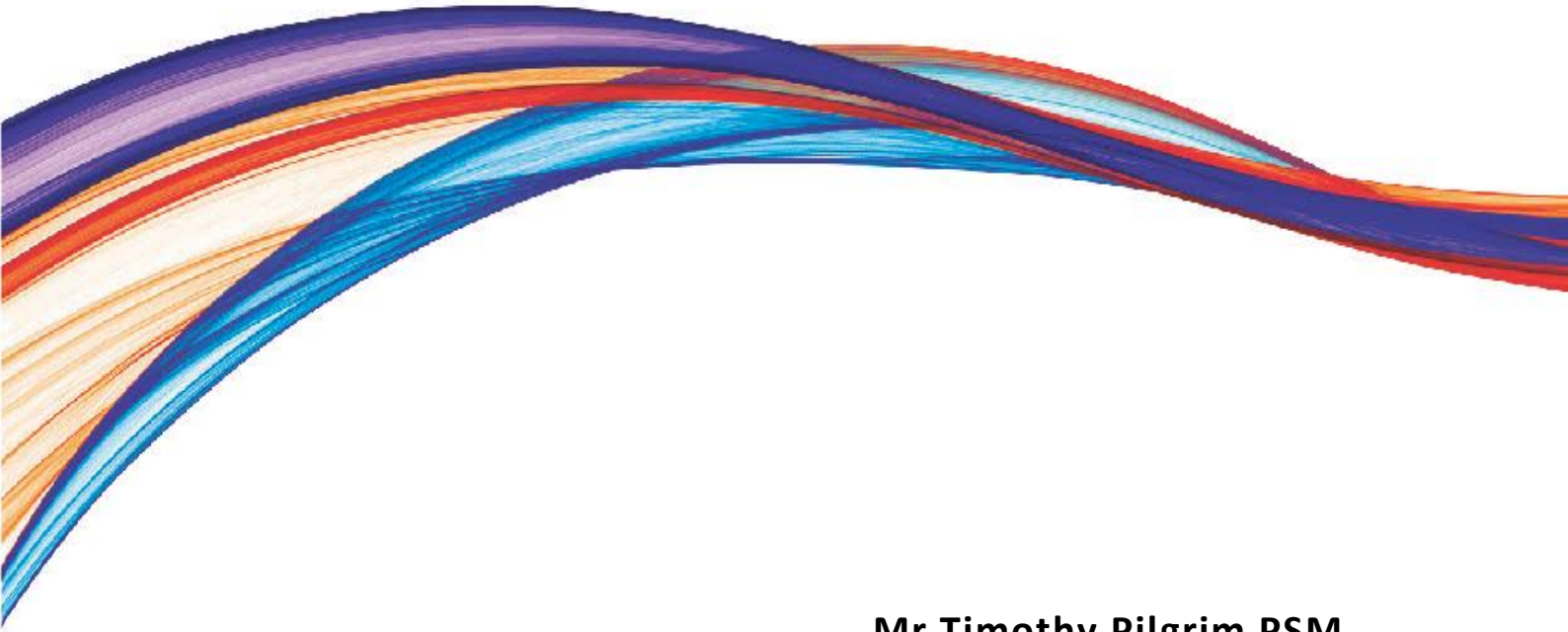
Australian Government
Office of the Australian Information Commissioner

Discussion Paper – Consent and Privacy

Submission to Office of the Privacy Commissioner of Canada

July 2016



Mr Timothy Pilgrim PSM
Acting Australian
Information Commissioner

Executive summary

I welcome the opportunity to comment on the Office of the Privacy Commissioner of Canada's (OPCC) Discussion Paper (the discussion paper) exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The discussion paper outlines a range of challenges and complex issues associated with the consent model. The consideration of these issues is timely, as my office, the Office of the Australian Information Commissioner (OAIC) is continually reflecting on the many opportunities presented by big data, the Internet of Things and the evolution to a continuously connected world, and how these intersect with individuals' expectations of privacy. The significant technological developments that have made big data practices and Internet of Things infrastructure a part of everyday life, demand that careful consideration be given to the way individuals exercise choice and control over their personal information – particularly, how individuals can be given notice of, and exercise meaningful consent to, an entity's often complex information handling practices.

In that context, this submission addresses consultation question 1, 'of the solutions identified in this paper, which one(s) have the most merit and why?', by outlining:

- steps taken by the OAIC to ensure notice given, and consent obtained, under the Australian *Privacy Act 1988* (Cth) (the Privacy Act), are meaningful
- the OAIC's focus on other measures to enhance privacy that complement transparency, notice and consent, such as de-identifying personal information and ensuring regulated entities implement good privacy governance mechanisms.

The submission also addresses consultation question 3, 'what roles, responsibilities and authorities should the parties responsible for promoting the development and adoption of solutions have to produce the most effective system?', by outlining the OAIC's regulatory powers under the Privacy Act, and how these are exercised in practice.

In my view, while facilitating individual choice and control through notice and consent remains an appropriate foundation for protecting privacy under Australian law, working closely with regulated entities to foster a culture of good privacy governance will complement and strengthen this model of privacy protection. The OAIC would also welcome the opportunity to engage with the OPCC in the future about other emerging models for privacy regulation that are intended to enhance privacy protections.

About the Office of the Australian Information Commissioner

The OAIC is an independent Commonwealth statutory agency within the Attorney-General's portfolio. The OAIC integrates three key functions:

- privacy functions conferred by the Privacy Act and other laws
- freedom of information functions, in particular oversight of the operation of the *Freedom of Information Act 1982* (the FOI Act) and review of decisions made by agencies and ministers under the FOI Act
- government information policy functions conferred on the Australian Information Commissioner under the *Australian Information Commissioner Act 2010*.

The integration of these three functions in one agency, gives the OAIC a unique perspective that comes from balancing the protection of personal information under the Privacy Act with the broader public interest in the free flow of information and with an individual's right to access government information under the FOI Act.

In exercising its privacy functions, the OAIC's central aim is to protect the community's personal information rights, and to work closely with Australian government agencies and private sector organisations to ensure that such information is respected and protected.

The Privacy Act

The Privacy Act includes thirteen Australian Privacy Principles (APPs), which apply to most private sector organisations and Australian and Norfolk Island Government agencies (referred to as APP entities). The APPs set out standards, rights and obligations for the handling, holding, accessing and correction of personal information. Additional protections apply to 'sensitive information', a subset of personal information, defined as information or an opinion about an individual's racial or ethnic origin, political opinions, religious beliefs, health information and other specified categories of information. A breach of an APP is an 'interference with the privacy of an individual'.

The APPs, which came into force on 12 March 2014, are technology neutral, applying equally to paper-based and digital environments. This helps to preserve their relevance and applicability, in a context of continually changing and emerging technologies. This principles-based law provides entities with the flexibility to tailor their personal information handling practices to their diverse needs and business models, and to the diverse needs of individuals.

The Privacy Act also contains provisions that regulate consumer credit reporting, specifically, the handling of personal information about the credit worthiness of an individual. For example, the provisions in Part IIIA of the Privacy Act outline:

- the types of personal information that credit providers can disclose to a credit reporting body, for the purpose of that information being included in an individual's credit report
- what entities can handle that information, and
- the purposes for which that information may be handled.

In addition, the Privacy Act regulates the handling of tax file numbers (TFNs). The *Tax File Number Guidelines 2011* issued under s 17 of the Privacy Act are legally binding guidelines that regulate the collection, storage, use, disclosure, security and disposal of individuals' tax file number information. These requirements supplement the protections in the APPs. This reflects the sensitivity attaching to TFNs, as unique identifiers, issued and handled by the Australian Government about many Australians.

The OAIC has a range of responsibilities under other laws, including laws relating to data matching, spent convictions, telecommunications, the Personal Properties Security Register, anti-money laundering and eHealth. For example, under the *My Health Records Act 2012,* the OAIC regulates the handling of personal information under the *My Health Record* system, the Australian government's digital health record system. The OAIC also regulates the handling of healthcare identifiers (issued to all individuals who receive healthcare in Australia) under the *Healthcare Identifiers Act 2010*, by all individuals and organisations, and can investigate complaints.[1]

The APPs – consent, transparency and notice

The APPs are structured to reflect the personal information lifecycle - from ensuring openness and transparency in information collection, through to use and disclosure, quality and security, access and correction.

Consent is not an APP in itself. It is relevant, however, to the operation of some APPs, namely those dealing with the collection of sensitive information (APP 3), use and disclosure (APP 6), direct marketing (APP 7) and cross-border disclosure of personal information (APP 8). In certain instances, consent can provide legal authority for an APP entity to deal with an individual's personal information in a particular way. For example:

- APP 3 – an APP entity must not collect sensitive information about an individual unless the individual consents and the information is reasonably necessary for the entity's functions or activities.
- APP 6 - an APP entity must not use or disclose personal information for a purpose other than the primary purpose of collection, unless the individual consents to the secondary use or disclosure.
- APP 7 – an organisation must not use or disclose personal information for the purpose of direct marketing unless the individual consents and the organisation

[1] More information about the OAIC's responsibilities in relation to the Health Records system and healthcare identifiers and about the OAIC's responsibilities under other laws is available on the OAIC website, www.oaic.gov.au

provides a simple way for the individual to opt out of receiving the direct marketing communications.
- APP 8 – an APP entity must not disclose an individual's personal information overseas unless it has taken reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. However, the entity may disclose the information overseas without taking any such steps, with consent providing the individual has been expressly informed that if they consent the entity will not have to take any such reasonable steps.

In each case consent is not the only basis for permitting personal information to be handled in a particular way under the Privacy Act. There are a range of other exceptions, under which an entity may collect sensitive information and use and disclose personal information. As outlined in the discussion paper (p. 3), this recognises that consent and the individual autonomy it protects do not override all other interests, and reflects the balance between privacy and other public interest objectives inherent in the Privacy Act.

Requiring entities to obtain an individual's consent before collecting sensitive information and handling personal information is a key privacy protection in the Privacy Act. It is adapted to the contextual nature of privacy, balancing individual privacy self-management with organisational accountability. As privacy regulator, a challenge is to ensure that any consent obtained is meaningful, and gives the individual the choice and control these provisions are intended to provide.

The OAIC has published advisory guidelines on the APPs and key concepts in the Privacy act, known as the APP guidelines, which outline four key elements of consent:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific
- the individual has the capacity to understand and communicate their consent, (including considerations relevant to children and young persons) (paragraph B.29) [2].

The APP guidelines also address some of the key challenges and issues in ensuring an individual's consent is meaningful. For example, the APP guidelines discuss:

- the limited circumstances in which use of an opt-out mechanism to infer consent may be appropriate (paragraph B.34)
- the potential for the practice of bundled consent to undermine the voluntary nature of consent (paragraphs B.39 – B.40)
- the assessment of whether an individual under the age of 18 has capacity to consent (as the Privacy Act does not specify an age after which individuals can make their own privacy decisions) (paragraph B.50 – B.52).

[2] The OAIC's APP guidelines have been published to assist in interpreting the APPs and key concepts in the Privacy Act. They are available at www.oaic.gov.au

Transparency and Notice

In addition to supporting the exercise of meaningful consent, the discrete transparency and notice requirements in APPs 1 and 5 underpin the exercise of individual choice and control and enhance the accountability of APP entities. APPs 1.3 – 1.6 require an APP entity to have a clearly expressed, up-to-date and freely available APP Privacy Policy about how the entity manages personal information. APP 5 requires an APP entity to take reasonable steps to notify an individual of certain matters relating to the collection of their personal information before collecting the information, or as soon as practicable after (APP 5).

Privacy policies and notices need to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. However, as outlined in the discussion paper, the complexity of today's information ecosystem, where unprecedented amounts of personal information are collected and shared for a range of different purposes, makes it challenging to give individuals' clear information about how their personal information will be handled. For example, a recent OAIC assessment (previously known as audit) of the privacy policies of Australian government and businesses, found the median length of these policies to be 3,413 words.[3] This length makes it difficult and time consuming to locate important information, and impacts the choice and control practically available to consumers.

The technology that leads to greater collection of personal information also presents the opportunity for more dynamic, multi-layered and user centric privacy policies and notices. The OAIC supports innovative approaches to privacy notices, for example 'just-in-time' notices, video notices and privacy dashboards and multi-layered privacy policies to assist with readability and navigability. Approaches aimed at ensuring privacy policies and notices contain clear, accessible and meaningful information have been recommended in a range of OAIC guidance, including the *APP* guidelines, the *Guide to developing an APP Privacy Policy* and *Mobile Privacy: a Better Practice Guide for Mobile App Developers.*[4] The OAIC also strongly encourages further innovation led by the business community to improve the way privacy information is displayed, so this information is given context, is provided at the right time, and can be easily read and understood.

Supplementing consent and notice

While transparency, notice and consent offer key privacy protections that facilitate individual choice and control, the Privacy Act includes a range of other complementary measures that protect individuals' privacy. Some of the measures the OAIC is currently focused on include fostering a culture of good privacy governance and facilitating an agreed understanding about the role of de-identification. These measures are outlined below.

[3] *OAIC Online Privacy Policies: Australian Privacy Principle 1 – Summary of Assessment* is available at www.oaic.gov.au

[4] *Guide to developing an APP Privacy Policy* and *Mobile Privacy: a Better Practice Guide for Mobile App Developers* are available at www.oaic.gov.au

Privacy governance

In Australia, APP entities are required to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs or a registered APP code that binds the entity (APP 1.2). The intention of APP 1.2 is to ensure that privacy compliance is embedded in the design of entities' practices, procedures and systems. APP entities will be better placed to meet their privacy obligations under the Privacy Act if they embed privacy protections in the design of their information handling practices. This also enhances individuals' opportunity to understand how their personal information is being handled and to make informed choices about that information handling.

APP 1.2 imposes a distinct and separate obligation upon an APP entity, in addition to being a general statement of its obligation to comply with other APPs. The purpose of APP 1.2 is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs.

Building on this principle, recent OAIC guidance and advice signal a shift in expectations regarding the integration of privacy management into APP entities' core business practices. The OAIC is working to foster cultural change to make open and transparent privacy practices second nature. For example, the OAIC has published a *Privacy Management Framework* (and *Privacy Management Plan Template*) which provides a top down and comprehensive approach to creating integrated and robust privacy governance systems. The Framework has four steps:

- Embed a culture of privacy that enables compliance
- Establish robust and effective privacy processes
- Evaluate your privacy processes to ensure continued effectiveness
- Enhance your response to privacy issues.[5]

The OAIC has also assessed entities privacy management frameworks in most recent privacy assessments, including two assessments of loyalty programs.[6] The recent assessments showed the organisations each had appropriate privacy notices that were consistent with their practices. However, given the amount of information used and disclosed by loyalty programs it is important that individuals are aware of the bargain they are making when they sign up. The OAIC and other regulators have a role in educating consumers about the privacy risks of disclosing personal information.

The OAIC has also released for public comment a draft advisory *Guide to big data and the Australian Privacy Principles*.[7] This guide recognises the potential social and economic benefits of big data analytics, while ensuring privacy protections are in place. The draft Guide outlines key privacy requirements and encourages the implementation of the Privacy Management Framework to embed 'privacy by design' in entities' culture, systems and initiatives from the design stage onwards. Many big data privacy challenges

[5] The OAIC's *Privacy Management Framework* and *privacy Management Template* are available at www.oaic.gov.au

[6] www.oaic.gov.au/privacy-law/assessments/

[7] The OAIC's consultation draft *Guide to big data and the Australian Privacy Principles* is available at www.oaic.gov.au

are addressed in this Guide, including notice and consent, collection and retention minimisation, as well as use limitation. The OAIC has encouraged all businesses and organisations interested in data analytics, data sharing and data innovation, to review the consultation draft and provide feedback to help inform the OAIC's future work in this expanding field.

De-identification

Under the Australian Privacy Act, personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable' (s 6(1)). De-identified information is not 'personal information' and is outside the scope of the Privacy Act.

The APPs support de-identification of personal information in specified circumstances. Examples include:

- if an entity no longer needs personal information for any permitted purpose, the entity must take reasonable steps to destroy or de-identify the information unless an exception applies (APP 11.2).
- organisations cannot collect health information about individuals for a research or public health or safety purposes permitted under the Privacy Act, if de-identified information would serve the same purpose (s 16B(2)(b)). If de-identified information would not serve the same purpose (and certain other conditions have been met) the organisation can only collect the information in accordance with guidelines issued by the National Health and Medical Research Council and approved by the Privacy Commissioner, about use of health information for research or public health or safety purposes.

De-identification can be a privacy enhancing tool with potential to unlock the value of big data. However, given the myriad of sectors using de-identification techniques, the bespoke solutions currently adopted by industry and government and the potential for re-identification if de-identification is not done properly, a key priority for the OAIC is to listen and consider the views of our stakeholders and revise our existing guidance on de-identification.[8] In doing so, the OAIC seeks to ensure that its guidance is not only an accurate reflection of the Australian Privacy Act, but also a practical and reliable solution that builds public confidence in the potential public benefit of data-driven innovation.

Regulatory powers

The discussion paper notes the importance of independent oversight to protect individuals' interests, particularly where individuals have limited control over their personal information.

[8] See OAIC *Privacy business resource 4: De-identification of data and information*, and *information policy agency resource 1: de-identification of data and information*, available at www.oaic.gov.au. These resources provide guidance about whether de-identification may be appropriate, choosing de-identification techniques and assessing the risk of re-identification.

The Privacy Act confers a range of regulatory action and enforcement powers on the Commissioner, which are based on an escalation model. These powers include:

- issuing guidelines for the avoidance of acts or practices that might interfere with privacy
- directing agencies to give the Commissioner a privacy impact assessment for proposed activities or functions that might have a significant impact on the privacy of individuals
- registering and, where necessary developing, APP and credit reporting codes of practice
- making binding rules, by legislative instrument, relating to the collection, use or disclosure of personal information in certain circumstances
- conducting an assessment (audit) of privacy compliance for APP entities
- accepting an enforceable undertaking and bringing proceedings to enforce an undertaking
- making a determination setting out the remedy for a breach of the Act both for an individual complaint investigation and a 'Commissioner initiated investigation' (CII)
- seeking a civil penalty from the courts in the case of a serious or repeated interference with privacy, or in the case of a breach of certain credit reporting provisions.

While the Commissioner has a range of regulatory action powers to draw on, the preferred regulatory approach is to work with APP entities to encourage compliance and best practice privacy practices and prevent privacy breaches.[9] The OAIC can use a range of steps as part of this approach, including engaging with entities to provide guidance, promote best practice compliance, and identify and seek to address privacy concerns as they arise, as well as engaging with entities who voluntarily and proactively notify the OAIC of a data breach incident.

The OAIC may commence an investigation into a suspected or alleged interference with privacy, either on receipt of a complaint or as a CII. If a complaint is received and certain conditions are satisfied, the complaint must be investigated.[10] When investigating a complaint, a reasonable attempt must be made to conciliate the complaint.[11] The majority of complaints are resolved in this way. In investigating a complaint or conducting a CII, the OAIC will seek to work with the parties concerned. Following a complaint investigation or CII, the Commissioner may decide to take enforcement action against an entity.

In addition to having a range of regulatory action powers to draw on, and the collaborative approach to regulation outlined above, the OAIC has extensive experience in complaint conciliation, meaning it provides a method for fast, informal and low-cost resolution of disputes.

[9] See OAIC *Privacy regulatory action policy*, paragraph 23, available at www.oaic.gov.au
[10] Sections 36, 40, 43 and 50 of the Privacy Act
[11] Section 40A of the Privacy Act

Ethical assessments

While the OAIC has recently been focused on fostering an accountability approach to privacy management, there is also great interest in understanding other emerging models for privacy regulation that are intended to enhance privacy protections. The OAIC is particularly interested in how ethical assessment models may operate in practice and the extent to which they can complement a choice and control model of privacy regulation. The OAIC would welcome the opportunity to engage with the OPCC about these matters in the future.