Australian Government

Department of Foreign Affairs and Trade

File No.: 18/1891#8

March 2018

Subject: Report of the Office of the High Commissioner for Human Rights on the right to privacy in the digital age

The Australian Government has the pleasure to provide the following information to assist in the preparation of the High Commissioner for Human Rights' report on the right to privacy in the digital age.

Privacy Protections in Australia and recent developments

In Australia, laws regulating the use and disclosure of information seek to strike an appropriate balance between safeguarding personal information and the right to privacy, the public interest in protecting and promoting the right to freedom of expression, the public interest in protecting public safety, and national security.

The *Privacy Act 1988* (the Privacy Act) sets out Australia's regulatory framework for privacy protection, including regulation of how government agencies and certain private sector organisations handle personal information about individuals. The Privacy Act promotes responsible and transparent handling personal information, and recognises that privacy protection must be balanced with the interests of regulated entities in carrying out their functions or activities.

The Privacy Act includes thirteen Australian Privacy Principles (APPs), which regulate the handling of personal information by private sector organisations with annual turnover of more than $3 million, certain kinds of smaller private sector organisations (such as private health providers), and most Australian Government agencies. These are known as APP entities. The design of the Privacy Act and the APPs was greatly influenced by the Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The APPs set out standards and obligations for the collection, use, disclosure, quality and security of personal information. The APPs also provide rights to individuals in relation to personal information that APP entities hold about them.

The APPs are framed in technology-neutral language to ensure that the Privacy Act will remain flexible and relevant in the face of technological change in the digital era. Although the Privacy Act does not specifically deal with new technologies or applications such as artificial intelligence or augmented reality, the Act's requirements will nonetheless apply where an APP entity handles personal information for the purposes of harnessing such technologies or applications.

Specific matters dealt with in the APPs include (but are not limited to):

- Open and transparent management of personal information (APP 1): APP entities must take reasonable steps to implement practices, procedures, policies and systems that will ensure compliance with the APPs and that will enable the entity to deal with inquiries or complaints.
- Notification of the collection of personal information (APP 5): APP entities must take reasonable steps to notify individuals of certain matters before collecting their personal information.
- Use or disclosure of personal information (APP 6): APP entities must not use or disclose personal information of an individual for a purpose other than the primary purpose of collection, unless the individual to whom the personal information relates has consented or an exception applies.
- Cross-border disclosure of personal information (APP 8): Before an APP entity discloses personal information overseas, the entity must take reasonable steps to ensure the overseas recipient does not breach the APPs in relation to the information (some exceptions apply). This approach is consistent with one of the objects of the Privacy Act – 'to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected.'
- Quality of personal information (APP 10): an APP entity must take reasonable steps to ensure that personal information it collects is accurate, up-to-date, and complete; and, must take reasonable steps to ensure that personal information it uses or discloses, having regard to the purpose of the use or disclosure, is accurate, up-to-date, complete and relevant.
- Security of personal information (APP 11): an APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification and disclosure. An APP entity must also take reasonable steps to destroy or permanently de-identify personal information it no longer needs for any purpose for which the information could be used or disclosed under the APPs (unless the information is contained in a Commonwealth record, or there is a legal obligation to retain the information).

A mandatory data breach notification scheme (the scheme) has operated under the Privacy Act from 22 February 2018, following the passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017*. The scheme requires notification where:

- an entity subject to the Privacy Act experiences a data breach of personal information, and
- the data breach would pose a likely risk of serious harm to affected individuals.

Where notification is required, entities will be required to notify the national privacy regulator, the Australian Information Commissioner, and take reasonable steps to notify affected individuals. The scheme includes requirements to provide timely notification of data breaches, or to undertake an assessment of suspected data breaches. Further information about the scheme and draft guidance material is available on the Office of the Australian Information Commissioner's (OAIC) website at: https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/.

Office of the Australian Information Commissioner (OAIC)

The OAIC is an independent statutory agency with functions relating to privacy law, freedom of information law and government information policy. The OAIC is responsible for handling complaints and conducting investigations concerning alleged breaches of the Privacy Act.

The Information Commissioner also has the power to:

- commence a Commissioner-initiated investigation into an act or practice that might breach the Privacy Act
- conduct a privacy performance assessment of whether an entity is maintaining and handling personal information in accordance with the Privacy Act, request an entity develop an enforceable code, and register enforceable codes
- direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function
- recognise external dispute resolution schemes to handle particular privacy-related complaints
- direct an entity to notify the Commissioner and individuals about a serious (notifiable) data breach.

Encryption

Australia supports the use of strong encryption to protect personal, commercial and government information. However, the increasing prevalence of encryption, particularly end-to-end encryption, is presenting significant challenges for agencies in lawfully accessing critical intelligence and evidence on computers, smart phones and other devices, and communications transiting across telecommunications networks. The Australian Government is seeking collaboration with, and reasonable assistance from, our industry partners in the pursuit of public safety. We will not, however, require the creation of so called 'backdoors' to encryption—that is, there will be no requirement that systemic weaknesses be built into encryption technologies. The law must apply online as it does offline.

Enhanced Privacy Protections in the Region – APEC

In the digital age businesses are increasingly transacting directly with, and collecting personal information from, consumers across the globe. This has required a global approach to privacy regulation and enforcement. Australia has been instrumental in the development of the Asia-Pacific Economic Coordination (APEC) Privacy Framework, which enables regional data transfers that benefit consumers and businesses in an environment supported by governments of member economies. The framework recognises that business has a key interest in protecting the personal information of customers and encourages a system in which personal information can be disclosed across borders with appropriate protections.

The Cross Border Privacy Rules (CBPR) system was developed by the APEC Data Privacy Subgroup, which Australia currently chairs, as the regional implementation mechanism for the APEC Privacy Framework. The CBPR system was endorsed by all APEC economies in 2011 and is based on the APEC Privacy Principles. The CBPR system ensures that participating businesses meet certain standards for the protection of personal information when moving data across borders. While participation by businesses is voluntary, the system has the potential to create a coherent approach across the region that will assist in building trust and confidence and protecting privacy in the digital economy. It is focused on business to business and business to consumer transactions. As such, government information and law enforcement or national security access to information, are expressly out of scope.

The CBPR system means that an economy has in place an appropriate legal framework to ensure the protection of personal information and one (or more) regulators that are able to take enforcement action in response to any breaches of the CBPR system requirements. Once a member economy has joined the CBPR system, businesses in that economy have the option of signing up to the CBPR system. Private sector bodies, referred to as 'accountability agents', assess whether applicant businesses satisfy the minimum criteria set out in the CBPR system, and then provide those businesses with ongoing dispute resolution and compliance services (as a third party assurance process).

Australia is in the process of becoming a participant of the CBPR system. The US and Japan have fully implemented the CBPR system (meaning businesses are actively using the system). Mexico, Canada, the Republic of Korea, Singapore, the Philippines and Chinese Taipei have announced their intention to participate and are at various stages of implementation of the CBPR system. With over one-third of the 21 APEC member economies being either CBPR participants or intending to participate, there is a growing impetus amongst Australian trading partners to provide a common mechanism for businesses to protect personal information in the digital and cross-border environments.

Recent discussions with the European Commission and APEC officials have also raised the prospect of some level of future interoperability between the EU General Data Protection Regulation (GDPR) and the CBPR system. Further information about the CBPR system can be found at: https://www.ag.gov.au/Consultations/Pages/APEC-cross-border-privacy-rules-public-consultation.aspx.

The OAIC is also active in a number of international privacy regulator networks (including the APEC Cross-border Privacy Enforcement Arrangement (CPEA), the Asia Pacific Privacy Authorities Network (APPA), and the Global Cross Border Enforcement Arrangement (GPEN)), which aim to encourage and facilitate better cooperation and collaboration between privacy enforcement authorities around the world.

Prohibition on interference with privacy and attacks on reputation

Article 17 of the ICCPR prohibits unlawful or arbitrary interferences with a person's privacy, family, home and correspondence. It also prohibits unlawful attacks on a person's reputation. It provides that persons have the right to the protection of the law against such interference or attacks.

This ICCPR prohibition on interference with privacy and attacks on reputation is incorporated into a wide range of government legislation, policies and programs, such as those that:

- involve the collection, storage, security, use, disclosure or publication of personal information
- regulate information held on a public register
- restrict access by individuals to their own personal information
- create or change confidentiality or secrecy provisions relating to personal information
- create an identification system
- provide for sharing of personal information across or within agencies
- relate to the use of personal information for statistical purposes
- authorise powers of entry to premises or search of persons or premises
- authorise surveillance (for instance by closed-circuit television)
- provide for compulsory physical intervention on a person (for instance to collect fingerprints, a DNA sample or biometric information)
- provide for mandatory disclosure or reporting of information (for instance by a doctor in relation to a patient)
- regulate matters pertaining to the family, such as the recognition of close or enduring personal relationships, the removal of children from a family by a public authority, adoption or guardianship
- authorise the compulsory occupation or acquisition of a home or regulate planning or environmental matters that may affect a person's home
- authorise the interception of communications, including written, verbal, electronic or telephonic
- affect the law relating to defamation, or
- affect the exemptions relating to disclosure of personal information under freedom of information legislation.

Scope of the ICCPR prohibition on interference with privacy and attacks on reputation

The Australian Government's public sector guidance sheet on the right to privacy and reputation notes that laws that affect privacy should be precise, and not give decision-makers too much discretion in authorising interferences with privacy. They should provide proper safeguards against arbitrary interference. To avoid being considered arbitrary, any interference with privacy must be in accordance with the provisions, aims and objectives of the *International Covenant on Civil and Political Rights* (ICCPR) and should be reasonable in the particular circumstances.

With reference to Article 17, we note that the UN Human Rights Committee (the Committee) has not defined 'privacy'. It should be understood to comprise freedom from unwarranted and unreasonable intrusions into activities that society recognises as falling within the sphere of individual autonomy.

The Committee has stated that the term 'family' should be given a broad interpretation to encompass the varied conceptions of the family as understood in different societies. In relation to Indigenous Australians, it is important that family be understood to include kinship structures, which encompass an extended family system often including distant relatives.

The Committee has given a broad interpretation to the term 'home', which includes a person's workplace. The Committee states that searches of a person's home should be restricted to those necessary to gather evidence and should not amount to harassment. Searches of a person should be carried out in manner consistent with the dignity of the person.

Interceptions of communications are not prohibited if they are authorised by law and not arbitrary. They are less likely to be regarded as arbitrary if they are subject to oversight by independent, preferably judicial, bodies.

The Committee has stated that countries have an obligation to adopt legislative and other measures to give effect to the prohibitions in Article 17, including the prohibition on attacks on reputation. Laws should provide effective remedies.

Conclusion

Australia is committed to ensuring individuals are able to enjoy the same human rights online as they enjoy offline. The Internet and digital communications provide an unparalleled opportunity for the exercise of the freedoms of expression, peaceful assembly and association, and the promotion and protection of other human rights. They also provide a unique platform to raise awareness of human rights issues enabling human rights defenders to better engage with vulnerable communities, as well as an amplified voice to carry out their work.

However, there is also a risk that digital technologies can be used to undermine the protection of human rights including through, for example, targeted hacking, arrest and intimidation of online activists, content censorship and Internet shutdowns. Such actions may amount to, or be seen to amount to, an arbitrary interference with privacy by governments, business or other third parties.

Australia uses multilateral fora, including membership of United Nations bodies, to advocate for a free, open and secure Internet. Freedom of expression, including freedom of expression online, was a focus of our Human Rights Council campaign and will continue to be a focus for Australia while on the Council. We are refining our strategies to ensure we leave a lasting legacy in the freedom of expression and freedom online space.