February 2026

# UPDATE

## Bunnings Appeal Decision and Developments to Watch in 2026

**New Privacy Law: Bunnings Appeal Decision**

The Administrative Review Tribunal (Guidance and Appeals Panel) decision in *Bunnings Group Limited and Privacy Commissioner [2026] ARTA 130 (4 February 2026)* overturns the Privacy Commissioner's view regarding when sensitive information can be collected without consent and materially reshapes how "generally permitted situations" may justify biometric data collection without consent.

While the Tribunal expanded the scope of lawful collection, signalling a more scope for organisations to deploy surveillance or AI-enabled security tools, any such proposed use must be described in the organisations privacy policy (APP 1) and reasonable steps take to notify each data subject (APP 5).

Bunnings had implemented a facial recognition technology (**FRT**) which momentarily collected facial recognition data in order to identify individuals who had previously stolen or engaged in violent or threatening acts within store premises. Biometric data is sensitive information under the Privacy Act. APP 3.3 requires express consent for collection of sensitive information unless an exception applies.

Bunnings argued that the collection was permitted under the exception in 3.3 (b) as a "generally permitted situation" (**GPS**). In particular either because:

- it was unreasonable or impractical to obtain consent and Bunnings reasonably believed the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (**GPS 1**).
- it had reason to suspect that unlawful activity, or misconduct of a serious nature, reasonably believed that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter (**GPS 2**).

These are two of the GPSs described in s16A of the *Privacy Act 1988*.

In the Commissioner's decision: *Commissioner Initiated Investigation into Bunnings Group Ltd (Privacy) [2024] AICmr 230 (29 October 2024)* (the subject of the appeal), the Commissioner found that a generally permitted situation did not exist under:

- GPS 1 because, although Bunnings had a "suspicion" of unlawful activity, the collection was not necessary to take "appropriate action" because of the disproportionate privacy intrusion and the availability of other methods; nor
- GPS 2 because , although Bunnings faced serious threats, the collection was not necessary to "lessen or prevent" them. Many serious threats (e.g., a one-off violent outburst) would not be prevented by FRT, and the mass collection of data was an excessive response to the specific threats identified.

The Tribunal found that the two generally permitted situations did apply because, in summary:

1. Bunnings held a "reasonable belief" that collecting sensitive information via FRT was "necessary" to take appropriate action against retail crime and violence.

- FRT helped identify repeat offenders and that its introduction was associated with a reduction in theft and improved feelings of safety among staff. Identifying known offenders allowed Bunnings to be proactive rather than reactive; and
- there were no comparable alternatives for identifying repeat offenders.

2. The use of FRT was proportional relative to the intrusion on privacy because:
   - The system held sensitive information (facial vectors) for approximately 4 milliseconds in the server's Random Access Memory;
   - Data for non-matched individuals was permanently deleted immediately after processing and
   - The risk of misuse or cyber-attack was considered "negligible".
3. the high levels of violent verbal and physical abuse, threats with weapons, and organized theft committed by repeat offenders constituted "unlawful activity" and "serious threats" that Bunnings had a valid reason to suspect and address**.**

The Tribunal affirmed the Commissioner's findings that Bunnings breached APP 5.1 (inadequate notice) and APP 1.2/ APP 1.3 (privacy governance and privacy policy). Even though Bunnings was entitled to use the FRT to collect sensitive information without consent it was a breach of the APPs by not including information about the practice in its Privacy Policy and not taking additional steps to ensure that relevant data subjects were informed as required by APP 5.1.

The Tribunal's decision represents a clarification of the law regarding the circumstances in which FRT might be deployed in order to ensure public safety and/or protection of assets.

---

**Key Regulatory Developments Affecting Digital Platforms and Telecommunications in 2026**

**1. The *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025***

This new law is likely to pass in early 2026 (Currently before the House of Reps). This law will create a Carriage Service Provider (CSP) registration scheme, giving ACMA clearer visibility of market participants and new enforcement levers, introduce direct enforceability of telecommunications industry codes and expand penalty and infringement notice powers.

Once implemented, registration as a CSP will be required for all carriage service providers. Licensed carriers are prevented from supplying carriage service for resale to unlicensed entities. Compliance with codes and customer-facing obligations will carry materially higher regulatory risk.

**2. Scam Prevention Framework –becoming operational**

The Scam Prevention Framework (SPF) is law and applies initially to telecommunications providers, banks and digital platforms.

Key features include:

- Mandatory governance, prevention, detection, disruption and response obligations.
- Information-sharing and "safe harbour" protections when taking reasonable steps to disrupt scams.
- Potential civil penalties and compensation orders for non-compliance.

The SPF shifts scams from a voluntary cooperation model to a regulated, enforceable framework. The law will be implemented on the coming into force of Ministerial Designation Instrument. consultation on the draft instrument closed on 4 January 2026 Regulators are expected to clarify

expectations around what constitutes “reasonable steps”, with increasing focus on cross-sector coordination.

**3. SMS Sender ID Register – mandatory verification regime commencing 1 July 2026**

The SMS Sender ID Register is now established in law as part of the Commonwealth’s anti-scam reforms, introducing a mandatory verification framework for alphanumeric sender IDs used in SMS messaging. The regime is designed to prevent impersonation scams by restricting the use of branded sender IDs to verified entities and shifting scam prevention obligations toward telecommunications infrastructure providers.

Implementation is proceeding on a staged basis:

- On 30 November 2025, the Sender ID Register opened for industry onboarding and registration of legitimate sender IDs.
- On 1 July 2026 mandatory enforcement commences. From this date, telecommunications providers and messaging intermediaries must treat unregistered sender IDs as “Unverified,” with blocking, filtering or other mitigation measures expected under applicable industry requirements.

The regime has direct implications for carriers, carriage service providers, messaging aggregators and digital platforms:

- CSPs and intermediaries will be required to verify and manage sender IDs carried on their networks and implement controls designed to prevent spoofing and impersonation.
- Businesses using branded SMS communications (including authentication, onboarding, service notifications or marketing) must ensure sender IDs are registered through a participating provider ahead of commencement.
- Messaging supply chains — particularly arrangements with offshore aggregators — are likely to attract increased regulatory scrutiny.

The Sender ID Register operates alongside the Scam Prevention Framework and telecommunications consumer safeguard reforms, reinforcing a shift toward proactive, network-level scam disruption rather than reactive enforcement.

**4. Privacy reform – tranche one in force, tranche two still pending**

The second tranche of Privacy Act reforms is anticipated in 2026 including a wider definition of personal information, removal of the exception for small business, changes to the employee records exemption, a generally applicable “fair and reasonable” use and disclosure test, a right of erasure, a right of objection, a direct right of action, stricter requirements for obtaining consent, a right to control and/or opt out of targeted advertising, and mandatory privacy impact assessments for new products and services.

Automated decision-making transparency obligations requiring disclosure any use of personal information for automated decision making commence on 10 December 2026.

**5. Online safety reforms – age restrictions and new industry codes**

Significant online safety reforms are now taking effect:

- Age-based restrictions on social media accounts for under-16s commenced in December 2025, requiring platforms to take reasonable steps to prevent account creation and retention.

- A suite of registered Online Safety Industry Codes commences progressively from 9 March 2026, covering social media services, app distribution services, designated internet services and relevant electronic services.

Obligations extend beyond "traditional" social media platforms and may capture app stores, ISPs, device ecosystems and AI-enabled services, depending on service classification.

**6. Digital ID – expanding use cases and regulatory oversight**

The *Digital ID Act* is now operational, establishing a national framework for accredited Digital ID providers, relying parties using Digital ID services and oversight by the **ACCC** (with privacy regulation by the OAIC).

Digital ID is increasingly relevant to onboarding, fraud prevention, age assurance and scams mitigation, and may become a practical compliance tool across multiple regulatory regimes.

**7. Artificial intelligence – policy hardening without a single "AI Act"**

The Government's Responsible AI in Government Policy took effect in December 2025. A National AI Plan has been released, with an AI Safety Institute expected to commence operations in 2026. AI regulation is emerging through existing frameworks (privacy, consumer law, online safety, critical infrastructure).

Accordingly, AI compliance risk is distributed across regulators, requiring boards to adopt cross-regulatory governance models rather than treating AI risk as a standalone legal domain.

**8. Digital platform competition – momentum toward ex ante regulation**

In its final 2025 Digital Platforms Services Inquiry Report the ACCC included recommendations for a move towards ex-ante regulation including rules against, self-preferencing, tying and impeding interoperability, new economy-wide prohibition on unfair trading practices and strengthening of the prohibition on unfair contract terms..

Reform is likely to affect not only large platforms but also businesses that depend on, compete with, or integrate into platform ecosystems, including telecommunications providers. The Government has provided "in-principle" support with the Unfair Trading Practices laws and the Digital Competition Regime expected to be central pieces of legislation introduced or finalized throughout this year.

**9. Electronic Surveillance reform**

Work has been underway on the government's response to the 2020 Report: "Comprehensive Review of the legal framework of the National Intelligence Community" led by Dennis Richardson. The report recommended replacing large parts of the current electronic surveillance architecture with a single tech-neutral Act.

The Department has indicated this consolidation is intended to repeal and replace the *Telecommunications (Interception and Access) Act 1979*, the *Surveillance Devices Act 2004*, and parts of the *Australian Security Intelligence Organisation Act 1979* that deal with relevant powers. The objective is to create a clearer framework that supports law enforcement and intelligence access to information for serious crime and national security threats, while also protecting privacy and promoting transparency for agencies, oversight bodies, industry and the public. It appears that work on this important reform will progress this year.

**10. Minimum security standards for consumer smart devices – mandatory regime from 4 March 2026**

Mandatory baseline cyber security requirements for consumer-grade smart devices commence on **4 March 2026** under the *Cyber Security Act 2024 (Cth)* and associated Security Standards Rules. The regime introduces enforceable "secure-by-design" obligations for manufacturers and suppliers of internet-connectable consumer products supplied in Australia.

The rules apply broadly to consumer IoT devices (such as routers, cameras and smart home equipment) and require:

- elimination of universal default passwords and implementation of secure authentication controls;
- vulnerability disclosure mechanisms and defined minimum security support periods; and
- manufacturer statements of compliance confirming adherence to the prescribed standard.

The framework has extraterritorial reach and is supported by compliance notices, stop-supply directions and other enforcement powers. For telecommunications providers, digital platforms and enterprise purchasers, the regime is likely to drive stronger vendor assurance expectations and contractual controls around connected devices used in customer-facing services.

---

**Please contact me if you have any questions regarding the matters discussed in this update. patrick@patrickfair.com 0411361534. You can subscribe to updates like this one at www.patrickfair.com**