implemented by a government institution. In this way, it is a core element of an effective "privacy-by-design" approach that has, to date, been supported through the Treasury Board Directive on Privacy Impact Assessment.

The Treasury Board Secretariat Directive on Privacy Impact Assessment requires that government institutions prepare a PIA for a new or substantially modified program or activity where personal information will be used as part of a decision-making process that directly affects the individual or substantial modifications are made to a program or activity that is contracted out or transferred to another level of government or the private sector. The Directive also requires that the completed PIA be provided to the Treasury Board Secretariat and the Office of the Privacy Commissioner.

When it reviews a PIA, the OPC may offer "guidance in the interests of improving the personal information handling processes of federal institutions"[4]. However, the OPC is of the view that "accountability for decisions on the appropriate level of mitigation for privacy risk, and acceptance of any residual risk, lies solely with the institutions."[5] The OPC has indicated that "that [the PIA] process is invaluable in identifying and mitigating privacy risks prior to project implementation. However, application of this policy requirement does not have force of law. As a result, the practice, quality and timeliness of PIAs have been very uneven across institutions."[6]

The Privacy Commissioner supports integrating into the *Privacy Act* a legal requirement to conduct a PIA and engage the Privacy Commissioner prior to the implementation of the underlying program. Several government witnesses before the ETHI Committee noted that many government institutions have found their PIA interactions with the OPC to be "constructive and collaborative", although the process can be complex, time-consuming, and resource intensive. Other witnesses underscored the importance of using the PIA as a preventative, rather than reactive, tool; the value that public input into the process could add; and the need to ensure that privacy impacts are continuously monitored in a recurring and ongoing way.

A key question is whether and how to most effectively introduce a requirement to undertake a PIA in the Act. The relevant considerations would include ensuring a timely process; making effective use of the resources, both of the Privacy Commissioner and government institutions; making sure the OPC has the information and discretion needed for the most useful and efficient interventions; and giving government institutions confidence in the outcome of the discussions.

[4] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2015-16/pa_20160517_cra/
[5] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2015-16/pa_20160517_cra/
[6] https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/

Q.4(b): Should a requirement to conduct a PIA be added to the Privacy Act? If so, is the current, policy-based "test"[7] for when a PIA is required the most appropriate approach or are there other circumstances in which an institution should be legally required to undertake a PIA?

Q.4(c): How can the full potential of the PIA process be realized?

Q.4(d): Could the PIA process be improved by setting out the role of the Privacy Commissioner in response to a PIA, including what must be included by the OPC in any response to a PIA it reviews?

ii. Advanced compliance rulings

Some jurisdictions have empowered their oversight bodies to issue what are known as advance rulings or advisory opinions to support the provision of early and reliable direction to regulated entities in particularly complex matters. In general, an advance ruling or advisory opinion will provide guidance to regulated entities about how an oversight body would approach a particular legal issue if a complaint about that matter were received or if its oversight powers were otherwise engaged. The degree to which an oversight body is bound to apply a ruling or opinion it has articulated in advance will vary according to how the authority has been structured in statute.

For example, under Prince Edward Island's *Freedom of Information and Protection of Privacy Act*, a public body can ask the PEI Commissioner to give advice and recommendations on any matter respecting any rights or duties under the Act. The Commissioner can, "in writing provide the head with advice and recommendations that are based on material facts stated by the head or on any other considerations the Commissioner considers appropriate".

The New Zealand Privacy Commissioner has established a process by which Ministers and government agencies can seek an "advisory opinion" from the Privacy Commissioner concerning the application of New Zealand's Privacy Act 1993 ("NZ Act"). While the legislation itself does not specifically provide a power to give advisory opinions, the New Zealand Privacy Commissioner has established a policy for Ministers and agencies to obtain an advisory opinion from the Commissioner concerning their obligations under the NZ Act.

Other federal public bodies in Canada have the power to issue advisory opinions. For example, the Commissioner for Lobbying has the power to issue advisory opinions, the Commissioner of Competition has the power to issue a binding written opinion regarding the application of one or more sections of the *Competition Act*, and the Canada Revenue Agency provides advance rulings through the Income Tax Rulings Directorate.

To the extent the Act may be amended to include a principles-based regime, government institutions would have some flexibility with respect to how to ensure compliance. In this context, new avenues for engaging with the Privacy Commissioner to obtain early guidance could support effective risk management and promote strategic use of OPC resources. At the same time, an important consideration would be ensuring that government institutions remain independently accountable for their own decision-making.

[7] Currently, a PIA is to be initiated "when personal information is used for or is intended to be used as part of a decision-making process that directly affects the individual; upon substantial modifications to existing programs or activities where personal information is used or intended to be used for an administrative purpose; and when contracting out or transferring a program or activities to another level of government or the private sector results in substantial modifications to the program or activities": Treasury Board Secretariat Directive on Privacy Impact Assessment, 6.3.1, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308

Q.4(e): Is there a role for advance rulings or advisory opinions to supplement more general guidance from the OPC?

Q.4(f): In what circumstances would the issuance of an advance ruling or advisory opinion be appropriate? Could it be integrated into the PIA process in some circumstances?

Complaints and investigations

When not satisfied with an institution's response to a request for personal information or when not satisfied with an institution's management of their personal information, individuals can file a complaint with the Privacy Commissioner. Like other ombuds-models, this complaint-based system is intended to promote access to justice by allowing individuals to obtain remedies informally, outside of a highly structured adjudicative system. However, the effectiveness and efficiency of complaint resolution also impacts access to justice.

The Privacy Commissioner's complaint investigation function is not currently structured to allow the Privacy Commissioner to most effectively regulate government institutions' compliance with the *Privacy Act.* Some aspects of this function may even hinder the Commissioner's ability to secure maximum compliance with the *Privacy Act* in the most strategic and efficient way possible.

For example, the *Privacy Act* requires the Privacy Commissioner to accept and investigate each complaint the Office receives. Complaint volumes are increasing and the Commissioner has noted that "[i]n recent years, an increasing number of frivolous and vexatious complaints are lodged…which we have no choice but to investigate under the Act as it stands". Even in the case of meritorious complaints, the resources required to complete many investigations may be highly disproportionate to the public benefit gained from the exercise. A demand-led, complaint-driven oversight model that consumes significant resources can lead to important and broader compliance issues escaping the Privacy Commissioner's attention. The Canadian Bar Association's 2012 National Resolution calling for the *Privacy Act* to permit the Commissioner to decline to investigate certain complaints identified the absence of such a power an important access to justice issue. Such changes would be consistent with certain amendments to the *Access to Information Act* proposed under Bill C-58. Among other things, Bill C-58 proposes to authorize the Information Commissioner to refuse to investigate or cease to investigate a complaint that the Information Commissioner views as being trivial, frivolous or vexatious, or made in bad faith.

In April 2014, after a public consultation, the UK Commissioner introduced a new approach to complaints aimed at delivering its regulatory responsibilities as efficiently and effectively as possible. When the UK Commissioner receives a complaint, the complaint will be catalogued and analyzed. Complaints are assessed to determine whether they raise a one-off concern or evidence of a pattern of poor practices and the Commissioner's regulatory response will vary in intensity accordingly. The Commissioner publishes regular reports about its exercise of discretion in this context and relies on its cataloguing and preliminary analysis of complaints as an intelligence gathering exercise that allows it to more strategically direct its complaint investigation and broader public education resources.

Q.4(g): Should the Privacy Commissioner have the discretion to decline to investigate a complaint? Under what circumstances?

Q.4(h): Should the Privacy Commissioner have the discretion to discontinue a complaint investigation or decline to prepare a comprehensive investigation report? If so, in what circumstances?

Under PIPEDA, the Privacy Commissioner may refuse to investigate a complaint if other review procedures that are reasonably available have not been exhausted first. He is also permitted to discontinue a complaint

investigation if "the [private sector] organization has provided a fair and reasonable response to the complaint". These provisions generally work to give a private sector organization an opportunity to respond to a complaint first, before the Privacy Commissioner becomes involved. They may create effective incentives for organizations to be responsive to an individual's concerns as doing so can prevent a formal investigation by the Privacy Commissioner. Where this preliminary process was conducted in writing and under reasonable timelines, even unsuccessful efforts to resolve a complaint informally could streamline the Privacy Commissioner's evidence-gathering and complaint investigation function.

Q.4(i): Should the Privacy Act be amended to require a complainant to first address their complaint to the government institution involved?

Mediation of complaints

The Privacy Commissioner has developed and implemented an "early resolution" process that seeks to resolve complaints outside of a formal complaint investigation process. The Commissioner's 2017-18 Annual Report notes that the OPC resolved more than a third of *Privacy Act* complaints through early resolution over the last three years with an average treatment time of approximately four months, relative to approximately 11 months for a formal complaint investigation. The early resolution process constitutes an informally mediated complaint resolution process with a demonstrated ability to delivery timely and effective results for individual complainants.

Q.4(j): How can the Privacy Commissioner's mediation role be best reconciled with the potential introduction of order-making powers?

B. Enforcement tools to address non-compliance

The current, complaint-based ombuds-model has generally proven effective as a means of securing compliance with the *Privacy Act.* However, its efficiency and capacity to deliver the best results to Canadians has been questioned. Under the current model, the Privacy Commissioner receives and investigates complaints about federal institutions' compliance with the *Privacy Act*. He completes inquisitorial investigations and prepares reports, which may include non-binding recommendations. The report and recommendations can then form the basis for a negotiated resolution between the OPC and government. The *Privacy Act* does not currently empower the Privacy Commissioner to issue binding remedies.

Government institutions must consider a wide range of multifaceted and sometimes competing public policy considerations when designing and implementing government programs that utilize personal information. Budgets are not limitless; information technology may be dated and costly and difficult to enhance despite the benefits; and overlapping legal regimes and policy goals are usually at play. There are also often different ways of complying with the legal obligations set out in the *Privacy Act*, not a single path to compliance. Some of the delays in the existing complaint resolution process may relate to the increasing complexity of privacy issues. Given these realities, one important and complex question is what measures could be introduced in the Act to allow the Privacy Commissioner of Canada to most effectively address cases of potential non-compliance.

Compliance agreements

One tool that is available to the Privacy Commissioner of Canada under PIPEDA is the power to enter into compliance agreements with organizations. This is a relatively new power under PIPEDA available where the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a violation of PIPEDA. A compliance agreement allows an organization to agree to take certain measures aimed at ensuring compliance, whether non-compliance is conceded or not. Once entered into, a compliance agreement precludes the Privacy Commissioner from seeking legal remedies from the Federal Court in respect of any matter covered by the agreement. However, if an organization fails to respect commitments made in an agreement, the Privacy Commissioner is authorized to apply to the Federal Court for binding legal remedies, including an order requiring the organization to comply with the terms of the agreement.

When the Privacy Commissioner appeared before the Senate Standing Committee on Transport and Communications to discuss the amendments to PIPEDA that would, among other things, introduce compliance agreements, the Commissioner expressed strong support for this particular power. In his view, it would make it easier for the OPC to ensure that organizations carry through on commitments made during investigations; provide an incentive for organizations to effectively resolve issues and to honour their commitments; provide a recourse mechanism for the OPC should organizations fail to live up to an agreement; and give all parties more flexibility to reach resolution of complex issues within a more realistic and reasonable timeframe as an alternative to immediate litigation.

Given that compliance agreements are currently a tool used by the Privacy Commissioner in the private sector context, negotiated compliance agreements with government institutions could introduce the same intended benefits into the public sector, namely, minimizing the need for a protracted investigation or to engage Federal Court resources for enforcement purposes.

Q.4(k): Would introducing compliance agreements be an effective way of promoting a negotiated but binding resolution of complex privacy issues in the public-sector context?

Order-making powers

When compliance issues arise in the complaint investigation context, we know from the statistics maintained by the Privacy Commissioner that the need for coercive enforcement action to resolve them is very rare. The Privacy Commissioner's 2017-18 Departmental Results Report indicates that 97% of all public and private sector complaints and incidents were resolved to the satisfaction of the Office last year. In other words, in the public and private sectors combined, only 3% of complaints and incidents were not resolved to the satisfaction of the Privacy Commissioner by way of negotiated settlement.

While the Privacy Commissioner and government institutions typically reach negotiated compliance solutions, the Privacy Commissioner has identified issues with the process. He has expressed concern that the path to reaching a negotiated resolution can be "prolonged and arduous";[8] that government institutions "do not necessarily have to provide the OPC with complete documents at the outset";[9] and that "there is no sanction

[8] https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_20160310/
[9] ETHI, Evidence, 1st Session, 42nd Parliament, 1 November 2016, 1115 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

for government not to act promptly in responding to [an] investigation".[10] As well, there may be situations where negotiated compliance is not feasible.

In its report, the ETHI Committee noted a general consensus among witnesses that the current ombuds-model with powers of recommendation is not ultimately effective despite its results. Witnesses expressed the view that the *Privacy Act* was widely perceived as lacking adequate enforcement mechanisms. There were a number of different points of view about what oversight model could be the best replacement. Many provinces have a formalized, adjudicative order-making model. Newfoundland and Labrador has a "hybrid" model that allows its Commissioner to issue recommendations, which can be transformed into binding orders at the Commissioner's discretion. The evidence before the ETHI Committee suggests that both of these types of order-making models are effective. Since the ETHI Committee's report, the Government introduced Bill C-58, which sets out another approach to order-making developed for the federal access to information context. ISED is also exploring potential modifications to oversight by the Privacy Commissioner under PIPEDA for the private sector, including circumscribed order-making powers in the form of cessation and records preservation orders, among others.

The possibility of introducing order-making powers into the *Privacy Act* raises a number of important considerations.

(i) Institutional roles

Respect for institutional roles is one important consideration, particularly under a principles-based law that would give a government institution a measure of autonomy over the specific mechanisms it employs to satisfy the requirements of the law in some circumstances. Judicial review of discretionary decisions offers an analogy that effectively highlights the issue. A court that is judicially reviewing a discretionary decision will not normally order a particular result. Instead, the court will send the matter back to the statutory decision-maker to re-exercise his or her discretion in accordance with the court's analysis. This process respects the role of the court, which is to find issues that warrant judicial intervention, and the role of a statutory decision-maker, which is to properly exercise the discretion conferred by statute.

The Privacy Commissioner clearly has significant expertise in the identification of compliance issues under the *Privacy Act* and their resolution. However, the broader public policy complexities inherent in program design, a statutory framework that gives accountable organizations some discretion and the principles of ministerial accountability might all be factors that render institution heads best placed to take decisions about how, specifically, to bring themselves into compliance.

Many provincial jurisdictions with order-making powers address this issue of institutional roles by circumscribing the types of orders their Commissioners' may issue. Most provinces that confer order-making power typically limit their Commissioners to issuing specific orders to grant access to personal information, make corrections, destroy personal information or stop collecting, using or disclosing personal information. These strictly defined orders are intended to ensure the cessation of non-compliant practices identified through a complaint investigation and/or inquiry process. The substantive limits of these orders reflect the Commissioners' and government institutions' distinct institutional roles. The Commissioner is responsible for investigating non-compliance, ensuring non-compliant practices are stopped, and making additional recommendations. Government institutions are responsible for taking decisions about how to ensure compliance going forward. Commissioners are not normally empowered to order government institutions to implement particular compliance measures outside the scope of how their order-making powers have been defined in statute or to issue orders outside of their complaint investigation and adjudication functions (e.g. in

[10] ETHI, Evidence, 1st Session, 42nd Parliament, 10 March 2016, 0920 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

relation to PIAs).

Q.4(l): If order-making powers were introduced into the Privacy Act, how could they be designed to respect the Privacy Commissioner and government institutions' institutional roles under a modernized Act?

(ii) Impacts on access to justice

Potential impacts on complainants and access to justice must also be assessed. One of the most valuable features of the current regime is the advocacy role it allows the Privacy Commissioner to play on behalf of complainants. The complainant is not required to advance his or her own arguments during the Privacy Commissioner's investigation and may be represented by the Privacy Commissioner during an investigation and any related court proceedings under the Act. An adjudicative function giving rise to binding orders would require greater neutrality on the part of the Privacy Commissioner and/or alternative safeguards, such as a *de novo* judicial review process.

These issues have been well aired in the Parliamentary review of Bill C-58. In the case of Bill C-58, maintaining a *de novo* review process was identified as an important safeguard that allowed the Information Commissioner to retain the ability to represent and advocate on behalf of complainants, most notably in Federal Court in situations where a government institution could challenge the Information Commissioner's orders. And in provincial order-making power models that utilize a traditional – and not *de novo* – judicial review process – the Commissioners are not empowered to represent complainants before the courts. Under the existing models, a choice has always been made between *de novo* review (which allows the Commissioner to be an advocate for complainants before the courts on judicial review without prejudicing the other party) and a deferential judicial review model (which requires complainants to represent themselves, both during the Commissioner's decision-making process and in any judicial review process afterwards).

Q.4(m): How could an order-making model under the Privacy Act retain the elements of the existing regime that support access to justice for complainants?

(iii) Potential costs

Proportionality between the costs and benefits of moving to an order-making model is also important. The statistics indicate that compliance rates in the public sector are already very high, which strongly suggests that even with an order-making regime in place, few orders will ever be rendered. There is also a real possibility that procedural changes could be made to the existing model to improve the efficiency of the current process. In addition, a broad range of legislative modernizations are being explored, many of which could effectively mitigate risks, further proactive compliance, and shift the Privacy Commissioner away from a reactive, complaint-based oversight model. In these circumstances, an order-making model that necessitated significant or expensive administrative, organizational and machinery changes could be difficult to justify.

Q.4(n): Would expanding the Federal Court's judicial review jurisdiction to ensure comprehensive legal remedies were available for the full range of rights under the Privacy Act be a viable alternative to order-making powers as the impact of other significant changes was becoming known?

(iv) Unintended consequences

Finally, the evidence is also clear that government institutions benefit significantly from their dialogue with the Office of the Privacy Commissioner. It is possible that shifting towards a more formalized and adjudicative order-making model could have an effect opposite of that sought by the Privacy Commissioner. For example, the Canadian Bar Association has suggested that private sector organizations might experience a chill in their willingness to engage in cooperative dialogue with the Privacy Commissioner under an order-making power model. The same could be true of government institutions. However, provincial privacy commissioners have testified that this has not been their experience.

The potential for stifling productive dialogue through the introduction of order-making powers might be managed by strictly separating proactive advice and dialogue functions, along with negotiated complaint resolution mechanisms, from complaint adjudication. However, it would be essential that institutions had confidence in this separation of functions.

Q.4(o): What legislative provisions would be necessary to give government institutions confidence in an effective separation of functions within the Office of the Privacy Commissioner if order-making powers were introduced?