INDUSTRY FOCUS: AIRPORTS AND THE POTENTIAL DANGERS OF FACIAL RECOGNITION TECHNOLOGIES

DECEMBER 2019

With rapid improvements in technologies for digital facial recognition, movement tracking and sensing, a passenger will soon be able to walk through the doors of an airport and onto a flight with barely a pause. Technologies of this nature rely on high volume collection, processing and sharing of information about passengers, much of which is classed as sensitive in Australia under the *Privacy Act 1988* (Cth).

Despite the potential risks, trials of facial recognition systems for processing passengers have been happening at airports around the world, including Sydney and Canberra. These programs are often conducted by airlines in conjunction with government agencies. In Australia, the Commonwealth Government has proposed the *Identity-matching Services Bill 2019* (Cth) and the *Australian Passports Amendment (Identity-matching Services) Bill 2019* (Cth) to implement national facial recognition systems agreed by the Council of Australian Governments. Some States are reportedly already uploading driver licence photographs in anticipation of the passage of those laws.

In a world where data breaches seem all but inevitable, such data-intensive and sensitive activities as digital facial recognition pose a particular risk. For example, in May 2019, United States Customs and Border Protection reportedly admitted that photographs of individuals it held had been stolen. The recent rejection of the Commonwealth's facial recognition laws by the Parliamentary Joint Committee on Intelligence and Security, citing lack of safeguards and oversight, emphasises these concerns.

What are the likely repercussions of a breach of the data an airline or airport collects, holds and uses for facial recognition systems? In this article, we consider the probable outcomes, and suggest a checklist for mitigating the risks.

NOTIFICATION

Consider the following scenario: an airport's IT department reports to management that there has been unauthorised access to its information systems by an unidentified external actor. It quickly becomes apparent that the information includes facial recognition data used to identify, verify and track individual passengers as they move through the airport, along with associated key identification information such as passport details.

In such circumstances, aside from involving the police and immigration authorities, the airport will need to consider the application of the Notifiable Data Breach regime under Part IIIC of the Privacy Act. The regime requires that an entity notify individuals and the Office of the Australian Information Commissioner (**OAIC**) in the event of an 'eligible data breach', that is, where:

- There has been unauthorised access to or disclosure of personal information;
- This situation is likely to result in serious harm to the relevant individuals; and
- The entity has not been able to prevent the likely serious harm.

The Privacy Act dictates the issues to be considered when assessing the likelihood of serious harm. Looking at our scenario, 'biometric information' is not defined in the Privacy Act, but generally refers to features of an individual's face, fingerprints, iris, palm, signature or voice, clearly encompassing digital facial recognition data. Biometric information and biometric templates (that is, the reference points used by facial recognition systems to perform identity matching) are sensitive information for the purposes of the Privacy Act, and may be used to infer other sensitive information including in relation to health and race. The sensitivity of the information, taken together with

the fact that a person's face is generally immutable and the potential for sophisticated identity theft using such information, suggests that serious harm is likely.

The potential for serious harm may be mitigated, for example, if the airport had implemented strong encryption and other security measures in respect of the information that would render it impossible to use by the unauthorised actor. There may also be remedial measures available, depending on the particular circumstances.

Assuming that no mitigating or preventative factors apply, the airport will be required to notify the affected individuals and the OAIC as soon as practicable of:

- The entity's name and contact details;
- A description of the data breach;
- The kinds of information involved; and
- Recommendations about the steps individuals should take in response to the data breach.

However, before doing so, the airport will need to take into account third parties which may also be connected with the affected data. For example, if the airport obtained the biometric data from an airline, both entities may be subject to notification requirements, and will need to work together to respond appropriately. The OAIC's guidance publication *Data breach preparation and response* suggests that, generally, the entity with the most direct relationship with the affected individuals should notify. In this example, this would likely be the airline, however this means the airline has ultimate control over the details of the notification, including how it is made and what is included. The airport might have differing views to the airline on these points, but in the absence of any specific agreement around handling of these matters, does it have the right to insist on them? Also, if one or both of the involved entities has data breach insurance, the insurers will probably insist on determining which entity is primarily responsible for the breach.

The airport will also need to consider its international regulatory context. If any of the biometric data originated in another jurisdiction, the airport may need to comply with privacy regulation in other jurisdictions. For example, data collected from European passengers may be subject to the GDPR, which has different data breach notification requirements, including a fixed 72-hour notification period.

REPUTATION AND REGULATORY RISKS

Notification is, by its nature, a public process. Although any additional supporting information supplied voluntarily to the OAIC is treated as confidential, information provided to individuals becomes part of the public domain. There is a strong chance any data breach will attract media attention, and scrutiny is likely to be more severe where an entity's privacy practices are found wanting.

For example, to extend our hypothetical:

- The airport hasn't prepared for a data breach and fails to respond for the first few days. Senior managers scramble to decide who needs to be involved, and then determine a path forward. The OAIC directs the airport to make the requisite notifications. It also points to the recommendations in its data breach preparation and response guide for entities to have a detailed data breach response plan for eventualities such as this. The airport's failure to adequately respond to the breach compounds the public relations problem.
- Affected passengers take to social media to complain that they hadn't realised their biometric data was being collected by the airport, let alone consented to its collection or use. Phrases such as 'big brother' and 'social

credit' are used in viral posts naming the airport. A few people reflect that they had wondered why the airport convenience store seemed to know where they were travelling to without them having said anything. Apparently the airport's collection statement in this regard amounted to a line of fine print at the bottom of the posters informing passengers lining up for security screening what items are prohibited. The collection statement clearly does not satisfy the requirements of Australian Privacy Principle (**APP**) 5, drawing further criticism from the regulator. The OAIC also queries how the airport purports to have satisfied the consent requirements for collection of sensitive information under APP 3.4.

- The business tries to fend off criticism by blaming one of its service providers. A weakness in the service provider's security protocols has been identified as the front door for the attack. Unfortunately, leaked information soon makes it obvious that the airport had undertaken little to no due diligence on the service provider, which has a history of various other security incidents. Moreover, the service provider had failed to encrypt the data as it was supposed to under its contract with the airport. The airport was unaware of this contractual breach as it had not conducted any audits of the service provider's performance.
- A passenger emails a complaint, copying the OAIC, saying she had called the airport's customer service centre several months previously to ask what biometric data the airport held about her. Apparently the representative told her that only the airlines collect and hold biometric data, not the airport. The passenger (who is, incidentally, a well-connected privacy advocate) says she will report this breach of the Privacy Act to the regulator. In light of soon-to-be increased penalties for serious or repeated breaches of the Privacy Act, and the other breaches mentioned above, this may constitute a material risk for the business.[1]

PREPARATION

Airlines and airports can mitigate outcomes such as these by following the OAIC's recommendation to conduct a privacy impact assessment, particularly for complex projects involving broad or highly sensitive information.

A privacy impact assessment for the introduction of facial recognition technologies by an airport would involve:

- Describing the flow of personal information from passengers and other airport users to the airport (whether directly or via other intermediaries), between the airport and its partners and service providers or government agencies;
- Analysing how the collection and each proposed use and disclosure of the biometric data - for example, to government authorities, advertisers, other businesses operating within the airport - might impact on the privacy of passengers;
- Identifying options for minimising any risks of negative privacy implications for passengers; and
- Designing the implementation of facial recognition around considerations to enhance privacy, such as encryption.

This process could also incorporate an assessment of the impact of the business' facial recognition plans in light of other regulatory regimes. For example, how will the business prevent biometric data being used for racial or other profiling in contravention of discrimination legislation? How will the airport respond to requests from law enforcement for information which may assist with investigations unrelated to the airport's activities?

A privacy impact assessment should ideally be regarded as a living document. Adopting it as a tool to guide the business in implementing a facial recognition project could also double as a key risk management strategy for privacy and other regulatory risks.

CHECKLIST

Airports should follow these steps in preparing to introduce facial recognition technologies:

- Undertake a privacy impact assessment to identify the potential negative implications of the business' plans to introduce facial recognition, focusing in particular on interfaces with other entities and international jurisdictions;
- Put in place effective practices to manage any risks identified as part of the privacy impact assessment, as well as legal requirements:
  - Check your entity's privacy policy;
  - Update or draft a new collection statement for the purposes of collecting biometric information;
  - Create a data breach response plan, including identifying the specific individuals in the business who will be part of the response team;
  - Undertake thorough due diligence on any third parties which will be involved in collecting or handling biometric data, and implement active audits and other controls throughout the period of those relationships;
  - Identify and understand regulatory obligations to law enforcement, government agencies and international privacy regulators; and
  - Consider taking out a data breach insurance policy - or reviewing any existing policy.
- Be ready to respond quickly to any breach that comes to the attention of the business, including assessing whether notification to individuals and/or the OAIC is required.

HWL Ebsworth has extensive experience assisting businesses comply with their privacy obligations. Please contact a member of our team for further information on how we can assist you.

[1] See our article 'Australia the latest jurisdiction having a privacy law shake-up' from 29 March 2019: https://hwlebsworth.com.au/australia-the-latest-jurisdiction-having-a-privacy-law-shake-up/

This article was written by Luke Dale, Partner and Nikki Macor Heath, Senior Associate.

CONTACT *US*

For more information about how we can assist your business please contact one of the authors.

LUKE DALE
PARTNER, ADELAIDE
P +61 8 8205 0580
M 0412 956 566
E lcdale@hwle.com.au

NIKKI MACOR HEATH
SENIOR ASSOCIATE, ADELAIDE
P +61 8 8205 0515
E nmacorheath@hwle.com.au