Russell Kennedy Government CPD

Privacy Update - An overview of key developments over the past year and what to expect in 2022

18 February 2022

Gina Tresidder, Special Counsel

Russell Kennedy Lawyers

Melbourne > Sydney

Webinar housekeeping

- All attendees will be on mute and their cameras turned off for the entire webinar
- We have BD tech support live to assist with any technical issues
- Use the chat function for any comments/technical issues
- Use the Q&A function for specific questions related to the webinar content – Questions will be addressed at the end of the webinar
- There will be a post webinar survey link sent at the end of the webinar. We value attendee feedback
- We will also have a QR code linking to our feedback survey towards the end of the presentation so you can provide instant feedback

Disclaimer

The information contained in this presentation is intended as **general commentary only** and should not be regarded as legal advice

Should you require specific advice on the topics or areas discussed, please contact the presenters directly

Introduction

Privacy Update

This session will cover:

1. The proposed changes to the ***Privacy Act 1988*** **(Cth)** under the ***Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021***, including:
   - new privacy code for social media and other online platforms; and
   - increased penalties and enforcement measures.

2. The **Discussion Paper** released by the Attorney-General's Department as part of its ongoing review into the **Privacy Act**, which proposes significant reforms based on overseas legislation such as the European General Data Protection Regulation (GDPR).

3. Outcome and recommendations from **OVIC's recent audit**, which assessed four Victorian public sector organisations' adherence to Standard 2 of the Victorian Protective Data Security Standards.

4. Recent **OAIC** investigations, including into **7-Eleven Stores** and **Clearview AI**.

Privacy Refresher

Commonwealth Legislation: *Privacy Act 1988* (Cth)

- The *Privacy Act 1988* (Cth) imposes obligations on '**APP entities**' which is defined as an agency or organisation:
  - an agency refers to a **federal government entity** and/or office holder; and
  - an organisation includes an individual, body corporate, partnership, unincorporated association, or trust.
- An APP entity **does not include**:
  - a 'small business operator' (subject to the exceptions) if the annual turnover of the business is less than $3 million;
  - a registered political party;
  - a state or territory authority or prescribed instrumentality of a State or Territory.
- A **small business operator** will be required to comply with the *Privacy Act* if they:
  - operate another business with a turnover of $3 million or more;
  - provide a health service or otherwise hold health information (other than in an employee record);
  - disclose, or collect, personal information about another individual for a benefit, service or advantage;
  - are a contracted service provider for a Commonwealth contract;
  - are a credit reporting body.

Obligations under the *Privacy Act 1988*

- An **APP entity** will be deemed to have interfered with the privacy of an individual if the act or practice breaches:
    - an **Australian Privacy Principle** in relation to personal information about the individual; or
    - a registered **APP code** or **CR code** that binds the entity in relation to personal information about the individual.

- There are thirteen **Australian Privacy Principles**, which address the collection, use and disclosure of personal information, including the requirements for a privacy policy and notification of the collection of personal information.
- **Personal Information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

    (a) whether the information or opinion is true or not; and

    (b) whether the information or opinion is recorded in a material form or not. (section 6)

- **Sensitive Information** means information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices or criminal record that is also personal information; or health information about an individual; genetic information about an individual that is not otherwise health information; biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or biometric templates.

Key State Legislation

Victoria

- The ***Privacy and Data Protection Act 2014*** (Vic) (PDP Act) contains 10 **Information Privacy Principles** (IPPs) that outline how Victorian public sector organisations must handle personal information.
- the ***Health Records Act 2001*** (Vic), outlines how Victorian public sector agencies and health service providers manage health information.

NSW

- The ***Privacy and Personal Information Protection Act 1998*** (NSW) (PPIP Act) contains 12 **Information Protection Principles** (IPPs) that outline how NSW public sector organisations must handle personal information.
- The ***Health Records and Information Privacy Act 2002*** (HRIP Act) outlines how NSW public sector agencies and health service providers manage health information.

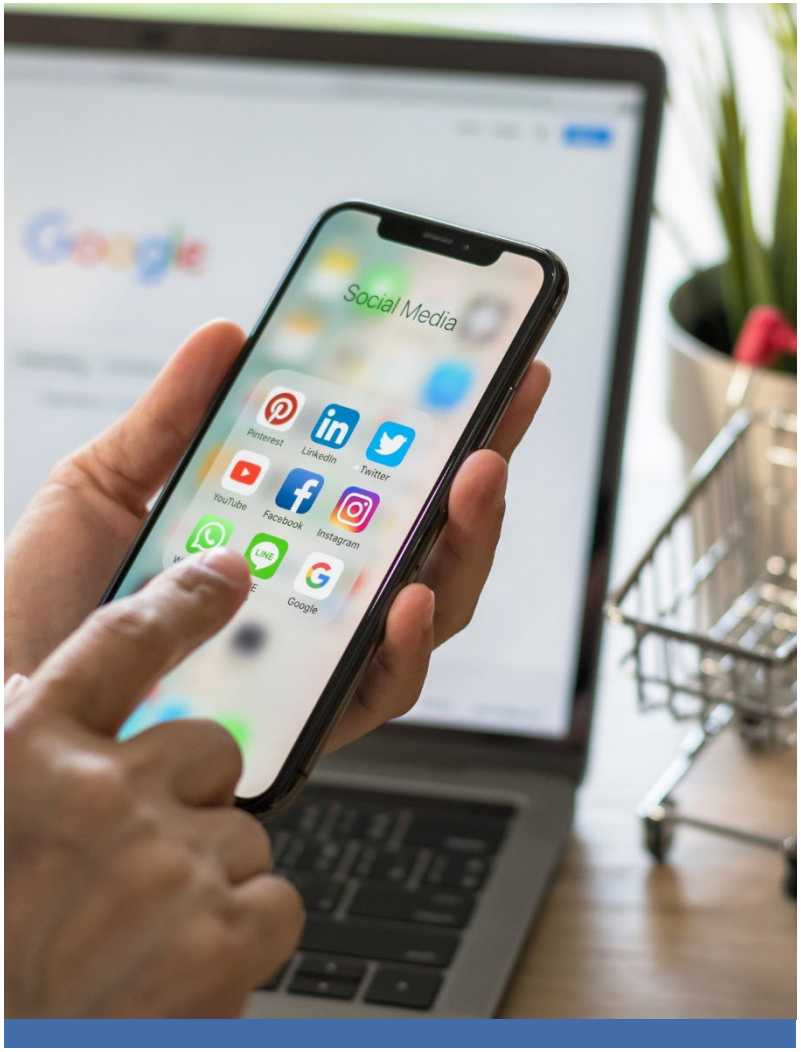
Online Privacy Bill

Proposed changes to the *Privacy Act 1988*

- In October 2021, the Attorney-General's Department released an exposure draft of the ***Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*** **(Online Privacy Bill).**

- The **Online Privacy Bill** aims to address:
  - the limitations of the *Privacy Act* in addressing the challenges posed by social media and online platforms; and
  - the need for strengthened penalties and enforcement mechanisms.

- Submissions on the Online Privacy Bill closed **on 6 December 2021**. The submissions and feedback received will shape the development of the Online Privacy Bill before it is introduced to Parliament.



Online Privacy Bill: Online Privacy Code

- At present, the Commissioner may register two kinds of binding privacy codes under the Privacy Act, namely, an **Australian Privacy Principle code** (**APP code**) and a **credit reporting code** (**CR code**).
- The Bill will require the Commissioner to put in place a third kind of privacy code, called the **OP code (online privacy)**, that will be binding on **OP organisations**, namely, those that provide social media services or data brokerage services, that operate a large online platform or that are otherwise specified.
- The OP code has not been drafted. However, the Bill sets out certain requirements that must be included in the OP code, such as:
  - Requiring OP organisations to take reasonable steps to **stop using or disclosing personal information** upon request from the relevant individual; and
  - **Stricter rules in relation to children** and other persons physically or legally incapable of giving consent. For example, social media services will need to take all reasonable steps to verify the age of users and to obtain the consent of a parent or guardian of a child under 16 (and take all reasonable steps to verify such consent).
- The Bill sets out various other matters that the OP code may address, including requiring large online platforms to report to the OAIC about the number of end-users they have in Australia.

Online Privacy Bill: Online Privacy Code

The Online Privacy Code will apply to **OP organisations**, which are **private sector organisations that are already subject to the Privacy Act**, and fall in one of the following categories:

1. Organisations providing social media services

An organisation that provides an electronic service that satisfies each of the following conditions:

(i) the **sole or primary purpose** of the service is **to enable online social interaction** between 2 or more end-users, including online interaction that enables end-users to share material for social purposes, but disregarding the following purposes:

(a) providing advertising material on the service; and

(b) generating revenue from the provision of advertising material on the service;

(ii) the service allows end-users to link to, or interact with, some or all of the other end-users;

(iii) the service allows end-users to post material on the service; and

(iv) such other conditions specified by the Minister.

2. Organisations providing data brokerage services

An organisation that collects personal information about an individual for the **sole or primary purpose of disclosing that information** (or information derived from that information) in the course of or in connection with providing a service (a ***data brokerage service***), and the information is collected by the organisation from the individual, or was previously collected by another organisation from the individual, by the use of an electronic service, other than a social media service described in 1 above.

3. Large online platforms

An organisation that had, in the previous year, at least **2,500,000 end-users in Australia** or, for an organisation that did not carry on business in the previous year, has in the current year at least 2,500,000 end-users in Australia, and collects personal information about an individual in the course of or in connection with providing access to information, goods or services (other than a data brokerage service) by the use of an electronic service (other than a social media service).

However, an organisation is not an **OP organisation** for the purposes of this section to the extent that the organisation collects personal information about an individual in the course of or in connection with providing a customer loyalty scheme.

4. Specified organisations

The Minister may also **specify conditions, organisations and classes of organisations that will and will not be OP organisations**, provided the Minister is satisfied that it is desirable in the public interest for the organisation, or organisations within the class, to be, or not to be, OP organisations. The Minister must also consult the Commissioner about the desirability of the decision.

Online Privacy Bill: Online Privacy Code

No Breach

An act or practice does not breach the registered OP code if:

- The OP organisation is a **contracted service provider for a Commonwealth contract** and the act or practice is required to meet an obligation in the contract;
- The act or practice involves the disclosure by an OP organisation of personal information in a record (as defined in the Archives Act 1983) **solely for the purposes of enabling the National Archives of Australia** to decide whether to accept, or to arrange, care (as defined in that Act) of the record; or
- The act is done, or the practice is engaged in, outside Australia and **is required by an applicable law of a foreign country**. However, the Bill will also remove the condition that an organisation has to collect or hold personal information from sources inside of Australia to be subject to the Privacy Act. This would mean that foreign organisations who carry on a business in Australia must meet the obligations under the Privacy Act, even if they do not collect or hold Australians' information directly from a source in Australia.

Online Privacy Bill: Penalties and Enforcement

There already exist a number of regulatory and enforcement powers available to the Commissioner under the Privacy Act. The Commissioner can, for example:

- direct an agency to provide the Commissioner with a **privacy impact assessment**;
- **conduct an assessment** of whether personal information is being maintained and handled by an entity as required by law;
- **direct an entity to notify individuals** at risk of serious harm, as well as the Commissioner, about an eligible data breach;
- **investigate and make a determination** on potential interferences with privacy, on the basis of a complaint or on the Commissioner's own initiative; and
- **commence proceedings** to enforce an enforceable undertaking, determination, seek an injunction or apply for a civil penalty.

Online Privacy Bill: Penalties and Enforcement

The Bill will strengthen the Commissioner's enforcement functions by:

- **increasing the maximum civil penalty** for a serious and/or repeated interference with privacy – for a body corporate, the maximum penalty will increase to an amount not exceeding the greater of:
    - $10,000,000;
    - three times the value of the benefit obtained by the body corporate from the conduct constituting the serious and repeated interference with privacy; or
    - if the value cannot be determined, 10% of their domestic annual turnover;
- **creating a new infringement notice** provision for failing to give information, answer a question or provide a document or record when required to do so as part of an investigation (with associated additional civil penalty provisions);
- **creating a new criminal penalty** for multiple instances of non-compliance by a body corporate;
- **expanding the types of declarations** that the Commissioner can make in a determination at the conclusion of an investigation;
- enhancing the Commissioner's capacity to **conduct assessments**; and
- **improving the Commissioner's information-sharing arrangements** with relevant enforcement authorities and enabling the Commissioner to disclose information in particular circumstances.

Other Pending Bills

Other Bills before the Commonwealth Parliament

- Individual states and territories have different protections in place, with some allowing personal information to be accessed for unrelated law enforcement purposes via a warrant, while other states and territories have prohibited it. The ***Privacy (COVID Check-in Data) Bill* 2021** seeks to prevent authorities from using personal data gathered from COVID check-in apps for enforcement-related activities. First reading before the House of Representatives took place on 25 October 2021.

- The ***Social Media (Basic Expectations and Defamation) Bill* 2021** aims to enable the minister to set basic expectations of social media service providers regarding the hosting of defamatory material on social media platforms, and ensures that service providers are liable for defamatory material hosted on their platforms which is not removed within a reasonable timeframe.
  - The Commissioner will have the power to obtain end-user identity information or contact details if the Commissioner believes that the provider of a social media service has such information and that such details are relevant to the operation of the Act.
  - The provider must comply with the above to the extent they are capable of doing so, if they do not, they face 100 civil penalty units.
  - First reading before the House of Representatives took place on 25 October 2021.

Privacy Act Review – Discussion Paper

Privacy Act Review – Discussion Paper

- On 25 October 2021, the same day the draft Online Privacy Bill was released, the **Attorney-General's Department** issued a discussion paper, seeking submissions on broader reforms to Australian privacy legislation. Submissions on the Discussion Paper closed on **10 January 2022**. Submissions and feedback received in response to the Discussion Paper will inform the review's final report.
- There is a long list of proposed changes, some of which will significantly impact how agencies and organisations handle personal information, and require reviews of privacy policies and privacy collection statements.
- Some noteworthy proposals include:

1. **Privacy Collection Notices**

- APP5 currently requires APP entities to take such steps (if any) **as are reasonable in the circumstances**, to notify individuals of certain matters at the time their personal information is collected or as soon as practicable thereafter.
- The Discussion Paper proposes that this notification become mandatory unless notification would be **impossible** or involve **disproportionate effort**.

3. Third Party Collection

- The Paper proposes a new requirement that where information is not collected directly from the individual then the APP entity must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP3. If requested by the individual, the organisation must also identify the source of such information unless that would be impossible or require disproportionate effort.
- Limitations on use and disclosure of personal information in the APPs often refer to the "primary purpose" and "secondary purpose" of collection. The Paper proposes that "primary purpose" be the purpose for the original collection ***as notified to*** the individual.
- The use or disclosure of personal information for the purpose of **influencing an individual's behaviour or decisions** must be a primary purpose notified to the individual when their personal information is collected.

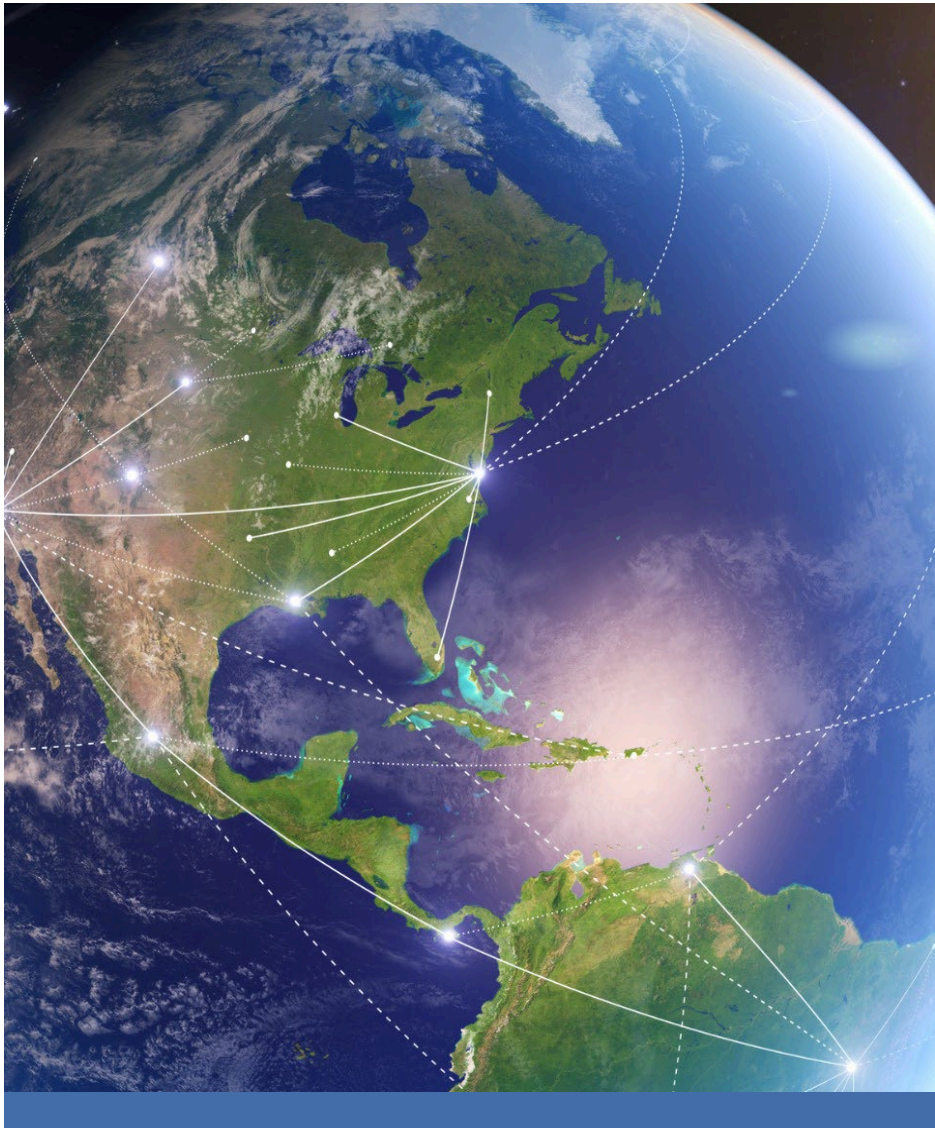
4. Consent

- Consent must be voluntary, informed, current, specific, and an unambiguous indication through clear action.
- Where a child is **under the age of 16**, consent must be provided by a parent or guardian.
- An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information.

Privacy Act Review – Discussion Paper

5. Overseas Data Flows

- APP8 currently requires that an entity may only disclose personal information overseas if it has taken reasonable steps to ensure the overseas recipient does not breach the APPs. One current exception is if the entity reasonably believes that the **overseas recipient is subject to comparable privacy laws**. It is proposed that a mechanism be introduced to **prescribe those countries**.
- Another exception is where the individual provides **informed consent** to the disclosure. It is proposed that this **exception be removed**.
- Make available **Standard Contractual Clauses** for transferring personal information overseas.
- Strengthen the transparency requirements to include **stipulating the countries** where recipients would be located as well as the **specific personal information** that will be disclosed.



6. Enforcement and Penalties

- Creating **tiers of civil penalty** provisions to give the OAIC more options.
- Create a **direct right of action** so that any individual whose privacy has been interfered with can bring an action in the Federal Court or the Federal Circuit Court.
- Introduce a **statutory tort of privacy**.

7. Restricted and Prohibited Acts and Practices

Option 1: APP entities that engage in a number of restricted practices with a high privacy risk or risk of harm to an individual must take reasonable steps to identify privacy risks and implement measures to mitigate those risks, for example:

- **Direct marketing**, including online targeted advertising on a large scale
- The collection, use or disclosure of **sensitive information**, **children's personal information**, or **location data** on a large scale
- The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software

Option 2: In relation to the specified restricted practices, **increase an individual's capacity to self-manage** their privacy in relation to that practice. Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted, or by ensuring that explicit notice for restricted practices is mandatory.

OVIC Audit

OVIC's Audit: Standard 2 – Information Security Value

- The Victorian Information Commissioner issued the **Victorian Protective Data Security Standards V2.0** in accordance with sections 86 and 87 of the *Privacy and Data Protection Act 2014* (Vic).
- The Office of the Victorian Information Commissioner (OVIC) recently audited the **Department of Treasury and Finance, Barwon Region Water Corporation, the Victorian Institute of Forensic Medicine and CenITex** and assessed their adherence to Standard 2 of the Victorian Protective Data Security Standards, which relates to information security, and the protection of information across the information life cycle from when it is created to when it is disposed or destroyed.
- The audit assessed each organization against the elements in Standard 2, and examined whether the organizations had accurately reported in their **2020 Protective Data Security Plans** to OVIC. The assessment was based on documentation provided by the organizations as well as interviews with personnel.
- The audit report was generally positive, with key outcomes as follows:
    - none of the audited organisation had an **Information Management Framework** that incorporated all security areas. While all the organisations had policies and procedures that dealt with security, none had a consolidated framework for managing security risks across all security areas (governance, information, personnel, ICT, and physical security);
    - three audited organisations have developed an **Information Asset Register** (IAR). One audited organisation is developing its IAR;
    - two audited organisations had developed contextualised **Business Impact Level** (BIL) tables to assist staff to assess the security value of information; and
    - two audited organisations apply protective markings.

Recommendation from OVIC's recent audit

Audit recommendations:

- **Recommendation 1** – Barwon Water, Cenitex, VIFM, and DTF to develop an Information Management Framework
- **Recommendation 2** – Barwon Water, Cenitex, VIFM and DTF review, validate and update the IAR at least annually
- **Recommendation 3** – Barwon Water, Cenitex, VIFM and DTF consult External Stakeholders
- **Recommendation 4** – Barwon Water, Cenitex, VIFM and DTF integrate the IAR into business processes
- **Recommendation 5** – VIFM and DTF develop and use a contextualised BIL table
- **Recommendation 6** – VIFM and DTF use contextualised BIL table to identify security attributes
- **Recommendation 7** – DTF review the organisation's IAR for inconsistent BIL ratings and protective markings
- **Recommendation 8** – Barwon Water and VIFM develop and implement the ability to protectively mark information
- **Recommendation 9** – Barwon Water to develop and implement information handling checklists
- **Recommendation 10** – Barwon Water and VIFM to embed aggregated security value management into existing or new policies or procedures.
- **Recommendation 11** –Barwon Water, Cenitex and VIFM strengthen the management and understanding of aggregated information assets.
- **Recommendation 12** – Barwon Water, Cenitex, VIFM and DTF develop comprehensive documentation (policies and processes), or strengthen existing policy or process, to support and promote the continual review of public sector information across the information lifecycle
- **Recommendation 13** – Barwon Water, Cenitex, VIFM and DTF create, or continue to develop, supporting process and guidelines for how personnel can manage the security value of externally generated information.

OAIC Investigation into 7-Eleven Stores Pty Ltd

- The Office of the Australian Information Commissioner (OAIC) recently initiated an investigation into 7-Eleven Stores collection of personal information via in-store tablets.
- Over a period of about a year in 2020/21, 7-Eleven deployed **facial recognition technology** in its stores as part of a customer feedback mechanism. A **tablet device** located inside the respondent's stores enabled a customer to complete a voluntary survey about the customer's in-store experience but each tablet also had a built-in camera that took facial images of a customer as they completed the survey. The purpose for capturing facial images and generating faceprints was to **detect if the same person was leaving multiple responses to the survey**. It also enabled 7-Eleven to have a broad understanding of the **demographic profile** of customers who completed the survey.
- The Commissioner was satisfied that the facial images and faceprints constitute **"biometric information that is to be used for the purpose of automated biometric verification or biometric identification"** and **"biometric templates"** and therefore "sensitive information" under the Privacy Act, requiring consent for collection.
- The stores had notices at the entrance stating **"Site is under constant video surveillance. By entering the store you consent to facial recognition cameras capturing and storing your image."**
- The 7-Eleven Privacy Policy also noted **"7-Eleven may also collect photographic or biometric information from users of our 7-Eleven App and visitors to our stores, again, where you have provided your consent. 7-Eleven collects and holds such information for the purposes of identity verification."**

OAIC Investigation into 7-Eleven Stores Pty Ltd

- The Commissioner held that **consent could not be implied** in these circumstances, because:
  - There was **no information provided on or in the vicinity of the tablet**, or during the process of completing the survey, about the respondent's collection of facial images and faceprints;
  - The **Store Notices were unclear**, and, given the prevalence of these kind of notices in stores and public places, may have created an impression that the respondent captured customers' images using a facial recognition CCTV camera as part of surveillance of the store; and
  - The respondent's **Privacy Policy did not link** the collection of photographic or biometric information to the use of in-store 'feedback kiosks'.
- Accordingly, the OAIC found that 7-Eleven Stores had interfered with the privacy of individuals whose facial images and face prints it collected through its customer feedback mechanism within the meaning of the *Privacy Act* by:
  - collecting those individuals' sensitive information **without consent**, and where that information was not reasonably necessary for the respondent's functions and activities, in breach of Australian Privacy Principle (APP) 3.3; and
  - **failing to take reasonable steps to notify individuals** about the fact and circumstances of collection and the purposes of collection of that information, in breach of APP 5.

OAIC investigation into Clearview AI, Inc.

- The OAIC and the UK's Information Commissioner's Office (ICO) opened a joint investigation into the personal information handling practices of Clearview AI Inc in July 2020.
- The investigation concerned Clearview AI's **facial recognition tool**, which includes a database of more than three billion images taken from social media platforms and other publicly available websites. The tool allows users to upload a photo of an individual's face and by using the biometric information collected by Clearview, find other facial images of that person collected from the internet. It then links to where the photos appeared for identification purposes.
- The Commissioner found that Clearview AI breached the Privacy Act by:
  - collecting Australians' sensitive information without consent;
  - collecting personal information by unfair means;
  - not taking reasonable steps to notify individuals of the collection of personal information;
  - not taking reasonable steps to ensure that personal information it disclosed was accurate, having regard to the purpose of disclosure; and
  - not taking reasonable steps to implement practices, procedures and systems to ensure compliance with the Australian Privacy Principles.
- The determination orders Clearview AI to cease collecting facial images and biometric templates from individuals in Australia, and to destroy existing images and templates collected from Australia.

OAIC investigation into Clearview AI, Inc.

- Clearview AI is appealing the decision based on the argument that the images were published in United States, outside Australia's jurisdiction.
- The OAIC also recently finalised an investigation into the **Australian Federal Police's** trial use of the technology and whether it complied with requirements under the Australian Government Agencies Privacy Code to assess and mitigate privacy risks.
- The Commissioner determined that the Australian Federal Police **failed to comply with its privacy obligations** in using the Clearview AI facial recognition tool.
- Commissioner Falk found the AFP failed to complete a **privacy impact assessment** (PIA) before using the tool, in breach of clause 12 of the **Australian Government Agencies Privacy Code**, which requires a PIA for all high privacy risk projects.
- The AFP also breached Australian Privacy Principle (APP) 1.2 by failing to take reasonable steps to implement practices, procedures and systems in relation to its use of Clearview AI to ensure it complied with clause 12 of the Code.

Q&A – Your Russell Kennedy Contacts

Gina Tresidder
Special Counsel

P: +61 3 8602 7243
E: GTresidder@rk.com.au

Sarah Manly
Principal

P: +61 3 9609 1691
E: SManly@rk.com.au

Feedback

Scan this QR code to provide instant feedback on the session.

Russell Kennedy Lawyers

Russell Kennedy Pty Ltd
info@rk.com.au
russellkennedy.com.au

Melbourne
Level 12, 469 La Trobe Street
Melbourne VIC 3000
PO Box 5146
Melbourne VIC 3001 DX 494 Melbourne
T +61 3 9609 1555 **F** +61 3 9609 1600

Sydney
Level 6, 75 Elizabeth Street
Sydney NSW 2000
Postal GPO Box 1520
Sydney NSW 2001
T +61 2 8987 0000 **F** +61 2 8987 0077