Australia stops use of facial recognition in a retail setting

A major Australian hardware chain breached several privacy principles when capturing faces of every individual on CCTV who entered its stores. By **Annelies Moens** of Privcore.

On 29 October 2024, the Office of the Australian Information Commissioner (OAIC) released its long-awaited determination[1] into the use of facial recognition technology (FRT) in Bunnings' stores. Bunnings is a major home and hardware retailer in Australia. The decision is relevant to all retailers with annual turnover greater than three million Australian dollars operating in Australia, as the Federal Privacy Act 1988 has extra-territorial application. The case highlights the importance of ensuring solutions or processes deployed to achieve a particular objective do not create a disproportionate level of privacy risk.

The Privacy Commissioner determined the collection of sensitive information through the FRT system was not necessary. The outcome of the decision is that Bunnings must not continue or repeat the practices the Privacy Commissioner found were in breach of the Privacy Act. Bunnings was also required to publish a statement[2] on its website setting out the decision – to be accessible for a year after publication. Bunnings is seeking a review of the Privacy Commissioner's decision before the Administrative Review Tribunal.

What happened

Bunnings Group Ltd (Privacy) [2024] AICmr 230 (29 October 2024)[3] is a seminal determination by the Office of the Australian Information Commissioner (OAIC) in that it outlines the steps to consider when deciding whether facial recognition technology (FRT) can be rolled out in retailer settings in Australia. Some information was redacted in the OAIC's published decision without providing reasons.

The OAIC's investigation into Bunnings commenced on 11 July 2022 and concluded with the publication of its long-awaited decision on 29 October 2024. In reaching the decision, the *Australian Privacy Principles Guidelines*[4] and the *OAIC Guide to Privacy Regulatory Action*[5] were taken into account.

Bunnings processed facial images of people entering 62 stores over a three-year period to match against a database containing (at its peak) 448 facial images of people whom it considered posed a risk to operations. Risks included individuals, who may impact the safety and security of others, as well as affect Bunnings' stock and facilities.

The FRT system involved the following four steps [para 25]:

1. Video decoding – each frame of the CCTV video was separated into still images.
2. Facial recognition processing – a Gabor filter was applied to each still image to determine whether it contained any images of human faces.
3. Facial feature calculation processing – where a human face was identified from a still image, vector points of the facial features were extracted to create a vector set (the biometric).
4. Comparison processing – each vector set was compared against vector sets previously extracted from the faces of individuals enrolled in the database by calculating the relative differences between the location of the vector points in each vector set.

Where step 4 resulted in a match, an alert was generated containing the information of the enrolled individual and the matched individual (including false positives). Bunnings advised non-matched facial images were automatically deleted within an average of 4.17 milliseconds. As such, its primary argument was it did not collect the personal information of non-matched individuals. The Privacy Commissioner determined there was a collection of the personal information of matched and non-matched individuals.

Bunnings had enrolled a relatively low number of individuals into the database (compared with the number of visitors to its stores). It enrolled people whom it deemed posed a risk to its operations. Bunnings appeared not to have a policy or guidance for the six relevant staff to determine whether to enrol an individual in the database to match against. It sourced facial images from its own CCTV system and state police.

Prohibition on the collection of sensitive information

APP 3.3 prohibits the collection of sensitive information (which includes biometrics), unless the individual consents to that collection or an exception in APP 3.4 applies. Bunnings sought to rely on APP 3.4(b) – that a permitted general situation under section 16A of the Privacy Act existed – in circumstances where it was found to have collected personal information. In particular, Bunnings argued it reasonably believed the collection of personal information was necessary:

1. For it to take appropriate action in relation to suspected unlawful activity, or serious misconduct that relates to its functions or activities; or
2. To lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

The Privacy Commissioner decided the following is relevant to determining whether the collection was necessary in the above exceptions [para 99]:

a) The suitability of the FRT system, including its efficacy in addressing the relevant activity or conduct.
b) The alternatives available to Bunnings to address the relevant activity or conduct.
c) Whether the use of the FRT system was proportionate, which involves balancing the privacy impacts resulting from the collection of sensitive information against the benefits gained by using the FRT system.

In relation to exception one above,

the Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 states at p.67: "The provision, by specifying that the unlawful activity or serious misconduct must relate to an entity's functions or activities, intends that the exception will apply to an entity's internal investigations." This is also reflected in the APP Guidelines and section 6 of the Act in relation to the definition of serious misconduct. As such, it would appear this exception relates to the processing of, for example, employees' personal information, not customer personal information. However, the Privacy Commissioner interpreted this exception broadly to allow the "unlawful activity" exception to apply to Bunnings' customers' personal information [para 107]. The Privacy Commissioner then considered the suitability, alternatives and proportionality points outlined above in relation to collection of sensitive information to take appropriate action to deal with suspected unlawful activity.

In relation to suitability of the FRT system, its effectiveness was predicated upon recidivism and not single acts of unlawful activity. In other words, a person had to be enrolled in the database. Further, enrolled individuals didn't know they were enrolled in the database, therefore it had no deterrent effect. Bunnings had considered a number of alternatives to address suspected unlawful activity. Unfortunately, the FRT system was the option which impacted the broadest cohort of individuals.

In terms of proportionality, the number of enrolled individuals in the database at its peak was 448 individuals. The Privacy Commissioner made the point that "of the significant volume of personal information collected via the FRT system, the respondent could only rely on the FRT system to take appropriate action in respect of unlawful activity on a relatively small number of occasions and in respect of a relatively small number of individuals" [para 144].

The Privacy Commissioner therefore determined the collection of sensitive information in relation to suspected unlawful activity through the FRT system was not necessary.

In relation to exception two above, in terms of suitability, in addition to the points raised above, the serious threat situations Bunnings was seeking to address could not be assisted by the FRT system, for example, someone wielding a weapon or someone wearing a face mask. Likewise, in terms of alternatives, the FRT system was the option which impacted the broadest cohort of individuals. In terms of proportionality, the FRT system, as with suspected unlawful activity, could only be relied upon to take appropriate action in respect of a relatively small number of incidents.

The Privacy Commissioner therefore determined the collection of sensitive information in relation to serious threats through the FRT system was not necessary.

Consent is another basis on which sensitive (biometrics) information can be collected. However, valid consent in these contexts is extremely difficult to obtain. The Privacy Commissioner, for completeness, found there was no consent from individuals for the collection of their personal information. "In order for consent to be valid, it must be informed, voluntary, current and specific, and given by individuals who have the requisite capacity" [para 85] and as outlined in B.38 of the APP Guidelines[6].

Notification of collection

The Privacy Commissioner also found it was reasonable for Bunnings to take steps under APP 5.1 to notify individuals of some or all of the matters outlined in APP 5.2. Further, the privacy notices displayed at entry points in stores did not meet the requirements of APP 5.2. The Bunnings' privacy notice shown between November 2018 and May 2021 at entries to stores indicated video surveillance was utilised. Bunnings considered it was unreasonable to expressly state it was using FRT in its privacy notice as it would undermine the efficacy of the FRT system. In fact, in the author's opinion, transparency would have increased the efficacy of the FRT system, as it would have provided a deterrent to some individuals behaving in ways Bunnings was trying to prevent. This type of strategy is seen in transparency reporting, adopted by some corporations such as, TradeMe[7] in New Zealand. TradeMe lists second hand goods for sale online and curbs the sale of stolen goods through its transparency reporting. The Privacy Commissioner supports this view in paragraphs 215 and 267 of the decision.

In its second privacy notice used between May and November 2021, Bunnings updated its notice to mention that "video surveillance, which may include facial recognition, is utilised".

None of Bunnings' company-wide privacy policies (which is a separate requirement to APP 5) mentioned its use of FRT, therefore Bunnings' breached APP 1.3.

The Privacy Commissioner determined Bunnings failed to notify individuals at or before the time of collection, or as soon as practicable after collection, of the collection of their sensitive information as required under APP 5.

Practice, procedures and systems

More broadly, the Privacy Commissioner found Bunnings had failed to meet the requirements of APP 1.2. This APP requires entities to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities to ensure the entity complies with the APPs, and will enable it to deal with inquiries or complaints from individuals about compliance with the APPs.

The Privacy Commissioner determined, in the circumstances, this necessitated the conduct of the following:

1. A Privacy Impact Assessment (PIA) prior to the implementation of the FRT system (or at the very least a privacy threshold assessment documenting the reasons why Bunnings believed a PIA was not necessary in the circumstances).
2. Written policies and procedures governing the use of the FRT system prior to its implementation.
3. Staff training for those receiving alerts from the FRT system and senior managers in stores using the FRT system.
4. Periodic review and reporting of privacy risks.

Prior to implementing the FRT system, Bunnings had obtained legal advice (which it did not share with the OAIC during the investigation), a

presentation delivered to senior management with passing reference to privacy, selection of a software product by considering its functionality against privacy risks, training by the biometrics vendor to the six staff using the FRT system to advise how to enrol individuals and perform back-ups. The Privacy Commissioner found the steps Bunnings took prior to implementation and during the operation of the FRT system did not meet the requirements of APP 1.2.

Conclusion

Biometrics carry high privacy risks as they involve unique data elements that are difficult to change if compromised (such as a face, iris or fingerprint).

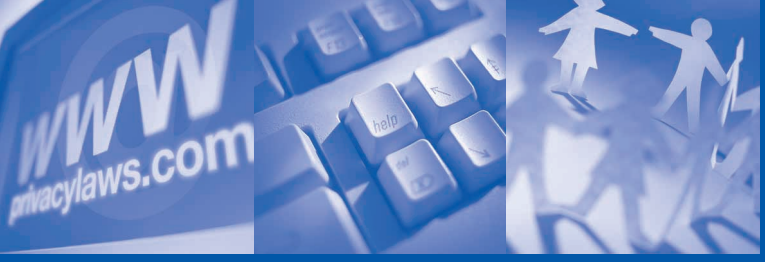
The Privacy Commissioner at paragraph 5 of the determination encourages "all APP entities to proactively consider whether and how their current and future acts and practices align with their obligations under the Privacy Act, particularly when those acts and practices involve the use of technology which may have an impact on the privacy of individuals. In particular, it may be prudent for APP entities currently deploying FRT to reassess their compliance with the Privacy Act in light of the guidance provided by this determination, including by, inter alia, undertaking a Privacy Impact Assessment."

AUTHOR

Annelies Moens is Managing Director at Privcore.
Email: moens@privcore.com

REFERENCES

1 www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2024/230.html
2 www.bunnings.com.au/about-us/facial-recognition-technology
3 www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2024/230.html
4 www.oaic.gov.au/__data/assets/pdf_file/0030/40989/app-guidelines-combined-December-2022.pdf
5 www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action
6 www.oaic.gov.au/__data/assets/pdf_file/0030/40989/app-guidelines-combined-December-2022.pdf
7 www.trademe.co.nz/c/trust-safety/transparency-reporting



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Non-material damages for data violations in Germany

Lea Stegemann of Noerr PartGmbB and **Jakob Horn** of Taylor Wessing LLP provide an overview of German case law on non-material damage claims.

The GDPR, with Article 82, explicitly introduced claims for non-material damages ("emotional damages") for data protection violations. In Germany, there are already thousands of court proceedings in which individuals claim non-material damages. Hence, data protection violations are increasingly being pursued not only by public but also by private enforcement, and claims for damages are becoming a

Continued on p.3

France: CNIL sanctions Orange with a hefty fine for ads appearing as emails

Zero-tolerance approach towards Orange's direct marketing practices. By **Nana Botchorichvili** of IDEA Avocats, France.

On 14 November 2024, France's Data Protection Authority (CNIL) issued a fine of €50 million against Orange, France's leading telecommunications operator, for displaying advertising messages in customer email inboxes without their prior consent[1].

Indeed, as part of its Internet, mobile and fixed phone services,

Continued on p.5

Issue 193 **FEBRUARY 2025**

INTERNATIONAL report

ISSUE NO 193 FEBRUARY 2025

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Nana Botchorichvili
IDEA Avocats, France

Jonathan Mendoza Iserte and Jesús Javier Sánchez García
INAI, Mexico

Sergio Maldonado
Privacycloud, US/UK

Lea Stegemann
Noerr PartGmbB, Germany

Jakob Horn
Taylor Wessing LLP, Germany

Roald Chao
International business law graduate, QMUL, UK

Annelies Moens
Privcore, Australia

Xawery Konarski and Mateusz Kupiec
Traple Konarski Podrecki & Partners, Poland

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

"comment

Change gathers pace in 2025

The international privacy community has been surprised by news about a new Chinese open source AI large language model Deep Seek. According to the BBC, OpenAI says that Chinese and other companies are "constantly trying to distil the models of leading US AI companies". From the Deep Seek user perspective, the question is about data security.

US President Donald Trump's executive orders affect privacy in the US and elsewhere, for example terminating the membership of the Democratic members of the Privacy and Civil Liberties Oversight Board with immediate effect. At a conference in Brussels on Data Protection Day, 28 January, organised by the European Data Protection Supervisor, the Privacy Salon (CPDP) and the Council of Europe, Marina Kaljurand, 1st Vice-President of the European Parliament's LIBE Committee, declared in the context of the GDPR and the Law Enforcement Directive, this decision is "not what we expect from an ally." Irena Moozová, Deputy Director-General for Justice and Consumers at the European Commission added "the EU won't be shy to use provisions we have available."

The message from politicians and privacy advocates was loud and clear: the EU will retain and defend its privacy principles and values. The main EU-wide task is now to oversee the implementation of the EU Digital Services Package (p.27) of data related legislation and continue work on the GDPR to ensure more consistency in enforcement. Karolina Mojzesowicz of the EU Commission confirmed again that the GDPR will not be reopened – she stressed that "solutions are embedded in the GDPR itself" due to its flexibility. The regulation on procedural rules that is expected soon is an example of this type of adjustment.

While Mexico is abolishing its independent Data Protection Authority (p.8), privacy principles are becoming more firmly established elsewhere. Malaysia's Personal Data Protection Act has been strengthened to significantly increase the powers of the regulator and strengthen individuals' rights (p.20) and South Korea has adopted an AI law (p.14).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked in advance of the free-place deadline. Excludes the Annual Conference. More than one place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

"An indispensable resource for anyone who has a serious interest in privacy, combining latest news with thoughtful commentary and analysis."

Richard Cumbley, Partner, Linklaters

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.