Between 7 and 11 Lessons You Can Learn from the Latest OAIC Privacy Case

Anna Johnston, Principal, Salinger Privacy, tells us why a case involving facial recognition technology and customer satisfaction surveys offers plenty of lessons in how privacy law applies to Australian businesses.

In June 2020, the 7-Eleven chain of convenience stores began using a new customer feedback survey system in 700 stores across Australia. Each store had a tablet device which enabled customers to complete a voluntary survey about their experience in the store. Each tablet had a built-in camera that took images of the customer's face as they completed the survey.

Those facial images were stored on the tablet for around 20 seconds, before being uploaded to a server in the cloud. A third party service provider converted each facial image to a 'faceprint', which is an encrypted algorithmic representation of the face. The faceprint was used to infer information about the customer's approximate age and gender. The faceprint was also used to detect if the same person was leaving multiple survey responses within a 20 hour period on the same tablet; if multiple responses were detected, they were excluded from the survey results.

In other words, the company was using a facial recognition technology on its customers, to prevent its employees gaming a customer satisfaction survey by leaving multiple positive survey responses about their own performance. At least 1.6 million survey responses were completed. It is not known how many unique customers this represents.

The Office of the Australian Information Commissioner (**OAIC**) launched an investigation, and on 14 October published the final **determination by the Privacy Commissioner** Angelene Falk. Falk found that 7-Eleven had breached APP 3.3 by collecting 'sensitive information' (namely, biometric templates) unnecessarily and without consent; and APP 5 by failing to provide proper notice.

The implications of this case extend beyond just the use of facial recognition technology, and offer salient lessons for organisations of all shapes and sizes.

Here are my top takeaways for businesses:

1. You can't contract out of your privacy obligations

You will be on the hook for what your tech provider is doing with your customers' data.

7-Eleven tried arguing that it had not 'collected' any personal information because the information stored in the cloud was handled by its service provider, and that it had no access to the data. The OAIC found that the retail company did 'collect' the personal information via its service provider, because the data was collected on behalf of 7-Eleven, and it had contractual control over the data.

The lesson here is that both you and your technology provider must comply with the Privacy Act.

2. You can't escape your privacy obligations by arguing that you couldn't identify anyone

Sometimes you just have to laugh. 7-Eleven argued that the facial images and faceprints were not 'personal information' because they were not used to identify, monitor or track any individual. But the whole *point* of facial recognition technology is to identify individuals, in the sense of being able to distinguish one person from another! (Otherwise, what was the tech vendor selling – photos for the fun of it?)

Further, its deployment in this case *was* to monitor individuals: to see if anyone was entering multiple survey responses within short spaces of time.

The OAIC made short shrift of 7-Eleven's claim, and found that the faceprints were 'personal information', because the facial images and the faceprints were 'about' individuals, who were 'reasonably identifiable'.

('Personal information' is defined in the Act to mean: "information or an opinion about an identified individual, or an individual who is reasonably identifiable".)

3. You can invade someone's privacy without knowing who they are

If your service provider can identify individuals, then in law so can you. No hiding behind your tech vendor; you're handling personal information.

Your data is not to be considered in a vacuum; the test is whether it is possible to identify an individual "from available information, including, but not limited to, the information in issue" (at [37]). If your data can be linked to other available data to identify someone, you're handling personal information.

The test for identifiability is not whether or not you can figure out a person's name or legal identity; it is whether one individual can be "distinguished from other individuals" (at [38]). If your system can single out people to interact with them at an individual level, you're handling personal information.

4. The collection of any type of personal information, no matter how benign, must be reasonably necessary

Under APP 3, collecting personal information because it will be "helpful, desirable or convenient" is not enough (at [58]); your collection of personal information must be "reasonably necessary" for one of your organisation's "functions or activities".

The OAIC in this case formulated this test as involving consideration as to whether the impact on individuals' privacy is "proportionate to a legitimate aim sought" (at [59]). While the OAIC noted that "implementing systems to understand and improve customers' in-store experience" (at [102]) was a legitimate aim of the business, the collection of biometric templates was not a proportionate way to achieve that aim.

In other words, the risk posed to the individuals must be weighed against the business objectives, and serious consideration must be applied to determining whether those objectives could be achieved in a less privacy-invasive manner.

Is using facial recognition to infer age and gender a proportionate response? No; as the OAIC noted, if such data was necessary 7-Eleven could have simply asked for age range and gender as part of the survey questions. (Which reminds me: sometimes you don't need to know about gender at all.)

Is using facial recognition a proportionate response to the desire to improve the accuracy of a customer satisfaction survey? The OAIC said no: "Any benefit to the respondent was disproportionate to, and failed to justify, the potential harms associated with the collection and handling of sensitive biometric information" (at [105]).

5. Plus if it is sensitive information, you also need consent

In addition to the 'reasonably necessary' test, if the personal information you want to collect is in a sub-category known as 'sensitive information', under APP 3.3 you will also need the consent of the individual. Sensitive information includes biometric information and biometric templates, as well as information about a person's health or disability, ethnicity, religion or sexuality, amongst other categories.

While consent may either be express or implied, the OAIC noted that generally speaking, when seeking to collect 'sensitive information', organisations should aim for *express* consent, given the greater privacy impact which could arise from the handling of these special types of data.

6. A valid consent is hard to get

All stores had a notice outside with an image of a surveillance camera. Some of the notices also had text next to the image, which said "By entering the store you consent to facial recognition cameras capturing and storing your image".

The 7-Eleven Privacy Policy said "By acquiring or using a 7-Eleven product or service or providing your personal information directly to us, you consent to 7-Eleven collecting, storing, using, maintaining and disclosing your personal information for the purposes set out in this Privacy Policy".

So 7-Eleven argued to the OAIC that "if a customer did not consent to the use of this technology, the customer could elect to not enter the store or not use the tablet".

Yeah, they really said that.

(By the way, by reading this article, you consent to give me a million dollars, which I may or may not have spelled out in another document you probably did not see before you began reading this article. What, not happy? You were completely free to not read this article, what's your problem?)

Except that's not the way consent works in privacy law.

As formulated by the OAIC, the four key elements which are needed to obtain a valid consent are:

- The individual must be adequately informed before giving consent
- The individual must give consent voluntarily
- The consent must be current and specific; and
- The individual must have the capacity to understand and communicate their consent.

So let's spell this out.

Consent is the 'would you like sauce with that?' question. The question must be very specific about what is being proposed, the question must be asked about only one thing at a time, and the customer must be free to say yes or no (or say nothing, which means 'no'), and *still get their sausage roll*.

Entering a store does not mean your customer consented to you collecting their personal information.

Answering a survey does not mean your customer consented to you collecting their personal information.

And importantly, your Privacy Policy is not a tool for obtaining consent. Also, your Privacy Policy is not magic. It cannot authorise a company to do anything that the privacy principles don't already allow. A Privacy Policy is solely there to inform people, in general terms, how your organisation handles personal information.

No surprise, the OAIC found that customers' consent could not be implied by 7-Eleven.

7. That lame sign in the window is not a collection notice

APP 5 requires organisations to take reasonable steps to notify people about the collection of their personal information – the who, what, when, where, how and why – at or before the time of the collection. (Offering a clear notice also happens to help you meet the 'informed' element of consent, as mentioned above. But you need to give notice *regardless* of whether you are also seeking consent for something.)

7-Eleven had signs at the entry to its shops, only some of them with text. Even those with text did not explain that facial recognition would be used on customers answering the survey. Even astute customers could have understood the signage to be about CCTV security cameras, not cameras on the tablets used for the customer satisfaction survey.

The OAIC found the signs insufficient to meet the requirements of APP 5, and noted that an easy approach to notice could have been taken: 7-Eleven "should have included a collection notice on, or in the vicinity of, the tablet screen. The collection notice should have notified customers … before the start of the survey, and crucially, before the first facial image of the customer was captured. This was a practical and cost-effective step that the respondent could reasonably have taken in the circumstances, to draw customers' attention to the collection of their sensitive biometric information and the purpose of that collection".

The lesson here: don't let your big tech spend be undone by the failure to include a cheap solution to your privacy notice obligations.

8. Taking a casual approach to using new tech is a legal risk

Companies need to be finely attuned to the risks that come from collecting personal information without care. 'Move fast and break things' should not be your mantra. A finding that there has been an unlawful collection by a retailer of biometric information about Australians at a large scale should cause company boards and Audit & Risk committees to ask questions about their own data practices.

And facial recognition technology? Well, that's a whole other world of pain and risk.

When facial recognition technology is attracting calls for a moratorium, or stricter regulation, and when a Bill to use the technology for law enforcement can't even get through Parliament because it is so controversial, and when some vendors of the technology are even re-thinking its use, and when the technology is criticised by the computer science profession for its problems with racial and gender bias, maybe don't go around casually implementing facial recognition software for trivial purposes.

Just… don't.

9. Do proper risk assessments

One of the most striking aspects of this case is that 7-Eleven was only one month into its rollout of the new technology when the OAIC began making preliminary inquiries about the company's compliance with the law. Yet the retailer continued with the program for another 13 months before pulling the plug, just before the Privacy Commissioner made her final determination.

That's some pretty brave risk-taking.

The OAIC noted that a better approach would have been to conduct a Privacy Impact Assessment in advance of the program starting, which could have identified "options for avoiding, minimising or mitigating adverse privacy impacts (including by identifying potential alternatives for achieving the goals of the project without collecting such information)", and "assisted in assessing the proportionality of collecting biometrics for the purpose of understanding customers' in-store experience" (at [103]).

Conclusion

So beware, organisations of all shapes and sizes – you have been put on notice by the OAIC. You can't hide behind your tech vendors.

You need careful, risk-based consideration of all projects which will collect or use personal information. The scope of what is regulated as 'personal information' is broad. Your collection must be reasonably necessary for a legitimate purpose, and you must be able to justify the potential harms to individuals as proportionate when measured against your business objective. Plus, if the personal information is one of the types of personal information defined as 'sensitive', you will also need an informed, voluntary, specific and current consent to collect it.

The days of "By entering our store/accessing this website you are consenting to whatever we put in our Privacy Policy" are over.

Contributions & Comments

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at: **clbeditors@gmail.com**