



Australian Government

Office of the Australian Information Commissioner

www.oaic.gov.au

GPO Box 5218 Sydney NSW 2001

P +61 2 9284 9800 F +61 2 9284 9666

E enquiries@oaic.gov.au

Enquiries 1300 363 992 TTY 1800 620 241

ABN 85 249 230 937

Our reference: D2017/009222

Digital Economy Strategy team
Department of Industry, Innovation and Science
GPO Box 2013, Canberra ACT 2601

Dear Digital Economy Strategy team

Submission on consultation paper - The Digital Economy: Opening up the conversation

I welcome the opportunity to provide comments on the Department of Industry, Innovation and Science's (DIIS) consultation paper for the Government's proposed Digital Economy Strategy (the Strategy).

The OAIC supports the proposed objects of the Strategy, which aim to maximise the value of digital technology for the Australian economy and community. The consultation paper refers to various digital economy initiatives, such as blockchain and open banking, which my Office actively monitors through our ongoing engagement with industry, government and international counterparts. From this engagement, I appreciate that maximising the potential of the digital economy will be best realised when data can be shared, used and built upon in new ways. However the protection of personal information needs to be a central consideration.

Emerging technologies and consumer trust

In my Office's experience, extracting value from emerging technologies can only occur sustainably when personal information protection is integral to the equation. It is important that the Digital Economy Strategy draws out the potential privacy risks and challenges of related initiatives, including options for mitigating these. My Office has extensive experience advising industry and government on how to unlock value from innovation within privacy frameworks.

A successful Digital Economy Strategy requires measures that can build trust and obtain social licence for data uses in the digital economy. When people have confidence about how their information is managed, they are more likely to support the use of that information to provide the services and value promised by digital economy initiatives.

The *Privacy Act 1988* (Privacy Act) provides a robust and flexible framework for facilitating community confidence in the Strategy. The Privacy Act contains 13 Australian Privacy Principles (APPs), which are technology-neutral and applicable to changing and emerging technologies. The APPs require regulated agencies and organisations to take reasonable

steps to keep personal information secure and to implement practices, procedures and systems to ensure compliance with the APPs. The OAIC works with agencies and organisations to facilitate compliance with the APPs and best privacy practice in information governance and data handling.

My comments below address these issues further, with a view to supporting the greater use of data for Australia's social and economic benefit at the same time as ensuring that individuals' privacy rights are protected in the digital economy.

About the Office of the Australian Information Commissioner (OAIC)

The Australian Parliament established the OAIC in 2010 to bring together three functions:

- freedom of information functions, including access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth)
- privacy functions through regulating the handling of personal information under the *Privacy Act 1988* (Privacy Act) and other Acts, and
- information management functions.

The integration of these three interrelated functions into one agency positions the OAIC to navigate the right to privacy and the right to access information, which should be recognised as a key national resource. It also provides my Office with a unique insight into many of the issues canvassed in the consultation paper, particularly with regard to realising the opportunities of the digital era alongside the robust protection of personal information.

In the exercise of these functions, the OAIC has established itself as a key advisory body, shaping how agencies and organisations harness emerging technologies and data practices to positively impact the lives of every Australian. Key initiatives include:

- the OAIC's suite of guidance to help entities innovate within a privacy framework, including the *De-identification Decision-Making Framework* (in collaboration with Data61), a draft *Guide to big data and the Australian Privacy Principles*, and a draft *Privacy and start-up businesses* resource
- being the independent regulator of the privacy aspects of the Health care identifiers service and the My Health Records system – two of the cornerstones of Australia's digital health ecosystem, and
- active engagement with international data protection authorities about new technologies through a range of forums, including the Asia Pacific Privacy Authorities Forum (APPA), the Global Privacy Enforcement Network (GPEN) and, at the 39th International Conference of Data Protection and Privacy Commissioners, which adopted the *Resolution on Collaboration between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy*.¹

¹ <https://icdppc.org/document-archive/adopted-resolutions/>

By leveraging the OAIC's existing capabilities in these areas, the Digital Economy Strategy will be better placed to maximise the potential of its initiatives while protecting personal information and privacy.

The role of Government as a privacy leader

The OAIC recognises that the digital economy opens up opportunities for government to use and share data in new and innovative ways to deliver better research, policy development and service delivery. In this context, it is increasingly important that agencies demonstrate privacy leadership, and cultivate a high-level of community trust in the way that these new activities are carried out. There are a number of activities being carried out across government in this regard, in which my Office is playing a significant role.

In May 2017, I jointly announced² the Australian Government Agencies Privacy Code (the Code) with the Secretary of the Department of Prime Minister and Cabinet (PM&C), which was registered on 27 October 2017 and commences on 1 July 2018. The Code will help build trust and 'informed confidence' with the public in relation to the handling of their personal information by ensuring that government agencies are subject to high standards when it comes to protecting and valuing the information they hold about Australians. This is particularly important given that public data is often derived from personal information which is collected on a mandatory basis, and it should therefore be respected, protected and handled in a way that is commensurate with broader community expectations.

My Office will shortly publish finalised guidance to assist entities to comply with the new notifiable data breach scheme (NDB scheme) that commences in February 2018³. The NDB scheme is aligned with similar requirements internationally and is designed to ensure that individuals are promptly informed about serious data breaches so that they can take action to protect themselves from harm, with an oversight role for my Office. Notification about serious data breaches also promotes transparency in information management, and is critical to public confidence in the capacity of entities to manage data breach incidents when things go wrong in the digital environment.

My Office is also involved in the Open Government Partnership⁴, which aims to secure commitments from governments to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance. In particular, commitment 2.2 in the Government's National Action Plan proposes to build and maintain public trust to address concerns about data sharing. A key milestone is to 'work with the Office of the Australian Information Commissioner to improve privacy risk management capability across the Australian Public Service'. The Code supports this commitment, and as part of this, my Office is collaborating with PM&C and other agencies to develop a framework that builds and maintains public trust, as well as addressing concerns about data sharing and

² [Developing an APS-wide Privacy Code](#)

³ For more information, see the OAIC's dedicated webpage at: www.oaic.gov.au/ndb

⁴ For more information, see the [Open Government Partnership Australia](#) website at: <https://ogpau.pmc.gov.au/commitment/22-build-and-maintain-public-trust-address-concerns-about-data-sharing-and-release>

release. This framework will ensure alignment across, and help build community trust in, the various data and digital initiatives under way within government.

Enabling and supporting the digital economy

The digital economy's initiatives involve handling personal information by businesses and government in new ways, such as through data sharing and processing arrangements enabled by applications in Internet of Things (IoT), FinTech, and artificial intelligence (AI). All of these initiatives have the potential to amplify existing privacy risks, for instance, where data sharing occurs for purposes that are different to the original purpose of data collection. On the other hand, there are significant opportunities for new technologies to yield positive privacy impacts for individuals.

While Australians are early adopters of technology, they have increasingly high expectations about how their personal information is managed. For the full potential of the digital economy to be realised, the Strategy must respond to the community's expectations, build trust, and achieve social license, so that Australians are willing to participate in its initiatives.

Privacy will be key to this equation. Over the past 16 years, my Office has conducted the Australian Community Attitudes to Privacy Survey (ACAPS), providing a clear indication of the community's expectations around personal information management. Of relevance to many digital economy initiatives, the 2017 ACAPS found that:

- 69% of Australians are more concerned about their online privacy than five years ago
- 83% believe there are greater privacy risks dealing with an organisation online compared to traditional settings
- 58% have decided not to deal with an organisation because of privacy concerns, and
- 79% are uncomfortable with businesses sharing their personal information.⁵

As outlined above, the OAIC plays a leading advisory role, both domestically and internationally, to support organisations in responding to the community's expectations by handling personal information appropriately. My Office already engages with industry and government to enable and support initiatives that are referenced by the consultation paper, including through:

- regularly providing advice, guidance and submissions on legislation, inquiries and proposals, for example, to the Treasury Department on the implementation of an Open Banking Regime⁶ and on the Productivity Commission's Inquiry Report into Data Availability and Use⁷
- observing Workstream 3 (Open Data & Privacy) of the IoT Alliance Australia and providing advice on data privacy guidelines for the use of IoT data, and

⁵ [Australian Community Attitudes to Privacy Survey 2017](#)

⁶ [Review into Open Banking in Australia – submission to the Treasury](#)

⁷ [Data Availability and Use – submission to Productivity Commission Draft Report; Data Availability and Use – submission to Productivity Commission Issues Paper](#)

- presenting at a range of RegTech and FinTech events to address questions from the financial sector on building privacy into new applications of technology.

For many of these initiatives, the OAIC's key messages reflect the importance of adopting a privacy-by-design approach towards innovation. Privacy-by-design is about finding ways to build privacy into projects from the design stage onwards. This enables entities to take steps at the outset of a project that minimise risks to an individual's privacy, while also optimising the use of data.

Privacy impact assessments (PIA) are an important tool that can assist the privacy-by-design approach. A PIA is a systematic assessment of a project that identifies the impact that it might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact. I strongly encourage DIIS to include privacy-by-design and PIAs in the Strategy, as measures to mitigate privacy risks and to enable successful digital economy initiatives.

A privacy-by-design approach is complemented by Australia's technologically-neutral privacy framework. As mentioned, the Privacy Act contains the APPs, which set how personal information is to be collected, used, disclosed, and secured. These principles can be applied to any digital environment, providing entities with the flexibility to tailor their personal information handling practices to diverse purposes and business models.

While the Privacy Act and a privacy-by-design approach enable and support innovation, unfortunately there are common misconceptions within industry and government that privacy is a 'roadblock' to innovation. In recognition of this, I welcome the opportunity for my Office to play a role in the Digital Economy Strategy, leveraging our networks and advisory experiences to help entities identify risks, build-in privacy safeguards, and address community concerns about the way personal information is handled.

Building areas of competitive strength to drive productivity and raise digital business capability

Privacy is increasingly acting as a commercial differentiator amongst competitors. When the community is confident about how a business will handle their personal information, they are more likely to trust its product or services, leading to improved business performance and competitive advantage. However, as the consultation paper notes, small businesses may struggle to unlock the potential of digital innovation.

While some exceptions apply, 'small business operators' (SBOs), with an annual turnover of \$3 million or less, are generally exempt from the Privacy Act.⁸

Although many SBOs may not have a legal obligation to handle personal information in accordance with the APPs, this is increasingly the expectation of the community. Yet, for a range of reasons, SBOs may face particular challenges in implementing privacy practices that meet consumer and community expectations.

⁸ Section 6D of the Privacy Act. More information on how the Privacy Act applies to small businesses can be found in the OAIC's [Privacy business resource 10: Does my small business need to comply with the Privacy Act?](#)

In recognition that many businesses outside of the Privacy Act's jurisdiction want to follow privacy best practice, my Office has developed a suite of resources⁹ to assist SBOs in embracing digital technologies and applying appropriate privacy safeguards.

Further, SBOs can choose to opt-in to the Privacy Act's requirements.¹⁰ By opting-in, these businesses are making a public commitment to good privacy practice, with the opportunity to benefit from any increase in consumer confidence and trust that may be derived from operating under the Privacy Act.

In raising the digital capability of businesses targeted by the Digital Economy Strategy, particularly small businesses, it will be important to overcome concerns about privacy so that businesses and consumers do not see digital transformation as a privacy risk. My Office would be pleased to assist DIIS in developing measures for the Digital Economy Strategy that empower all businesses to adopt new technologies and corresponding privacy practices.

Empowering all Australians through digital skills and inclusion

As the consultation paper canvassed, digital economy initiatives have a considerable potential to benefit individuals, yet those that could benefit most are at risk of being left behind. The Digital Economy Strategy needs to recognise that digital literacy goes beyond skills, to encompass confidence and online safety. Turning back to the 2017 ACAPS results, it is clear that many Australians do not feel empowered to exercise their privacy rights, particularly in online spaces:

- 47% of Australians do not know which organisation to report misuses of information to
- 58% are not aware of their ability to request access to their personal information
- only 29% normally read online privacy policies, and
- 69% are concerned that they may become a victim of identity fraud or theft in the next 12 months.

These concerns are magnified when individuals are unfamiliar with new technologies or unclear on how new applications will affect the way that their personal information is handled. Therefore, digital economy initiatives, which would for instance make big data practices and IoT infrastructure a part of everyday life, demand that careful consideration be given to the way individuals exercise choice and control over their personal information. In particular, the Strategy should outline how individuals can be given notice of, and exercise meaningful consent to, increasingly complex information handling practices.

For example, privacy policies and notices need to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. An OAIC assessment of Australian government and businesses' privacy policies found the median length to be 3,413 words, making it difficult to locate important information and limiting the choice and control practically available to individuals.¹¹

⁹ See [*Privacy business resource 18: Privacy and start-up businesses*](#) and [*FAQs for start-ups*](#)

¹⁰ Section 6EA of the Privacy Act

¹¹ [*Online privacy policies: Australian Privacy Principle 1 – Summary of assessment*](#)

New technologies also present the opportunity for more dynamic, multi-layered and user centric privacy policies and notices. The OAIC supports government and businesses to develop innovative approaches to privacy notices, for example ‘just-in-time’ notices, video notices, privacy dashboards and multi-layered privacy policies to assist with readability and navigability.

In addition to our working relationships with business and government, the OAIC undertakes substantial work with the community to help Australians understand their privacy rights and safely participate online. For example, we:

- host the Consumer Privacy Network (CPN), with representatives from 14 consumer organisations, which regularly meets to discuss consumer-specific privacy issues
- hold an annual Privacy Awareness Week (PAW), which in 2017 boasted 369 private and public sector partners
- have a strong working relationship with the eSafety Commissioner, and
- continue to develop educational resources and materials for individuals, such as our suite of *FAQs for individuals* and *Ten privacy tips to assist parents and carers*.

For the Digital Economy Strategy to foster digital skills and inclusion, it must contain measures that enable and empower individuals to make informed decisions about how their personal information is used. My office would appreciate the opportunity to provide DIIS with a privacy perspective as these are developed.

Conclusion

To assist DIIS in developing a Digital Economy Strategy that is underpinned by strong privacy practices and is consistent with community expectations, my Office would be pleased to participate in an advisory capacity. The OAIC has already provided extensive advice on many of the initiatives identified in the consultation paper, including on the international stage, and is uniquely placed to help DIIS strike an appropriate balance between the protection and free flow of information in the digital economy. Resourcing implications for my Office will also need to be considered as the Strategy is developed.

If you would like to discuss these comments or have any questions, please contact [REDACTED]

[REDACTED]
[REDACTED]

Yours sincerely

[REDACTED]
Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

29 November 2017