From: s47F
To: s47F ;s47F .s47E(d) @infrastructure.gov.au>
Cc: s47E(d) @esafety.gov.au; s47F ; s47F s47F s47F s47F
Subject: For redline feedback by 7/10: Draft OAIC guidance on Part 4A (Social Media Minimum Age) of the Online Safety Act 2021 [SEC=OFFICIAL:Sensitive]
Date: Friday, 3 October 2025 11:12:05 AM
Attachments: D2025 023149 20251003_OAIC SMMA Privacy Guidance_Draft_for interagency consultation.docx
Importance: High

OFFICIAL: Sensitive

Hi s47F and s47F ,

As foreshadowed, please find attached OAIC's draft guidance on Part 4A (Social Media Minimum Age) of the *Online Safety Act 2021*.

Apologies for the tight timeframes – we are seeking any redline feedback by **COB Tuesday 7 October**.

Thank you for working with us in bringing this together.

We look forward to receiving your feedback.

Kind regards,
s47F

s47F
Director, Privacy Reform Implementation
Office of the Australian Information Commissioner
Melbourne
P s47E(d) E s47E(d) @oaic.gov.au

Working remotely from Melbourne, Monday to Friday
The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.

Subscribe to Information Matters

Australian Government

Office of the Australian Information Commissioner

DRAFT - Privacy Guidance on Part 4A (Social Media Minimum Age) of the *Online Safety Act 2021*

1 October 2025 - DRAFT

OAIC

Contents

1. Key considerations

- **Part 4A of the *Online Safety Act 2021* operates alongside the *Privacy Act 1988* and Australian Privacy Principles.** Part 4A introduces additional, more stringent obligations on age-restricted social media platform providers and third-party age assurance providers when handling personal information for social media minimum age (SMMA) compliance purposes. These providers are collectively described as 'entities' in this guidance.
- **When choosing or offering an age-assurance method (or combination of methods) ensure it is necessary for SMMA compliance purposes and proportionate to the legitimate aim of preventing age-restricted users from having accounts**. Consider alternate methods and how you can use low-intrusion techniques within an age assurance method(s). Escalate to more intrusive personal information handling only as necessary.
- **Take a privacy by design approach** and consider the privacy impacts associated with each age assurance method (e.g. inference, estimation and verification) and whether the circumstances surrounding the specific chosen method(s) justify the privacy risks.
- **Undertake a privacy impact assessment (PIA) when choosing an age-assurance method(s)** to identify potential privacy impacts at the outset and implement recommendations to manage, minimise or eliminate them. This will assist to ensure that a privacy by design approach is embedded from the start.
- **Minimise the inclusion of personal and sensitive information in age assurance processes**. Only retain enough personal information in outputs to meet defined purposes, such as to explain the measures implemented for a user and to facilitate reviews or complaints, then destroy on schedule.
- **Using personal information that was originally collected for a non-SMMA purpose (e.g. age inference) does not, by itself, put that information within the remit of s 63F of Part 4A.** Existing personal information used for age assurance does not need to be destroyed where the original purposes are ongoing. However, entities must apply Australian Privacy Principle (APP) 6 to establish the basis for this type of secondary use.
- **Destroy any inputs that have been collected immediately once the purposes of collection have been met**. Personal information, including sensitive information, that is collected for SMMA compliance purposes (e.g. biometric information, biometric templates, identity documents) must be destroyed once all purposes have been met. Avoid purpose 'padding' and ensure destruction includes caches and storage.
- **Be thoughtful when designing consent requests for secondary uses and disclosures of personal information collected for SMMA**. Secondary use and disclosure should be strictly optional and easily withdrawn. The consent request should be written and designed so users of all abilities can understand what they are being asked to agree to and change their mind.
- **Be transparent, at the moment it matters**. Use APP 5 just-in-time notices to explain key information such as what is collected, why, by whom, how long it is retained, and the user's choices (including alternative methods and review processes). APP 1 privacy policies should be updated with clear and transparent information, with clear policies and procedures to facilitate this transparency.

2. Overview

Part 4A of the *Online Safety Act 2021* (Part 4A) requires a provider of an age-restricted social media platform to take 'reasonable steps' to prevent age-restricted users (under 16 years) from having an account with the platform.[1] The onus is on providers to introduce systems, processes and controls that can be demonstrated to ensure that people under the minimum age cannot create and hold a social media account.

Part 4A does not prescribe what 'reasonable steps' platforms must take. eSafety has published regulatory guidance on this topic. However, it is expected [2]that at a minimum, the obligation will require platforms to implement some form of age assurance as a means of identifying whether a prospective or existing account holder is an Australian child under the age of 16 years.

Age assurance is an umbrella term for a set of processes and methods used to verify, estimate and/or infer the age or age range of an individual. This enables entities to make age-related eligibility decisions.[3]

Part 4A is technology-neutral and does not mandate any single method or combination of methods. Whether an age assurance methodology meets the 'reasonable steps' requirement is to be determined objectively having regard to the suite of methods available, their relative effectiveness, costs associated with their implementation, and data and privacy implications on users, amongst other things.[4] The Office of the Australian Information Commissioner (OAIC) recommends reading this guidance alongside eSafety's regulatory guidance.

Part 4A recognises that entities undertaking age assurance may handle personal information for SMMA compliance purposes.[2] Part 4A operates alongside the *Privacy Act 1988* (Privacy Act) and introduces additional, more stringent obligations when handling personal information to meet the SMMA requirement.

2.1. What is personal information in the SMMA context?

For SMMA compliance, information involved in age assurance will likely be personal information because it is information or an opinion about an identified individual, or an individual who is reasonably identifiable. This includes situations where the information is inferred, generated or incorrect.

In practice, the personal information involved in age assurance may be one or more of the following:

---

[1] To help you assess if a service is an age-restricted social media platform, consult the self-assessment tool developed by eSafety: How to assess if a service is an age-restricted social media platform | eSafety Commissioner.

[2] Explanatory Memorandum, Online Safety Amendment (Social Media Minimum Age) Bill 2024 (Cth).

[3] ISO FDIS 27566-1 – Information security, cybersecurity and privacy protection - Age assurance systems – Age assurance is a set of processes and methods used to verify, estimate or infer the age or age range of an individual, enabling organisations to make age-related eligibility decisions with varying degrees of certainty.

[4] Explanatory Memorandum, Online Safety Amendment (Social Media Minimum Age) Bill 2024 (Cth).

- Inputs – personal information about an individual that is collected and processed by an age assurance technology (e.g. photo, voice, document scan).
- Outputs – the SMMA decision artefact created as part of the age assurance process (e.g. '16+ yes/no' token) and linked to an account.
- Existing personal information – information already held about an account holder.

An individual does not need to be named in the specific information for that information to be personal information. An individual can be 'identified' if they are distinguishable from others. For example, even if a name is not present, it may identify an individual, as it will usually be associated with a record of the user or could be linked back to the person it relates to.

Sensitive information is a subset of personal information that is generally afforded a higher level of privacy protection under the Australian Privacy Principles (APPs) than other personal information. This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual.

'Sensitive information' is a subset of personal information[5] and is defined as:

- information or an opinion (that is also personal information) 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
- health information about an individual
- genetic information (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 (s 6(1)).

Where there is uncertainty, the OAIC encourages entities to err on the side of caution by treating the information as personal or sensitive information and handle it in accordance with Part 4A and the Privacy Act obligations.

[5] For more detail about sensitive information see Paragraph B.141 in Chapter B: Key concepts | OAIC

2.2. Privacy obligations under the SMMA scheme

Part 4A of the *Online Safety Act 2021* operates alongside the *Privacy Act 1988* (Privacy Act) and APPs. Part 4A introduces additional, more stringent obligations on age-restricted social media platform providers and third-party age assurance providers when handling personal information for social media minimum age (SMMA) compliance purposes. These providers are collectively described as 'entities' in this guidance.

In summary, Part 4A privacy obligations are:

- **Purpose limitation** (s 63F(1)) – An entity that holds personal information about an individual that was collected for the purpose of (or purposes including) the SMMA obligation must not use or disclose the information for any other purpose. The following exceptions apply:
    - In circumstances where APP 6.2(b), (c), (d) or (e) apply; or
    - With the voluntary, informed, current, specific and *unambiguous* consent of the individual (s 63F(2)).
- **Information destruction** (s 63F(3)) – An entity that holds personal information about an individual that was collected for the purpose of (or purposes including) the SMMA obligation must destroy the information after using or disclosing it for the purposes for which it was collected.

Diagram 1 illustrates these obligations and references the sections of this guidance where the relevant issues are discussed.

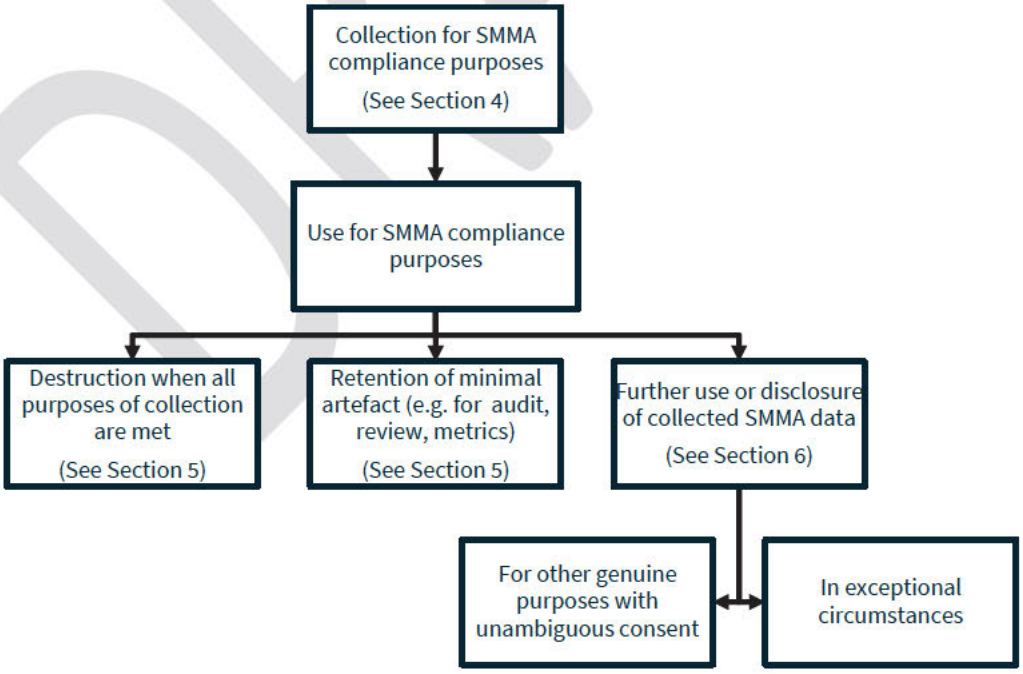

Diagram 1: High-level summary of personal information handling in the SMMA context

Failure to comply with the obligations contained in s 63F is an interference with the privacy of the individual for the purposes of the Privacy Act. This brings non-compliance with s 63F within the remit of the Information Commissioner's enforcement powers under the Privacy Act. It also entitles an individual to complain to the Information Commissioner about an alleged contravention of s 63F.

Steps to comply with the SMMA obligation will not be 'reasonable' unless an entity also complies with its information and privacy obligations under Part 4A, as well as the Privacy Act and the APPs.[6]

2.3. About this guidance

Part 4A envisages the processing of personal information for SMMA compliance purposes. The Office of the Australian Information Commissioner (OAIC) has developed this guidance for age-restricted social media platform providers and third-party age assurance providers that must comply with the Privacy Act[7] and Part 4A.[8]

This guidance aims to help entities understand their privacy obligations in the SMMA context. It does not cover the entirety of the privacy obligations that apply and should be read in conjunction with the Privacy Act and the Australian Privacy Principles guidelines (APP guidelines).

Other important resources to review include:

- Guide to developing an APP privacy policy
- Guide to securing personal information
- Guide to undertaking privacy impact assessments

This guidance should also be read in conjunction with eSafety's guidance on reasonable steps for more information on how to evaluate and select appropriate age assurance technologies for SMMA compliance purposes.[9] eSafety is responsible for formulating the written guidelines for the taking of reasonable steps in relation to the SMMA to prevent age-restricted users from having accounts, as well as continuing monitoring, compliance, and enforcement functions associated with Part 4A.

[6] See eSafety, 'Social Media Minimum Age Regulatory Guidance' ('eSafety SMMA Guidance') (September 2025).

[7] Note that while small businesses with an annual turnover of $3 million or less are generally exempt from the Privacy Act, section 6D(4)(c) of the Privacy Act states that an entity is not considered a small business operator if it discloses personal information about an individual to anyone else for a benefit, service, or advantage. As a result, such an entity must comply with the Australian Privacy Principles (APPs) and other relevant provisions.

[8] Section 63F in Part 4A refers to 'entity', which has the same meaning as in the Privacy Act. Section 63F therefore applies not only to providers of age-restricted social media platforms but also any other entity that handles personal information for the purpose (or one of the purposes) of the SMMA obligation. This includes small business operators.

[9] See eSafety, 'Social Media Minimum Age Regulatory Guidance' ('eSafety SMMA Guidance') (September 2025).

3. Adopting a privacy by design approach when choosing an age assurance method or combination of methods

Age assurance methods have the potential to interfere with the privacy of individuals. Each scenario, or combination of scenarios, employs different technologies and processes and raises different privacy implications depending on how personal information is handled and the sensitivity of the personal information.

The OAIC encourages entities to adopt a 'privacy by design' approach when selecting an assurance method. A Privacy Impact Assessment (PIA) is a systematic assessment that identifies the privacy impact on individuals, and sets out recommendations for managing, minimising or eliminating that impact. A PIA demonstrates commitment to, and respect of, individual's privacy.

This guidance highlights some key privacy considerations for entities to consider, in accordance with the SMMA information lifecycle, particularly regarding collection, use, disclosure and destruction.

Other examples of privacy risks that could be captured and addressed through a PIA include:

- Transparency - the complexity of age assurance methods can make it difficult to understand how personal information is used and how decisions about age verification are reached. Entities should ensure they update their privacy policies (APP 1) and use notifications (APP 5) with clear and transparent information about their use of age assurance methods.
- Accuracy and quality - issues in relation to accuracy or quality of information, particularly for inferred information (see 4.1.2, 4.3.1 and 7 below). Entities must comply with their obligation to take reasonable steps to ensure the accuracy of personal information under APP 10 when using age assurance methods.
- Security and data breach - age assurance may increase the risks related to data breaches. This could be through unauthorised access or through attacks. It is important to consider an entity's security obligations under APP 11 and the Part 4A destruction obligations when selecting an age assurance method.

Entities should also consider principles such as necessity and proportionality in implementing chosen technologies and methods, particularly given age assurance technologies may involve the handling of personal and sensitive information such as biometric templates, behavioural signals and formal identification documents.

Entities should consider low-intrusion techniques within an age assurance method(s) and escalate to more intrusive information handling only as necessary. Entities should also consider the privacy impacts associated with each age assurance method (e.g. inference, estimation and verification) and whether the circumstances surrounding the specific chosen method(s) justify the privacy risks.

In determining whether an age assurance method is necessary, entities should consider factors including:

- the suitability and effectiveness in addressing the SMMA obligation

- whether the method is proportionate to the legitimate aim of preventing age-restricted users from having accounts, particularly where handling of sensitive information is proposed[10]
- alternative age assurance methods available to address the SMMA obligation.

It is the responsibility of the entity to justify that the age assurance method is reasonably necessary. The fact that a particular age assurance method or combination of methods is available, convenient or desirable should not be relied on to establish necessity.

[10] Sensitive information under the Privacy Act is afforded a higher level of privacy protection and must generally be collected with the individual's consent.

4. Privacy guidance – collection

4.1. New collection of information for SMMA compliance purposes

4.1.1. What it looks like

An entity asks a user to provide certain personal information or go through a process that allows the entity to collect personal information to determine whether the user is an age-restricted user (under 16 years) for SMMA compliance purposes.

Example - Age estimation

- Facial age estimation that collects a single or burst of selfie photos, plus anti-spoof signals; this is processed on-device or via a third-party provider and returns a '16+ yes/no' result.

Example - Age verification

- Document check via on-device scan that reads the date of birth (DOB) from a government ID via an on-device app and returns a '16+ yes/no' result.[11]
- Tokenised assertion from a digital identity credential (provided by an accredited identity provider such as a bank, telco or education institution) that the user is 16+; no other identity attributes are collected.[12]

4.1.2. Privacy considerations

Legal application

Both the Privacy Act and Part 4A apply. In addition to the APPs, entities must comply with the stricter obligations introduced by Part 4A.

APP 3.4(a) (the collection is required or authorised by law) operates in this context to permit information handling that is *necessary* in the circumstances to achieve the objective of preventing age-restricted users having accounts. Handling will additionally need to be *proportionate* to satisfy this necessity requirement.

Where the APP 3.4(a) exception is not engaged, the requirement in APP 3.2 and APP 3.3 for collection of personal or sensitive information to be 'reasonably necessary' will apply to collection of any such information. This limits what information may be collected to those steps that would fulfil a platform's function to comply with s 63D of Part 4A.

[11] There must be alternatives to this method since this involves government-issued identification – see Online Safety Act, s 63DB.

[12] There must be alternatives to this method if using an accredited service within the meaning of the *Digital ID Act 2024* – see Online Safety Act, s 63DB.

APP 5 (Notification of the collection of personal information) and APP 10 (Quality of personal information) are also of particular relevance when collecting personal information for age assurance.

The OAIC provides the following practical considerations in relation to collection:

Minimise what you collect

- Where possible, collect binary outcomes ('16+ yes/no') rather than DOB or exact age.
- If scanning a document, only parse the DOB and redact or avoid non-DOB fields.

Process information temporarily

- Use technology solutions and/or providers that temporarily process personal information inputs (e.g., document images/fields, face frames, liveness videos) as part of age assurance and do not retain them.
- Transient processing of personal information is considered a 'collection' where the information is included in a record.

Good practice case study – Collection of information for age check at sign-up

GlowLoop is a social media app that must comply with the SMMA obligation. At signup, any prospective user in Australia (determined by a one-off country signal using IP address) sees a short explainer screen:

"Before we create your account, we need to confirm you're 16 or over. Pick the option that suits you. We don't keep your photos or documents." [How we handle your personal information]

Tapping the 'How we handle your personal information' opens a simple APP-5 compliant notice dialogue box.

Users can choose between two big tiles, side-by-side:

1. Digital ID / device-wallet token

   "Use a credential to share a simple 16+ yes/no with GlowLoop. No other details collected."

2. Facial age estimation (no selfie storage)

   "Take a quick selfie on this device. We'll process it to estimate if you're 16+. We don't save the images."

Eva (20) chooses facial age estimation. The app asks her to hold the phone steady and blink; a short progress ring spins. Ten seconds later, she sees: "You appear to be 16+. Continue to create your account." The app explains that Eva's selfie was processed locally and not stored. She taps Continue and finishes signing up.

Sam (24) chooses Digital ID. His phone opens a device wallet card issued by his bank (which supports age assertions); he consents to sharing a "16+" assertion only. Back in GlowLoop, he sees: "We received a 16+ confirmation. You're set." The app explains that no document numbers or dates of birth are shared. Sam taps Continue and finishes signing up.

Kendra (17) tries facial age estimation first. The result comes back borderline, so GlowLoop escalates to a higher-assurance option – Digital ID / device-wallet token. Kendra selects the school-issued digital credential in her wallet, shares a binary 16+ assertion, and completes sign-up.

Privacy tip:

Good practice includes instant destruction of raw selfies; short-lived, scoped tokens; and ring-fencing the minimal decision artefact. Higher risk practices include storing selfie frames, logging tokens in a way that enables cross-service tracking, or making the escalation automatic without clear consent and alternatives (e.g. forcing an ID upload).

4.2. Using existing information directly to confirm the residency and age of an account holder

4.2.1. What it looks like

An entity uses information it already holds about a user to directly determine whether they are under 16 years. This is typically done to detect and deactivate accounts belonging to age-restricted users. Using existing information to *infer* the age or location of a user is discussed separately in section 4.3.

- Example - Existing DOB or self-declared age on file is referenced.
- Example - Existing third-party assertion or token (e.g., from a telco, bank or digital wallet) confirming 16+ is still within validity.

4.2.2. Privacy considerations

Legal application

Part 4A

The s 63F obligations in Part 4A apply to personal information that was collected for SMMA compliance purposes. If an entity uses information it already holds to conduct age assurance and no new collection occurs, then s 63F will not apply. Using personal information that was previously collected for a different purpose does not, by itself, put that information within the remit of s 63F.

However, if the entity creates a new piece of information for SMMA compliance purposes (e.g., using the existing DOB on file to create a new '16+ flag' for the account holder), that new artefact would constitute a collection that is subject to s 63F.

Privacy Act

The APPs continue to apply in this scenario, including APP 3 (Collection) where new information is generated or inferred from existing information.

It will be particularly important for the entity to comply with APP 6 (Use and disclosure) and identify and document an appropriate pathway for the secondary use of existing personal information:

- APP 6.1(a) – Obtain consent from the individual,
- APP 6.2(a) – Reasonable expectation and relatedness to the original purpose, and/or
- APP 6.2(b) – Required or authorised by law (i.e. s 63D of Part 4A).

Diagram 2 below explains the process for determining the most appropriate pathway.

Where appropriate, entities should generally obtain **consent** for secondary use of personal information already held.

Where seeking consent is not appropriate, entities should generally rely on the individual having a **reasonable expectation** that the entity will use or disclose the information already held, for the secondary purpose. The secondary purpose must also be **related to the primary purpose** of collection (or directly related for sensitive information).

Where neither of the previous options are appropriate and the entity is a platform, the entity may seek to rely on s63D as a required by law exception that permits collection, use or disclosure **where necessary** to give effect to the SMMA scheme. The exception does not include information handling that is merely incidental or convenient.

An assessment of what information handling is necessary in the circumstances involves taking into account competing interests, including the privacy of individual users.

Privacy considerations will be a significant consideration in assessing what is appropriate and privacy impacts will need to be weighed against a totality of factors.

Factors may include:
- The size, resources and technological maturity of the entity
- The efficacy and cost of the method
- The availability of alternate methods and their relative efficacy and risks
- The nature, sensitivity and quantity of personal information to be handled
- The security of the personal information
- How long it will be retained.

Diagram 2: APP 6 bases for secondary use of personal information

The OAIC provides the following practical considerations when using existing information directly to meet the SMMA obligation:

Minimise what you use

- As long as the transparency and secondary use obligations are met, using existing information directly to confirm residency and whether the user is over 16 is a data minimising option because it does not require a new collection or the handling of additional personal information.
- Use only the fields that are needed to determine age.

Document the APP 6 basis

- Assess and be able to demonstrate the APP 6 basis for information reuse.

Handle sensitive information carefully

- Be very cautious if using existing biometric templates, images or other sensitive kinds of information for SMMA compliance purposes.
- Ensure handling is necessary and proportionate to meeting the requirements of s 63D. If unsure, establish a clear expectation from the user and ensure a close relationship to the primary purpose of collection; otherwise obtain consent.

4.3. Using existing information to infer the residency and age of an account holder

4.3.1. What it looks like

The entity uses information it already has about the account holder to infer whether they are under 16 years and whether they are ordinarily resident in Australia. This could involve drawing probabilistic conclusions based on behavioural patterns, contextual data, digital interactions, metadata or other information and subsequent collection of a 16+ decision artefact.

Examples include:[13]

Location-related signals

- IP address, GPS or other location services
- Device identifier, language, time settings
- Phone number
- App store, operating system, account settings

[13] Extract from eSafety's SMMA Guidance, p 32.

- Photos, tags, connections, engagement, other kinds of activity.

Age-related signals

- Age of account (e.g. the account has existed for 10 or more years)
- Engagement with content targeted at children or early teens
- Linguistic analysis or language processing
- Analysis of end-user-provided information and posts
- Visual content analysis (e.g. facial age analysis performed on photos and videos uploaded to the platform or entity)
- Audio analysis (e.g. age estimation based on voice)
- Connection with other end-users who appear to be under 16
- Membership in youth-focused groups, forums or communities.

4.3.2. Privacy considerations

Legal application

Part 4A

Inference would be typically conducted using information that was not collected for SMMA but rather other purposes, such as account management, safety and content moderation, providing core features and services, etc. Therefore, s 63F generally will not apply to the original inputs.

Where an entity uses inference methods to generate personal information (e.g. +/-16 score, pass/fail age flag, Australian resident flag), such information will be considered a collection of personal information and is subject to the restrictions in s 63F including purpose limitation and destruction (see section XX of this guidance).

Privacy Act

The APPs continue to apply. APP 3 is relevant where new information has been inferred and generated from existing information. It will also be important for the entity to have an appropriate APP 6 pathway for conducting inference on existing personal information:

- APP 6.1(a) – Obtain consent from the individual,
- APP 6.2(a) – Reasonable expectation and relatedness to the original purpose, and/or
- APP 6.2(b) – Required or authorised by law (i.e. s 63D of Part 4A).

While the APP 6 pathways for use of existing information for inference is the same as use of existing information directly to meet the SMMA obligation, their application is more nuanced in the case of inference. This is due to the wide categories and sensitivities of information that could potentially be reused for inference.

See Diagram 2 above.

Given the breadth of potential information that may be reused for inference, APP 10 (Quality) is especially important. Entities must take reasonable steps to ensure that the personal information involved is accurate, up-to-date, complete and relevant to the SMMA obligation.

Although the use of information for age inference may result in a more frictionless experience for the individual, it may also result in the collection and retention of disproportionate amounts of personal information in a way that undermines individuals' privacy.

Practical considerations

The OAIC recommends taking a risk-based approach which ensures information used for inference is proportionate and privacy impacts are minimised. This means less intrusive information is preferred over more intrusive information to achieve an acceptable inference outcome. It also means that where privacy risks are higher, entities should explore other methods for age assurance.

The OAIC provides the following proportionality considerations tailored to age inference, drawing on the factors outlined in Section XX above:

Sensitivity – How intrusive is the personal information you plan to reuse, and what harm could result if it is wrong or mishandled?

- Prefer non-sensitive information, non-content signals such as metadata and system data.
- Treat behavioural and content data (e.g. posts, events, groups, interests, affinities, communications and other user interactions) as higher privacy risk.

Volume – How much, how often and for how long will you use personal information for inference?

- Use event-based, point-in-time checks rather than continuous monitoring.
- Avoid building long-lived behavioural profiles; only add more signals if they materially improve confidence.

Purpose – Is the reuse strictly necessary to achieve the SMMA decision and nothing more?

- Define the outcome precisely and assess whether inference is an effective method.
- Use a less intrusive method if it can deliver the same outcome while using less information.

Relatedness – How closely is the reuse of personal information for age inference related to the original purpose?

- Ask whether an individual would reasonably expect the personal information to be reused for age assurance purposes.

Different cohorts of users may require different approaches. eSafety guidance confirms there is no one-size-fits-all approach that will be suitable in all circumstances. For a substantial proportion of

users on long-standing platforms, it may be possible to confirm at a high level of confidence that they are 16+ years old based on the account tenure or creation date. More work, effort and personal information will be required to infer age where account tenure is short, or where the user is in a younger age threshold.

eSafety's regulatory guidance provides further detail on assessing the reliability, accuracy, robustness and effectiveness of age inference as a method of age assurance.

To minimise privacy impacts on individuals, the OAIC recommends handling less intrusive information over more intrusive information (e.g. age analysis performed on photos and videos, or audio analysis on voice), to achieve an acceptable inference outcome. It also means that where privacy risks are higher, entities should explore other methods for age assurance.

Good practice case study – inference using existing signals

VibeTrail is a social media platform. Once the SMMA obligation takes effect, VibeTrail implements a back-end system that uses information it already holds to infer (a) whether an account holder is ordinarily resident in Australia and (b) whether they are under 16. It doesn't ask existing account holders for age checks, unless the inference raises a doubt about whether they are over or under 16.

1. 'Long-time user in Australia'

Alan (45) has used VibeTrail for twelve years. His language/time settings are English (AU)/Australia, and he signs in from an AU IP address.

These signals may reflect a proportionate secondary use of personal information to reasonably infer 'resident in Australia' and 'likely 16+'. Alan continues to use his account without experiencing any additional prompts. Use of additional existing information may be considered disproportionate or unreasonable in the circumstances.

2. 'Borderline new account'

Tia (16) created an account one month ago, before the SMMA obligation commenced. Signals show AU IP address and an AU phone number attached to the account but as the account duration is short and there have been no prior age checks, it may be proportionate and reasonable to use other existing personal information to trigger a more reliable age assurance method. For instance, her public bio says 'Year 10 goalie'.

The system flags the account as 'possibly under 16' and shows Tia an in-app notice explaining why. She is offered a choice to resolve it (for example, Digital ID yes/no token, on-device facial age estimation). If she doesn't act, the account is restricted.

Privacy tip:

Use inference sparingly and proportionately. Start with non-sensitive information, low-volume signals; treat outputs as short-lived and ring-fenced; require consent or clear legal basis for any higher-intrusion reuse, especially before taking adverse action. Practices to

avoid include always-on surveillance and reusing sensitive information without assessing necessity and proportionality.

5. Privacy guidance – destruction

5.1. General obligation to destroy personal information

5.1.1. What it looks like

When conducting age assurance activities to meet the SMMA obligation, an entity will likely collect and handle **personal information** relating to current and prospective users.

Examples include:

- **Inputs (e.g. document images/text, selfies, biometric information, biometric templates)** that are used for a point-in-time age check.
- **SMMA artefact (e.g. 16+ flag)** that is created from inputs, existing DOB information on file or inferred from multiple data points.
- **Third-party assertion/token** received from an identity provider.
- **Documents received as part of a formal review or complaint escalation process** to meet the SMMA obligation.

5.1.2. Privacy considerations

Legal application

Section 63F(3) of Part 4A states that an entity that holds personal information about an individual that was collected for the purpose(s) of the SMMA obligation must destroy the information after using or disclosing it for the purposes for which it was collected.

Section 63F(3) is a stricter standard than APP 11.2 (retention of personal information) in two key ways:

1. The information must be destroyed; there is no allowance for de-identification.

2. The destruction must happen once all the purposes for which the personal information was collected during age assurance is met; there is no allowance for retention just because there is another potential business use case.

APP 11.2 continues to apply to all other personal information handled by entities.

Pre-existing information that is used to directly meet the SMMA obligation or for age inference is covered by APP 11.2 rather than s 63F. However, any new record created from this process for the purpose of the SMMA obligation is covered by s 63F.

You can find more information on security responsibilities in the Guide to Securing Personal Information, and Chapter 11: APP 11 Security of personal information.

The OAIC provides the following practical considerations in relation to destruction:

Distinguish between inputs and outputs

- Age assurance inputs (generally higher risk) – examples include document images/text, selfies, liveness videos, other biometric information or templates and any other personal information that is used as input for an age assurance method.
  - Process for the purpose of age assurance, then destroy immediately
  - Do not store 'just in case'
  - Ensure destruction covers caches and transient storage.
- Age assurance outputs (generally lower risk) – examples include binary outcomes (16+ yes/no), methods, provider IDs, timestamps and non-linkable references/tokens; third-party assertions or tokens received from an identity provider (such as a bank, telco or education institution).
  - Retain strictly for limited purposes – that is, evidence of compliance, troubleshooting, complaint or review handling, dealing with fraud or circumvention
  - Set bright-line, limited retention windows.

Ring-fence the age assurance outputs

- To ensure compliance with the s 63F destruction obligation, the entity should create a distinct ring-fence or 'SMMA environment' that enables it to be fully aware of the outputs that it handles and where they are kept.
- Different entities will have different implementation arrangements. For example:
  - **Physical/logical separation** – Combination of people, technology and processes to ensure that personal information for SMMA is separated from other parts of the entity and only interface with the entity in limited and controlled ways.
  - **Documented boundary** – To aid compliance and demonstrate accountability, the SMMA environment could be documented in a way that shows the inputs, transient processing, outputs, retention points and destruction paths.
  - **Destruction readiness** – The environment could be configured such that personal information for SMMA is able to be destroyed automatically and independently of other organisational data.

- There may be legitimate business reasons for co-mingling personal information for SMMA with other personal information (e.g. processing them in shared pipelines or storing them in shared databases). However, this may make it harder to prove purpose limitation and to meet the strict destruction obligation. Each entity needs to make its own assessment, considering the compliance requirements in s 63F of Part 4A.
  - The most straightforward path to compliance, and the one that best aligns with the intention of s 63F, is to ring-fence personal information used for SMMA compliance purposes.

Good practice case study – destruction

GlowLoop is a social media app. After the SMMA obligation takes effect, anyone signing up in Australia must pass an age check.

1. Destruction example – usual path

Daniel (25) picks facial age estimation. GlowLoop uses ProviderX, a specialist age-assurance provider, under a contract that: (i) limits processing to SMMA purposes only, (ii) forbids retention of raw inputs, (iii) requires destruction once processing has been conducted, and (iv) provides destruction attestations.

Daniel completes a quick blink-and-turn selfie. Ten seconds later, GlowLoop receives from ProviderX only a binary '16+ yes' plus a non-linkable transaction ID. ProviderX automatically destroys the selfie frames and liveness clips. GlowLoop does not store anything from the raw capture. ProviderX's destruction attestation for Daniel's transaction is recorded.

In the back-end, GlowLoop writes a small decision artefact into its ring-fenced 'SMMA store':

- outcome: 16_plus
- method: face_estimation_v3
- provider_id: ProviderX
- checked_at: 2025-09-18T03:21Z
- token_ref: 9f2a… (opaque)

GlowLoop's product teams can't see this table; they call a read-only /is_16_plus API that returns only 'yes/no'. Advertising, analytics and machine learning pipelines are blocked from the SMMA store.

2. Destruction example – reviews path

Aria (16) tries to sign up and follows the blink-and-turn prompts. Ten seconds later ProviderX returns 'cannot confirm 16+' result, which is communicated to Aria. GlowLoop writes a short-lived 'under_16' decision artefact in the SMMA store.

A short explainer appears: "This result is an estimate only. If it's wrong, you can choose another way to confirm your age or start a quick review." Aria taps 'Review this decision'. The review flow is tightly scoped and clearly explained:

- What she uploads – A photo of an ID page showing only DOB (other fields are masked in-app).
- Where it goes – A view-only reviews bucket that auto-destroys items after 30 days.
- Who can see it – A single human reviewer in a restricted console; downloads are blocked.

The reviewer checks Aria's DOB, records '16+ confirmed via review' and hits 'Resolve'. At this point:

- The document image is destroyed; no copies or OCR text is kept.
- The original 'under_16' artefact is superseded by a new '16_plus' artefact.

Aria receives a message saying "Thanks – we've fixed this. Your age is confirmed as 16+ and you may proceed to creating your account."

Privacy tip:

Good practice includes destruction-on-decision by the provider, truly temporary handling of raw inputs, a ring-fenced minimal artefact, read-only APIs, and automated destruction of personal information used for SMMA compliance purposes. Practices to avoid are retention and use of personal information for its own purposes (e.g., quality assurance, training) without consent or exceptional circumstances.

5.2. Information destruction when there are multiple purposes

5.2.1. What it looks like

Section 63F(3) of Part 4A acknowledges there may be multiple purposes for which the personal information is collected, as long as meeting the SMMA obligation is one of them. A relevant consideration for destruction is what happens in such circumstances, especially where one or more of the other purposes may require the information to be retained for longer than meeting the SMMA obligation.

Examples include:

- **Sign-up age check** – User completes facial age estimation to open an account. The same event creates a short-lived decision artefact for audit logging and reviews purposes.
- **One age gate, several compliance needs** – A single age check is used to satisfy the entity's obligations with respect to (i) SMMA, (ii) app-store age policy, and (iii) another jurisdiction's age rule.
- **Know Your Customer flow for creator** – An ID and selfie are captured for AML/CTF onboarding; the entity also needs to know that the creator is over 16 years to meet the SMMA obligation.

5.2.2. Privacy considerations

Legal application

Section 63F(3) of Part 4A requires the entity to destroy the information collected for the SMMA obligation, once it has used or disclosed the information for all the purposes for which it was collected.

The OAIC provides the following practical considerations when considering destruction in the context of multiple purposes:

Avoid 'purpose padding'

- Consistent with Chapter 6 of the APP Guidelines, purposes must be construed narrowly and not be so general in nature that they comprise a function or activity of an entity. Do not include broad, speculative or open-ended purposes as part of collection for age assurance (e.g. product improvement, research).
- Additional purposes must be genuine. Merely asserting that the collection is for other purposes does not allow you to retain the information collected for longer than meeting the SMMA obligation.

Develop a retention matrix

- Where the information collected (e.g. SMMA artefact) serves multiple purposes, ensure that each purpose has a defined retention period and destroy the information once the last retention period has expired.

Further partition the personal information where there are additional requirements

- If a different legal regime (e.g. AML/CTF, overseas jurisdiction) requires retention following an age check, produce and retain separate non-SMMA artefacts or records.

5.3. Information retention in limited circumstances

5.3.1. What it looks like

There are narrow situations where an entity may need to retain a minimal record after an age check to operate the service responsibly and evidence compliance.

Examples include:

- Audit logging and evidence of compliance – Prove that a check has occurred, the outcome, how it was done, and when.
- Troubleshooting, fraud and circumvention – Investigate errors, suspected spoofing and re-registration attempts.

- Complaints and reviews – Respond to user/parent challenges to the age check or its outcome.

In such cases, it is sufficient that a SMMA artefact is collected and retained, which contains minimal information such as binary outcome (16+ yes/no), method, provider ID, timestamp and non-linkable reference/token.[14]

5.3.2. Privacy considerations

The OAIC considers that tightly limited retention of personal information is acceptable and can be done in accordance with Part 4A and the Privacy Act.

All the practical considerations above regarding destruction in the context of multiple information collection purposes are applicable here. In particular, the entity should be transparent about the directly related purposes arising from the age check that involve retention for a longer period.

The one additional consideration is for entities to set time-based limits for each purpose that involves personal information for SMMA (e.g. evidence of compliance, troubleshooting, complaints and reviews). The timing should be justified by the business practice and accord with standard industry practice.

The time-limits for each purpose should determine when and how the personal information is accessed and used. Once the time period for the last allowed purpose has expired, the entity should destroy the relevant artefact.

Privacy tip - example do's and don'ts for good practice

Audit evidence, proof a check occurred

- Do retain a minimal decision artefact (e.g. binary outcome, method, provider ID, timestamp, non-linkable token), with documented retention periods; enable auto-destroy.
- Don't store selfie frames, ID images, biometric templates or age scores/confidences that are no longer required.

Troubleshooting, fraud and circumvention

- Do retain the minimal artefact for a case-linked time window; require a Case ID; purge once case is closed.
- Don't build open-ended watchlists or keep biometric templates or raw documents indefinitely 'in case of future abuse'.

Complaints and reviews

[14] This is consistent with eSafety's guidance that providers are not expected to retain personal information as a record of individual age checks (eSafety SMMA Guidance, p 25). Although note that to the extent SMMA artefacts are linked with users or account information, they may be considered personal information.

- Do accept redacted DOB evidence in a view-only bucket; destroy the document immediately after the decision; keep only the updated minimal. Don't keep copies of documents or OCR text beyond the review; store full DOB or document numbers in the SMMA store.

6. Privacy guidance - secondary use or disclosure of personal information collected for SMMA compliance purposes

6.1.1. What it looks like

An entity may seek to reuse age assurance inputs for other business purposes or disclose the output (e.g. 16+ artefact) to another entity.

6.1.2. Privacy considerations

Legal application

Section 63F(1) of Part 4A restricts the use or disclosure of personal information collected for the SMMA obligation. Secondary use or disclosure is only permitted with the unambiguous consent of the individual, or in exceptional circumstances outlined above.

The definition of consent in s 63F(2) is notable for including 'unambiguous' as one of the elements of consent. This is a requirement specific to the SMMA scheme that precludes entities from seeking consent through pre-selected settings or opt-outs.

'Exceptional purposes' align with the following paragraphs in APP 6.2 (refer to Chapter 6 of the APP Guidelines for further information on these exceptions):

- **Para 6.2(b)** – It is required or authorised by or under an Australia law or a court/tribunal order. For example, a subpoena or statutory notice compels the disclosure of the SMMA artefact for specific users.
- **Para 6.2 (c)** – A permitted general situation exists. For example, use of the SMMA artefact to triage a suspected unlawful security breach as part of a security incident response.
- **Para 6.2 (d)** – A permitted health situation exists. For example, a credible, serious safety threat necessitates disclosure of the SMMA artefact to an emergency health services provider.
- **Para 6.2 (e)** – The organisation reasonably believes that it is necessary for one or more enforcement related activities. For example, an enforcement body requests information for enforcement related activities (see Chapter B of the APP Guidelines).

Consented purposes

- The OAIC provides the following practical considerations when seeking to use or disclose personal information used for SMMA for secondary purposes with unambiguous consent:
  - **Limit what you use and disclose:** Use or disclose only a binary assertion ('16+ yes'), one-time or short-lived tokens where possible, that are specific as to purpose.
  - **Make consent truly optional:** Implement a separate consent flow dedicated to secondary purposes; do not bundle with the primary (SMMA obligation) purpose. Avoid general or broad terms of use or agreement obtained through use of dark patterns. Set defaults to 'off'.
  - **Design for users of all abilities:** Present icons, visuals and choices in the user interface. Offer additional clarifying information and prompts to aid comprehension. Implement easy withdrawal toggles in a dedicated privacy setting or contextually appropriate screen.

Exceptional circumstances

- Exceptional circumstances are non-routine. However, as a matter of best practice, it is useful for entities to have processes in place to deal with them. For example:
  - Identify the presenting issue and which APP 6.2 exception is relevant.
  - Apply a necessity and proportionality test to determine whether use or disclosure is warranted.
  - Default to using or disclosing the minimum amount of information required.
  - Keep a record of the decision(s) made and action(s) taken.

Good practice case study – Secondary use and disclosure

FlareHub is a social media platform. It complies with the SMMA obligation and conducts age checks on its users, retaining a SMMA artefact indicating that a user is 16+.

David (22) signs up to FlareHub and undertakes facial age estimation to assure his age.

Later, David wants to join a music community, StageDoor, which also requires users to be over 16 and is linked to Flarehub. On a hand-off screen, FlareHub shows a just-in-time notice:

> Share your 16+ confirmation with StageDoor?
> - We can send a one-time '16+ yes' token to StageDoor to help create your account.
> - No name, DOB or other personal information is shared.
> - Token expires in 7 days or when you withdraw.
> - [Share] [Not now] [Learn more]

David selects [Share]. FlareHub generates a scoped token that encodes only '16+ yes', the method, vendor ID, and a timestamp. It is kept in a 'consented-tokens' store, separate from the SMMA data store, and sent via a secure API to StageDoor. StageDoor is contract-bound to use the token once, not retain it beyond 7 days, and not disclose to other parties or for other purposes.

If David later revokes sharing in FlareHub's settings, FlareHub sends a webhook to StageDoor and the token is immediately purged on both sides.

Privacy tip:

Good practice involves outputs-only sharing via a one-time, partner-scoped token; separate token stores; clear just-in-time notices; and a separate, unambiguous opt-in for a clearly described purpose. Do not bundle consent at sign-up or use pre-selected tick boxes.

7. Privacy guidance – frequency of checks

The SMMA guidance issued by eSafety observes that the measures taken by providers to meet the SMMA obligation should not be static. Rather, '[p]roviders should proactively monitor and respond to changes in their platforms' features, functions, and end-user practices, especially where these or other changes may introduce new risks.'[15] Furthermore, eSafety expects providers to take proactive steps to detect accounts held by age-restricted users on an ongoing basis.

The OAIC notes that steps taken by entities to comply with the SMMA obligation on an ongoing basis will likely handle personal information (including collection and reuse) in ways that are addressed by the preceding sections.

Ongoing compliance (e.g. recurring checks or triggers) should be proportionate and necessary to comply with the SMMA obligation. Any reuse that relies on existing personal information should have consent or another clear legal basis (APP 6). Entities should build and maintain their age assurance practices so that quality (APP 10), security and retention limitations (APP 11) are enforced by design.

[15] eSafety SMMA Guidance, p 29.

From: s47F
To: s47F s47F
Cc: s47F SAVARY,Marcel
Subject: RE: For review by 4pm 9 September: eSafety reg guidance on social media minimum age [SEC=OFFICIAL:Sensitive]
Date: Tuesday, 9 September 2025 1:51:31 PM
Attachments: image011.png
image012.png
image013.png
image014.png
image015.png
image016.png
image017.png

OFFICIAL: Sensitive

Hi s47F and s47F

Thank you for seeking our input on this important document.

Please find below our quick turnaround feedback in response to the attached version shared with OAIC.

We have focussed our analysis on the privacy aspects of this guidance. We are offering feedback that reflects our role as the national privacy regulator, and that is designed to encourage the prominence of privacy considerations throughout the guidance.

References to privacy laws, the OAIC, and information handling practices

1. Page 2 – ~~*'This guidance should be read alongside the OAIC's privacy guidance'*~~ – we recommend removing this sentence given the disclaimer is a short and clear explanation of how privacy laws and relevant legislation apply.
2. Page 6 – ~~*'The OAIC is responsible for: Monitoring and enforcing compliance with certain provisions in Part 4A relating to privacy and the use and collection of information as well as ensuring compliance with Privacy Act provisions. See OAIC's privacy guidance for more information.'*~~ - please replace this sentence with the following:

   The Information Commissioner is responsible for:
   - *Providing advice to the Minister on the kinds of information that must not be collected by 'age restricted social media platforms'.*
   - *Functions under the Privacy Act that are triggered if an 'interference with the privacy of an individual' occurs as defined in subsections 63F(1) and (3) of the Act.*
   - *Preparing and publishing platform provider notifications if satisfied that an 'age restricted social media platforms' has contravened subsection 63F(1) or (3) of the Act.*
   - *Making sure regulated entities follow the Privacy Act 1988 and other laws when handling personal information, including sensitive information. This can involve conducting investigations and handling complaints.*

3. Page 11 – We presume the following paragraph relates to personal information and therefore recommend making the following updates (underline and strikethrough) for clarity, noting inference may involve use and/or collection - *'Providers should also carefully consider ~~the proportionality of data collection~~ user privacy, in particular user expectations, data minimisation and the sensitivity of personal information handled to inform inference results and be prepared to report on the range of ~~data~~ personal information being ~~collected~~handled for this ~~purpose~~method. This should include the type and amount of personal information necessary and the frequency and timing of use or collection required to operate ~~effective~~ inference methods.'*
   - The above may also sit better within Part 2, for example at the top of Page 18 where recording of metrics is discussed.
     - Reference to reporting on the range of personal information being collected should also be added to section 3.1.1.
4. Recommend checking each occasion 'collect' is used. 'Handle' or 'Use and collect' may be more appropriate. E.g. Page 15 – we recommend the following change 'including to handle ~~collect~~ sufficient data…'. 'Handle' has the added benefit of applying to non-personal information.
5. Page 20 - References to 'delete' should be re-phrased as 'destroy' to align with Part 4A and the Department's fact sheet – this should be checked throughout the document.
6. Page 20 – *'What personal information will be used, how it will be stored and protected, possible outcomes, and what the provider will do with the result—including what is retained or deleted and relevant ~~data and privacy protections~~*transparency obligations under the Privacy Act*'* – we recommend the changes in underline and strikethrough.

7. Page 33 – for completeness, the section *'2.5.4 Allowing end-users to make complaints or seek review'* should encourage providers to make clear to users that they can make a privacy complaint to the OAIC
8. Page 35 – the following sentence should also be amended to reflect the OAIC complaints pathway *'The SMMA obligation is not a public complaints scheme, eSafety expects providers will accept and manage all user reporting and disputes. '*
9. Page 36 – ~~*'Where providers retain records that contain personal information, this should be subject to robust privacy protections (see Part xx).'*~~ - this sentence could be deleted due to the reference to privacy legislation in the opening sentence of the same paragraph.

Queries/comments regarding privacy impacts of particular policy positions / statements

s47C

[redacted]

11. Page 12-13 – ~~*'Benefits of using third party vendors include that they are often subject to independent accreditation and/or evaluation, whereas in-house solutions deployed by social media platforms generally have not been subject to transparent, independent testing. … Drawbacks include third-party vendors may be unknown to users, exacerbating issues relating to public trust and the risk of scams.'*~~ – We recommend removing this phrasing as it could be interpreted as a selective reflection of the pros and cons of third party systems and of little value given the key message in this section is that it is a matter for providers to decide the range of methods they offer and to conduct their own due diligence. Current accreditation and evaluation offerings in Australia may also fall short of legal compliance.
12. Page 14 – successive validation – *'eSafety considers that based on the trial and current technology, successive validation is the recommended approach to age assurance.'* To avoid a sense that multiple methods will be appropriate in all circumstances, we recommend adding a qualifier to this sentence – perhaps *'is the recommended approach to age assurance <u>for the subset of cases where confidence using other methods alone would otherwise be low</u>.'*
13. Page 22 - Recommend adding '<u>Community expectations of privacy</u>' as a new dot point to the list of changes to maintain an awareness of. Also recommend amending the scams one as follows *'Scams, <u>privacy complaints and data breaches</u> that may emerge in response to increased uptake of age assurance'*.
14. Page 24 – *'Using existing data and signals can offer a frictionless ~~and data-minimising~~ way to infer whether a user is ordinarily a resident of Australia, and to detect potential age-restricted users.'* – suggest removing the words in strikethrough as the method itself isn't inherently data-minimising - that aspect will be determined by the controls put in place i.e. it can be data-maximising if poor controls are in place.
15. Page 25 – We recommend adding a qualifier here, to ground this in privacy obligations - *'In most cases, individual signals should not be relied upon in isolation. eSafety recommends providers draw on multiple signals – such as*

profile information, behavioural patterns, and engagement data - to form a more reliable basis for determining that an account is held by user who is ordinarily resident in Australia, or that it may be held by an age-restricted user, to the extent permissible within obligations in privacy laws. [49]'

16. Page 25 – *'Providers should continue to monitor signals over time , to the extent permissible; in case there is a change indicating that further age assurance may need to be conducted.'*
    - As eSafety are aware, the OAIC is conscious about the need for clarity regarding the legal basis for ongoing monitoring – we there recommend adding a qualifier such as the above in underline.
17. Page 30 – *'Successive validation, or a waterfall approach, that escalates only when prior methods are insufficient in isolation or inconclusive, or where the measures create cumulative confidence, is a way to balance assurance strength with user experience and proportionate impacts on privacy.'* Suggest the addition of the underlined wording to acknowledge the high impact on privacy but noting this may be proportionate in this case.
18. Page 32 - *'Examples of reasonable steps providers can take to prevent, detect and respond to circumvention'* – recommend adding qualifiers to this heading such as replacing 'can' with 'may' and perhaps removing 'reasonable' and just describing these as 'steps' to allow space for assessment of what would be reasonable in the circumstances.
    - Recommend also adding a link to OAIC guidance on sensitive information = Chapter B: Key concepts | OAIC.

Recommended revised wording for 2.4.2

19. We strongly recommend the following amendments (see underline and strikethrough) to this section, including the addition of the below callout box:

2.4.2 Privacy-~~preserving~~compliant and data-minimising

Privacy and the protection of personal information is important for everyone's agency, dignity, and safety.[1]

What is personal information?

Personal information includes a broad range of information, or an opinion, that could identify an individual. This may include information such as a person's name, date of birth, contact details and images or videos where a person is identifiable. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances. Personal information is a broad concept and includes information which can reasonably be linked with other information to identify an individual.

***Sensitive information** is a subset of personal information that is generally afforded a higher level of privacy protection. Examples of sensitive information include photographs or videos where sensitive information such as race or health information can be inferred, biometric templates, biometric information that is to be used for the purpose of automated biometric verification or biometric identification, as well as information about an individual's political opinions or religious or philosophical beliefs.*
Importantly, information can be personal information whether or not it is true.

Steps to comply with the SMMA obligations will not be reasonable unless they ~~are private, data-minimising, secure and trustworthy~~comply with privacy laws, including Part 4A of the Act and the Privacy Act.
Providers must comply with the information[2] *and privacy*[3] *obligations under Part 4A of the Act, as well as the Privacy Act and Australian Privacy Principles regulated by the OAIC. Providers should also have regard to any guidance ~~from~~ released by the OAIC.*
~~Providers should assess the minimum information and data needed to make decisions appropriate for their service and circumstances. Policies should be calibrated to ensure the collection, use and retention is proportionate, necessary and compliant with applicable privacy laws.~~
eSafety acknowledges that effective age assurance measures are likely to involve the ~~collection~~ handling of personal information, but providers are strongly encouraged to take a data minimising approach, use non-personal information as far as possible, and avoid ~~collection of~~ handling sensitive personal information.[45] *(footnote: Chapter B: Key concepts | OAIC)*
eSafety does not expect platforms to retain ~~user data~~ personal information as a record of individual age checks. See Part X for more ~~information~~detail about the types of ~~information~~data, indicators and metrics that eSafety may require to assess compliance.
~~When determining what information is proportionate to collect, providers must consider their obligations under the Privacy Act. Providers should also have regard to eSafety's advice above regarding the data associated with accuracy and effectiveness of measures, and below regarding the principle of proportionality. Providers should also consider relevant guidance from the OAIC.~~

General observations / comments

20. The following phrase set out in the Explanatory Memorandum appears once at the end of section 2.1 but may need to be more prominent within section 2.2 - *'what is reasonable will be determined objectively, having regard to the suite of methods available, their relative effectiveness, costs associated with their implementation, and data and privacy implications on users, amongst other things.*
21. There are aspects in Part 1 that come across as guidance on reasonable steps – it would be good to keep like information together.
22. Technology that handles location data is not referred to in Part 1 – this would be valuable for added context.
23. For clarity, there may be some value in reducing terminology where the same thing is meant e.g.
    - waterfall, layering, successive validation
    - robust measures, cumulative confidence
    - measures, methods, interventions.
24. Page 9 – *'Age inference methods: verified information which indirectly implies that an individual is over or under a certain age or within an age range.'* – this phrasing has been lifted from the AATT report but is not the same as the scope of the term 'age inference' that is used in this document. To avoid confusion and duplication, we recommend keeping one set of descriptions and, for age inference, phrasing the description as the one on page 10 - *'Age inference draws probabilistic conclusions about facts other than a date of birth to imply a likely age or range, based on behavioural patterns, contextual data, digital interactions, metadata or other information.'*
25. A definition or description of 'vouching' would be useful to add.
26. The paragraph immediately under 1.3 would benefit from cross referencing to Part 2.
27. Page 43 - Key terms - Recommend adding the following underlined words to limit mention of purpose to where it appears in the Online Safety Act, to separate it from OAIC terminology on purpose and primary purpose (see Chapter 6: APP 6 Use or disclosure of personal information | OAIC)
    - Purpose, as it appears in the Online Safety Act, means the objective for which anything exists or is done, made, used etc.
    - ~~Primary purpose is the predominant purpose or the purpose highest in rank or importance; chief; principal.~~ → suggest delete as this doesn't appear elsewhere in the document.

We'd be happy to jump on a call to discuss if helpful,

s47F

s47F (she/her)
Director, Privacy Reform Implementation
Office of the Australian Information Commissioner
Melbourne
P s47E(d) E s47E(d) @oaic.gov.au

Working remotely from Melbourne, Monday to Friday
The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.

Subscribe to Information Matters

OFFICIAL: Sensitive

From: s47F s47E(d) @eSafety.gov.au>
Sent: Monday, September 8, 2025 11:26 AM
To: s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Cc: s47F s47E(d) @eSafety.gov.au>
Subject: For review by 4pm 9 September: eSafety reg guidance on social media minimum age [SEC=OFFICIAL:Sensitive]
Importance: High

OFFICIAL: Sensitive

the sender and know the content is safe.

OFFICIAL: Sensitive

Hi s47F

I hope you both had a great weekend. As promised, please find attached eSafety's draft SMMA reg guidance for OAIC's review. Due to tight timeframes, we would be grateful for any redline feedback as soon as possible and **no later than 4pm tomorrow**.

As you will see it's a working document and we're continuing to make minor edits and refinements, but the guidance is mostly settled.

We encourage you to read the whole document if possible and have identified specific sections related to privacy for you to consider.

Thank you again for being so collaborative – we look forward to receiving your feedback.

Best,
s47F

s47F
Manager, Social Media Age Restriction
Industry Compliance and Enforcement

She | Her

s47E(d)
esafety.gov.au

signature_4012186592

eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses – land, waters and community. We pay our respects to First Nations people, and to Elders past, present and future.

[1] Article 17 of the *International Covenant on Civil and Political Rights* provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation, and that everyone has the right to the protection of the law against such interference or attacks. For interference with privacy not to be arbitrary, it must be lawful and in accordance with the provisions, aims and objective of the ICCPR and should be reasonable in the particular circumstances.

[2] OSA ss 63DA and 63DB

[3] OSA s 63F

From: s47F
To: s47F s47F s47F
Cc: s47F s47F s47F
Subject: OAIC feedback on AATT draft final report
Date: Thursday, 17 July 2025 4:52:00 PM
Attachments: OAIC Feedback - Age Assurance Technology Trial - Draft Final Report.msg
image012.png
image013.png
image014.png
image015.png
image016.png
image017.png
image018.png
image019.png

Hi all

As discussed - sharing the OAIC's feedback on the draft final report for the Age Assurance Technology Trial, attached for your visibility.

Happy to discuss any aspect.

Kind regards,

s4

s47F (she/her)
Policy and Program Manager | Privacy Reform Implementation
Regulatory Intelligence & Strategy Branch
Office of the Australian Information Commissioner
Sydney | GPO Box 5288 Sydney NSW 2001
P s47E(d) E s47E(d) @oaic.gov.au

The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.

Subscribe to Information Matters

From: s47F
Sent: Thursday, 17 July 2025 12:20 PM
To: s47F ; s47F ; s47F ; s47F
Cc: Ahram Choi ; Ainsleigh Hawke
Subject: eSafety feedback on AATT final report [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

OFFICIAL: Sensitive

Hello everyone,

As discussed, please see attached eSafety's feedback on the draft final report for the Age Assurance Technology Trial.

Please let us know if you have any questions or would like to discuss.

Kind regards,

s47F (She/Her)
Manager – Strategic Policy and Tech Futures
eSafety logo Email-Signautre
s47E(d)
esafety.gov.au

signature_4012186592

eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses — land, waters and community. We pay our respects to First Nations people and to Elders past and present.

OFFICIAL: Sensitive

From: s47F
To: s47F
Cc: KIND,Carly; SAVARY,Marcel; s47F
Subject: OAIC Feedback - Age Assurance Technology Trial - Draft Final Report
Date: Thursday, 17 July 2025 4:48:00 PM

Hi s47F

Thank you for seeking our feedback on the draft final report of the Age Assurance Technology Trial.

We recognise the immense work that has taken place throughout the Trial. In the context of implementing new social media minimum age legislation, and more generally, the findings highlight the responsibility on digital platforms and age assurance service providers to conduct their own privacy impact assessments, and ongoing privacy compliance monitoring, when providing age assurance services to users, in accordance with Australian laws.

Feedback

In the time available and noting the above context, we have reviewed the 'Main Report – Part A' and reviewed references to the OAIC for accuracy. We understand from DITRDCSA that ACCS will incorporate feedback provided on Part A to the other sections of the final report.

While we appreciate that changes were made on 13 June in the context of the preliminary findings, we have provided additional feedback in the numbered paragraphs below. We also refer you to prior feedback provided on 29 April and 17 January for consideration as you and the team iterate the various sections of this draft final report.

1. **Our overarching concerns remain regarding the conclusive references to privacy and language in the report that overstates the privacy evaluation that has taken place in the Australian context.**
    0. The Trial has applied the relevant draft International Standard and has not been a systematic assessment of the privacy impacts of technologies in the deployment context.
    1. As we understand, assessment against the Australian Privacy Principles has not been feasible despite this having been envisaged in the evaluation proposal released on 6 February.
    2. In this light, the OAIC encourages the inclusion of a clear statement in the main report that the trialled technologies have not been assessed for compliance with Australian privacy laws or related legislation.

2. **The full report should be checked for this issue. Specific sentences where the level of analysis could be made clearer in the Main Report – Part A include (see suggested**

changes in red underline and strikethrough :

0. Page 7 – '*Readers can expect a thorough examination of age assurance technologies, including their effectiveness against a broad range of criteria in ISO/IEC FDIS 27566 including accuracy, interoperability, reliability, ease of use, minimisation of bias, protection of privacy and data security and readiness for deployment.'*

1. Page 29 - *In summary, age verification is a technically mature, ~~privacy-conscious~~ and inclusive method of age assurance. When implemented with strong safeguards, ethical oversight and adherence to international standards and Australian laws, it offers a viable and trustworthy solution for protecting children and enforcing age-based access controls in Australia's digital environment.*
2. Page 30 – *Most providers implemented ~~robust,~~ privacy-focused data handling practices, such as securely binding DOB to individuals, minimising retention and returning binary age signals (e.g., "Over 18") - though some configurations retained more data than strictly necessary.*
3. Page 32 – *Vendors demonstrated strong alignment with privacy and security expectations in international standards*
4. Page 42 - *Successive validation systems demonstrated internal consistency and standards alignment. Providers articulated well-defined escalation logic, fallback triggers and confidence thresholds, supported by ~~privacy-preserving data handling and~~ compliance with clauses from ISO/IEC FDIS 27566.*

3. **Given the Trial methodology, we also recommend removing references to 'privacy by design'.**
   0. For example on page 28 – *'Privacy by design and data minimisation were consistently observed across the participating providers'* and page 42 – *'Strong privacy-by-design principles were observed across successive validation stages'*.
   1. Privacy-by-design has a very specific meaning in the Australian context and does not carry weight without application of the Australian Privacy Principles – see: Privacy by design | OAIC.

4. **Discussion of the adequate amount of personal and sensitive information for different systems and contexts would be a valuable addition to the main report.**
   0. This would be an insightful addition given the report contains several findings regarding data minimisation and unnecessary data retention.
   1. This information should be lifted out of practice statements and any other relevant documents and ideally summarised in the main report.

5. **There are numerous references to privacy, especially in the sections on age estimation and age inference, which require far more detail and specificity to be meaningful and informative**.

0. Without this detail, terms such as 'privacy sensitive', 'privacy-respecting', 'privacy-preserving' are inflated.

1. We recommend these phrases be replaced with a specific description of the relevant risk and control/mitigation.

2. We also recommend checking and fixing areas of the report that make claims that are inconsistent when read together. For example on page 28 – *'Privacy by design and data minimisation* ***were consistently observed*** *across the participating providers.* ***In most cases,*** *systems were designed to avoid long-term storage of full identity or biometric information.'*

3. This should be fixed through using less conclusive phrasing and adding numbers and detail to neutrally explain the ways in which a method or technology mitigates a described risk.

6. **We request the following adjustments to references to the OAIC in Methodology and Ethics – Part B.**
   0. Page 46 – We would like the below text in red strikethrough to be removed for accuracy as our intention with the meeting on 13 March 2025 was simply to be briefed on the privacy aspects of the Trial within our capacity as an external stakeholder.

> ***'B11.2 Engagement with the OAIC***
> ~~***Ethics oversight and privacy compliance***~~
> - ~~*The Trial proactively liaised with the OAIC to adapt safeguarding practices around personal and biometric data for minors, including collaboration on the Trial's Ethics Committee.*~~
>
> ***Participant privacy safeguards***
> - *The School information pack, the informative guide created to assist schools with understanding what participation in the Trial would look like, clearly informed participants and families that they could contact the OAIC with any concerns about privacy or data use, embedding regulatory oversight at the participant-facing level.'*

   - Page 48,74,and 81– We would like the below text in red strikethrough to be removed for accuracy. The OAIC provided invited feedback as an external stakeholder but was not required to provide checks and clearances as may have been the case for others listed.

> *'When it came to Final Report Production, the quality control associated with that included the necessary pre-publication checks and clearances that were required to include:*
> - *The Department.*
> - *eSafety Commissioner* ~~*and Office of the Australian Information Commissioner (OAIC)*~~.
> - *Ethics Review in accordance with the AIATSIS Code of Ethics for*

Aboriginal and Torres Strait Islander Research.

- *Peer Review by Prof. Toby Walsh at the University of South Wales.'*

- With removal of the above on pages 48, 74 and 81, ACCS may wish to add a separate sentence that says OAIC provided feedback, but not under the checks and clearances heading.

We hope this feedback can be incorporated in the final report.

Kind regards,
s47F

s47F (she/her)
Policy and Program Manager | Privacy Reform Implementation
Regulatory Intelligence & Strategy Branch
Office of the Australian Information Commissioner
Sydney | GPO Box 5288 Sydney NSW 2001
P s47E(d) E s47E(d) oaic.gov.au

The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.

Subscribe to Information Matters

From: s47F s47E(d) @accscheme.com>
Sent: Monday, 30 June 2025 9:06 AM
To: KIND,Carly s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; SAVARY,Marcel s47E(d) @oaic.gov.au>
Cc: s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Subject: Re: Feedback - Age Assurance Technology Trial - OAIC Preliminary Findings Discussion [SEC=OFFICIAL]

Dear Carly,

I'm really pleased to be able to send you a copy of the final draft content for the Age Assurance Technology Trial reports, which has today been submitted to the Department for Infrastructure. The content for all 10 reports are now completed an the current version is you your AATT Share File for each of them by clicking on the link below.

AATT Share Folder - OAIC

I have also attempted to do a PDF Combined Report of all 10 reports, but for some reason it wouldn't let me do Part B (I'll have to examine why that is). In the meantime the other 9 Parts are on the following link (please note that the combined report is 707 pages and 188,465 words - so I'd think twice before hitting print!)

[PDF Draft 20250630] Combined Report.pdf

You will also find your share file:

- All of the consolidated practice statements for all of the technologies under test
- All of the consolidated privacy policies for all vendors and participants in the trial
- All of the consolidated vendor interviews conducted with representatives from participant companies
- All of the consolidated test reports for all of the vendors
  (Please Note: these add up to 1,926 pages)
  Also, not all of these documents have yet been checked and verified by the vendors)

We now move to our pre-publication phase. Broadly, this includes:

- Transfer of all of the content to Adobe InDesign and then fitting into our reporting template
- Carrying out Procedural Fairness checks on all of the content and supporting materials
- A further ethics and legal review (including checks on copyright materials)
- Implementation of any further feedback from your team, the Department or eSafety received before **Friday 18th July 2025**.
- Proof Reading, Cross-Referencing, Hyperlinks Checks and Verification of all materials

We are aiming to complete that process by 31st July.

I hope that all of this work meets with your approval. It has been a fabulous project to work on and is, by far, the biggest ever analysis of this technology anywhere in the World. I hope it is going to enormously useful for you as you progress with your duties.

Best Regards

s47F

From: KIND,Carly s47E(d) @oaic.gov.au>
Sent: 12 June 2025 12:39 AM
To: s47F s47E(d) @accscheme.com>; s47F s47E(d) @oaic.gov.au>; SAVARY,Marcel s47E(d) @oaic.gov.au>
Cc: s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Subject: RE: Feedback - Age Assurance Technology Trial - OAIC Preliminary Findings Discussion [SEC=OFFICIAL]

Thanks s47F , we'll review and come back to you with any feedback.

Carly

From: s47F s47E(d) @accscheme.com>
Sent: Wednesday, 11 June 2025 6:55 PM
To: KIND,Carly s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Cc: BOAG,Annan s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Subject: Re: Feedback - Age Assurance Technology Trial - OAIC Preliminary Findings Discussion [SEC=OFFICIAL]

Hi Carly,

I hope that you and the team are well.

Following on from the draft preliminary findings, we have been conducting further ethics and legal reviews and taking on board feedback from the Government, eSafety Commissioner, yourselves and others. As a result, we are making a few amendments to the preliminary findings, which are attached (with a tracked changes version too).

I continue to welcome feedback from you and the team as we work on developing the full report.

Best Regards

s47F

From: KIND,Carly s47E(d) @oaic.gov.au>
Sent: 26 May 2025 5:51 AM
To: s47F s47E(d) @accscheme.com>; s47F s47E(d) @oaic.gov.au>
Cc: BOAG,Annan s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Subject: RE: Feedback - Age Assurance Technology Trial - OAIC Preliminary Findings Discussion [SEC=OFFICIAL]

Dear s47F

Many thanks for sharing this Preliminary Report, I'm looking forward to reviewing and the team will do the same and forward any feedback that surfaces.

Kind regards,

Carly

From: s47F s47E(d) @accscheme.com>
Sent: Sunday, 18 May 2025 7:55 PM
To: s47F s47E(d) @oaic.gov.au>
Cc: KIND,Carly s47E(d) @oaic.gov.au>; BOAG,Annan s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Subject: Re: Feedback - Age Assurance Technology Trial - OAIC Preliminary Findings Discussion [SEC=OFFICIAL]

Dear Carly,

Thank you to you and the team for all of your comments and suggestions in relation to our preliminary report. As promised, our report has been through our initial internal 'challenge' sessions with lawyers and our audit team; we have sought initial feedback from yourselves, eSafety Commissioner and DITRDCA; and our team have been refining their analysis appropriately.

I am, therefore, please to be able to provide to you, in confidence, a final version of our Preliminary Report. You will note that the '14' observations have been refined to '12' observations and it is entirely possible that they will be refined further as we head towards our final report.

We also recognise that there is plenty of opportunity for sub-editing, reducing repetition and improving the clarity of connections between sections and across aspects of the report. We will be addressing these in our final report, as well as further challenge sessions, quality assurance and pre-publication final checks.

In the meantime, however, please do not consider the attached as a final or settled position. We would still welcome any further feedback from you or your team as we continue to develop the final report.

Best Regards

s47F

From: s47F s47E(d)
Sent: 29 April 2025 6:26 AM
To: s47F s47E(d) @accscheme.com>
Cc: KIND,Carly s47E(d) @oaic.gov.au>; BOAG,Annan s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Subject: Feedback - Age Assurance Technology Trial - OAIC Preliminary Findings Discussion [SEC=OFFICIAL]

Hi s47F

Thank you for your time yesterday and for taking us through the 14 emerging observations from the ongoing Age Assurance Technology Trial. We thought it best to follow up in writing capturing the feedback we provided yesterday.

As discussed in the meeting, our concerns relate to the particular phrasing of the observations and the risk of the inference being that the tested technologies are legally compliant when that level of analysis has not taken place.

For transparency, we would appreciate if refinements could be made to make clear in the observations that the trialled technologies have not been assessed for compliance against the Privacy Act and related legislation such as the privacy provisions in Part 4A of the Online Safety Act. Further detail is provided below.

Broad language inferring privacy compliance

Our concerns centre around the use of relatively broad terms related to privacy that don't appear to be calibrated to the Privacy Act/Australian Privacy Principles (APPs)/related legislation but are more general statements around privacy. For example, 'privacy-preserving', 'appropriate data-handling practices', 'no evidence of exploitative data practices' and 'collateral intrusion to individual privacy'.

Our view is that technologies that involve the handling of personal information cannot be claimed as inherently 'privacy-preserving' or 'appropriate' in the Australian context without applying the APPs (and any related legislation) to the actual context in which the technology operates. Under Australian privacy law, compliance is dependent on a range of contextual variables – such as fairness, proportionality, necessity, whether the relevant standard of consent has been met, the lifecycle of the personal information that is handled, and so on. We can appreciate the draft International Standard has been closely applied noting there are differences between the standard and Australian legal obligations.

We had encouraged analysis of the APPs in the Trial context and a cautious approach to the assessment of privacy in our feedback on 17 January 2025, and while this was incorporated into the final evaluation proposal (p55), the observations could be adjusted to better reflect this. This could be achieved by perhaps reiterating some of the content in the evaluation proposal. For example, it was 'not feasible to perform a comprehensive privacy assessment in this trial' (p55) and 'technical testing for protection of privacy' was out of scope (p40). During the meeting you mentioned there may also be some wording in the participation agreements with vendors about the trial not constituting a privacy assessment.

The above will also assist in setting regulatory expectations. Relying parties, age assurance providers and the public should have a realistic view of the assessment that has occurred so that any early compliance activity by OAIC is anticipated. This will also assist parties in understanding what has and hasn't been done for any certification/accreditation purposes. It will be the OAIC's role to assess what age assurance systems are actually doing in the context in which these systems are potentially deployed, to investigate any complaints by individuals and identify non-compliance.

<u>Other points raised</u>

- It would be valuable if the report could discuss the necessary amount of personal and sensitive information for different systems and contexts. During the meeting you mentioned the tech participant's practice statements may have this information.
- Regarding Observation 1, the phrasing 'in the context of Australia' may be inconsistent with the assessment undertaken. A better phrase may be 'through adherence to the international standard in the Australian context'.
- It would be valuable if the tech-side observations could be balanced with observations from the user's perspective, including insights about useability challenges. During the meeting there was discussion of the enthusiasm and willingness of children to be involved but more reporting about their fears, concerns and expectations of privacy would be natural observations from the user testing.

During the meeting the team kindly shared insights from the school testing which included some of the children's concerns.

- Additional queries not raised at the meeting:
  - Would Observation 13 extend to future purposes generally?
  - Should Observation 14 capture legislative compliance for public trust?

We hope this feedback can be incorporated and look forward to the next steps in this important work, including the opportunity to comment on the draft final report.

Happy to set up another discussion if that would be helpful.

Kind regards,
s47F

s47F (she/her)
Policy and Program Manager | Privacy Reform Implementation
Regulatory Intelligence & Strategy Branch
Office of the Australian Information Commissioner
Sydney | GPO Box 5288 Sydney NSW 2001
P s47E(d) E s47E(d) @oaic.gov.au

The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.

Subscribe to Information Matters

From: s47F s47E(d) @accscheme.com>
Sent: Monday, 21 April 2025 3:52 PM
To: s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) s47F s47E @avpassociation.com>
Cc: BOAG,Annan s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Subject: Re: Age Assurance Technology Trial - OAIC Preliminary Findings Discussion

Hi s47F

I hope that you have had an enjoyable Easter Break. In advance of our meeting next Monday with your team, I wanted to share with our our emerging observations from the ongoing Age Assurance Technology Trial. These will be subject to our challenge sessions next week and some further refinement before being incorporated into our final report. They must, therefore, be treated in confidence and as being subject to further review.

We propose to make 14 observations (noting that our remit did not extend to making recommendations):

1. **Age assurance can be done in the Australian context, conveniently, privately and efficiently.**

Age assurance can be done in Australia. This report sets out how our analysis of age assurance systems in the context of Australia demonstrates how they are secure, privacy-preserving, robust and effective. There is a plethora of choice available for providers of age-restricted goods, content, services, venues or spaces to select the most appropriate systems for their use case.

2. **No technological barriers prevent its implementation to meet policy requirements.**

We found no technological impediment to age assurance technologies being utilised in response to age-related eligibility requirements established by policy makers. We identified careful, critical thinking by providers and policy makers on the development and deployment of age assurance systems, considering efficacy, privacy, data and security concerns. Some systems were easier for initial implementation than others, but they were all eventually capable of integration to a user journey.

3. **Age assurance service provider claims were independently validated.**

We found that the practice statements provided by technology providers with a technology readiness level of 7 or above accurately and fairly reflected the technological capabilities of their products, processes or services. Those with a technology readiness level below 7 would need further analysis when their systems mature. By making the statements publicly available from the trial, they will help to maintain a transparent and open approach to what age assurance systems are actually doing and it is anticipated that public trust and confidence will be enhanced as a result.

4. **There is no one-size-fits-all solution, but wide choices for different use cases.**

We found a plethora of approaches that fit different use cases in different ways, but we did not find a single ubiquitous solution that would suit all use cases. The range of possibilities across the 53 trial participants demonstrates a rich and rapidly evolving range of services each tailored to particular use cases and designed for customer ease and reducing friction.

5. **We found a dynamic, innovative and evolving age assurance service sector.**

We found a vibrant, creative and innovative age assurance service sector with both technologically advanced and deployed solutions and a pipeline of new technologies

transitioning from research to minimum viable product to testing and deployment stages indicating an evolving choice and future opportunities for developers. We found private-sector investment and opportunities for growth and economic development.

6. **We found robust, appropriate, secure data handling practices.**

We found deep understanding and appropriate policy decisions regarding the handling of personal data – particularly by independent age assurance service providers, where no evidence of exploitative data practices was found. Separating age assurance services from those of relying parties was useful in maintaining appropriate data handling practices.

7. **There is broad demographic consistency in the operation of the systems.**

The systems under test performed broadly consistently across demographic groups and despite an acknowledged deficit in training age analysis systems with data about indigenous populations, we found no discernible difference in the outcomes for First Nations and Torres Straights Islander Peoples using the age assurance systems. We found variances across race and gender were within tolerable parameters.

8. **There is room for continuous technical improvement including emerging technologies.**

We found opportunities for technological improvement of age assurance systems including through one-way blind access to government verification; enabling connection to data holder services (like digital wallets); and improving the accreditation, certification, continuous monitoring, testing and analysis of the systems in accordance with the evolving international standards.

9. **There are limitations to parental control systems particularly during adolescence.**

Although we found that parental control and consent systems were initially effective, we found limited evidence that they could cope with the evolving capacity of children (particularly through adolescence), were able to enhance the rights of children to participate in the breadth of digital experiences or were effective and secure in the management of a child's digital footprint.

10. **There are innovative, interoperable age token management systems emerging into the marketplace with future potential.**

We found opportunities for holding and managing age assurance results (tokens) at different levels of the technology stack, but none of the solutions offered for the trial have yet reached an appropriate technology readiness level to be able to demonstrate this in practice. This we anticipate will improve as holder services (like digital wallets) enhance their capabilities. The emerging concept of 'app-store' level or 'device' level age assurance

was explored and found to lack effective thinking about risks and unintended consequences.

11. **Proximity to risk builds user trust and understanding of the need for age assurance.**

Age assurance activities deployed at or near to the age-related risk provided a clearer linkage for users on the need for the age assurance process. This proximity to risk is an important factor in making the age assurance process trustworthy, transparent and proportionate. We found the potential for collateral intrusion to individual privacy the less proximate age assurance systems were to the risk identified.

12. **Systems demonstrated cybersecurity compliance and most actively counter AI-driven threats.**

We found that the systems tested were secure, well-built and established in accordance with information security management standards. We found an industry that is acutely aware of, planning for and actively defeating artificial intelligence generated threat vectors – such as presentation attack, video injection attack and document or record forgeries and counterfeits.

13. **We caution against inadvertently promoting unnecessary data retention through audit trails driven by anticipating the future needs of regulators or judicial processes (such as Coroners).**

We found some concerning evidence that service providers were over-anticipating the eventual needs of regulators or judicial processes about providing data for future investigations. Some providers were found to be building tools to enable Regulators, Law Enforcement or Coroners to retrace the actions taken by individuals to verify their age which could lead to potential security vulnerabilities without clear guidance and policy decisions.

14. **Accreditation and certification, enduring system monitoring and recertification of age assurance systems is essential to enhancing public trust.**

The standards-based approach adopted by the Trial, including through the ISO/IEC 27566 Series, the IEEE 2089.1 and the Systems and Software Engineering - Product Quality Model all provide a strong basis for the development of accreditation of conformity assessment and subsequent certification of individual age assurance providers in accordance with Australia's National Quality Infrastructure.

I hope that makes for interesting reading and I look forward to meeting with your team next Monday.

Best Regards

s47F

From:
Sent: Sunday, April 13, 2025 12:37 PM
Subject: Age Assurance Technology Trial - OAIC Preliminary Findings Discussion

---

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 327 692 370 922 8
Passcode: 9BU2rN3Y

For organisers: Meeting options

Notice:

The information contained in this email message and any attached files may be confidential information, and may also be the subject of legal professional privilege. If you are not the intended recipient any use, disclosure or copying of this email is unauthorised. If you received this email in error, please notify the sender by contacting the department's switchboard on 1300 488 064 during business hours (8:30am - 5pm Canberra time) and delete all copies of this transmission together with any attachments.

Notice:

The information contained in this email message and any attached files may be confidential information, and may also be the subject of legal professional privilege. If you are not the intended recipient any use, disclosure or copying of this email is unauthorised. If you received this email in error, please notify the sender by contacting the department's switchboard on 1300 488 064 during business hours (8:30am - 5pm Canberra time) and

delete all copies of this transmission together with any attachments.

From: s47F
To: s47F s47F ; s47F
Cc: BOAG,Annan; s47E(d) @infrastructure.gov.au; s47F
Subject: FW: Feedback - Age Assurance Technology Trial - OAIC Preliminary Findings Discussion [SEC=OFFICIAL]
Date: Tuesday, 6 May 2025 1:16:09 PM

Dear colleagues
Below is the feedback we shared with s47F and his colleagues following a presentation of the preliminary findings from the Age Assurance Technology Trial. As mentioned in our last catchup, we shared with the team some concerns we have regarding the broad language used in regards to privacy, and that the language may infer compliance with the Australian Privacy Principles, when the Trial has not undertaken such analysis. We hope this will be helpful in your own evaluations of the findings and as the trial progresses. We are happy to discuss further in our regular meetings or on a call,
Thanks

s47F (she/her)
Director, Privacy Reform Implementation
Office of the Australian Information Commissioner
Melbourne
P s47E(d) E s47E(d) @oaic.gov.au
Working remotely from Melbourne, Monday to Friday
The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.
Subscribe to Information Matters

From: s47F
Sent: Tuesday, April 29, 2025 3:27 PM
To: s47E(d) @accscheme.com
Cc: KIND,Carly ; BOAG,Annan ; s47F ; s47F ; s47F
Subject: Feedback - Age Assurance Technology Trial - OAIC Preliminary Findings Discussion [SEC=OFFICIAL]

Hi s47F
Thank you for your time yesterday and for taking us through the 14 emerging observations from the ongoing Age Assurance Technology Trial. We thought it best to follow up in writing capturing the feedback we provided yesterday.
As discussed in the meeting, our concerns relate to the particular phrasing of the observations and the risk of the inference being that the tested technologies are legally compliant when that level of analysis has not taken place.
For transparency, we would appreciate if refinements could be made to make clear in the observations that the trialled technologies have not been assessed for compliance against the Privacy Act and related legislation such as the privacy provisions in Part 4A of the Online Safety Act. Further detail is provided below.

Broad language inferring privacy compliance

Our concerns centre around the use of relatively broad terms related to privacy that don't appear to be calibrated to the Privacy Act/Australian Privacy Principles (APPs)/related legislation but are more general statements around privacy. For example, 'privacy-preserving', 'appropriate data-handling practices', 'no evidence of exploitative data practices' and 'collateral intrusion to individual privacy'.
Our view is that technologies that involve the handling of personal information cannot be claimed as inherently 'privacy-preserving' or 'appropriate' in the Australian context without

applying the APPs (and any related legislation) to the actual context in which the technology operates. Under Australian privacy law, compliance is dependent on a range of contextual variables – such as fairness, proportionality, necessity, whether the relevant standard of consent has been met, the lifecycle of the personal information that is handled, and so on. We can appreciate the draft International Standard has been closely applied noting there are differences between the standard and Australian legal obligations. We had encouraged analysis of the APPs in the Trial context and a cautious approach to the assessment of privacy in our feedback on 17 January 2025, and while this was incorporated into the final evaluation proposal (p55), the observations could be adjusted to better reflect this. This could be achieved by perhaps reiterating some of the content in the evaluation proposal. For example, it was 'not feasible to perform a comprehensive privacy assessment in this trial' (p55) and 'technical testing for protection of privacy' was out of scope (p40). During the meeting you mentioned there may also be some wording in the participation agreements with vendors about the trial not constituting a privacy assessment.

The above will also assist in setting regulatory expectations. Relying parties, age assurance providers and the public should have a realistic view of the assessment that has occurred so that any early compliance activity by OAIC is anticipated. This will also assist parties in understanding what has and hasn't been done for any certification/accreditation purposes. It will be the OAIC's role to assess what age assurance systems are actually doing in the context in which these systems are potentially deployed, to investigate any complaints by individuals and identify non-compliance.

Other points raised

- It would be valuable if the report could discuss the necessary amount of personal and sensitive information for different systems and contexts. During the meeting you mentioned the tech participant's practice statements may have this information.
- Regarding Observation 1, the phrasing 'in the context of Australia' may be inconsistent with the assessment undertaken. A better phrase may be 'through adherence to the international standard in the Australian context'.
- It would be valuable if the tech-side observations could be balanced with observations from the user's perspective, including insights about useability challenges. During the meeting there was discussion of the enthusiasm and willingness of children to be involved but more reporting about their fears, concerns and expectations of privacy would be natural observations from the user testing. During the meeting the team kindly shared insights from the school testing which included some of the children's concerns.
- Additional queries not raised at the meeting:
    - Would Observation 13 extend to future purposes generally?
    - Should Observation 14 capture legislative compliance for public trust?

We hope this feedback can be incorporated and look forward to the next steps in this important work, including the opportunity to comment on the draft final report.

Happy to set up another discussion if that would be helpful.

Kind regards,

s47F

s47F (she/her)

Policy and Program Manager | Privacy Reform Implementation
Regulatory Intelligence & Strategy Branch
Office of the Australian Information Commissioner
Sydney | GPO Box 5288 Sydney NSW 2001
P s47E(d) E s47E(d) @oaic.gov.au

The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.
Subscribe to Information Matters

From: s47F s47E(d) @accscheme.com>
Sent: Monday, 21 April 2025 3:52 PM
To: s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>; s47F s47 @avpassociation.com>
Cc: BOAG,Annan s47E(d) @oaic.gov.au>; s47F s47E(d) @oaic.gov.au>
Subject: Re: Age Assurance Technology Trial - OAIC Preliminary Findings Discussion

Hi s47F

I hope that you have had an enjoyable Easter Break. In advance of our meeting next Monday with your team, I wanted to share with our our emerging observations from the ongoing Age Assurance Technology Trial. These will be subject to our challenge sessions next week and some further refinement before being incorporated into our final report. They must, therefore, be treated in confidence and as being subject to further review.
We propose to make 14 observations (noting that our remit did not extend to making recommendations):

1. **Age assurance can be done in the Australian context, conveniently, privately and efficiently.**

Age assurance can be done in Australia. This report sets out how our analysis of age assurance systems in the context of Australia demonstrates how they are secure, privacy-preserving, robust and effective. There is a plethora of choice available for providers of age-restricted goods, content, services, venues or spaces to select the most appropriate systems for their use case.

2. **No technological barriers prevent its implementation to meet policy requirements.**

We found no technological impediment to age assurance technologies being utilised in response to age-related eligibility requirements established by policy makers. We identified careful, critical thinking by providers and policy makers on the development and deployment of age assurance systems, considering efficacy, privacy, data and security concerns. Some systems were easier for initial implementation than others, but they were all eventually capable of integration to a user journey.

3. **Age assurance service provider claims were independently validated.**

We found that the practice statements provided by technology providers with a technology readiness level of 7 or above accurately and fairly reflected the technological capabilities of their products, processes or services. Those with a technology readiness level below 7 would need further analysis when their systems mature. By making the statements publicly available from the trial, they will help to maintain a transparent and open approach to what age assurance systems are actually doing and it is anticipated that public trust and confidence will be enhanced as a result.

4. **There is no one-size-fits-all solution, but wide choices for different use cases.**

We found a plethora of approaches that fit different use cases in different ways, but we did not find a single ubiquitous solution that would suit all use cases. The range of possibilities across the 53 trial participants demonstrates a rich and rapidly evolving range of services each tailored to particular use cases and designed for customer ease and reducing friction.

5. **We found a dynamic, innovative and evolving age assurance service sector.**

We found a vibrant, creative and innovative age assurance service sector with both technologically advanced and deployed solutions and a pipeline of new technologies transitioning from research to minimum viable product to testing and deployment stages indicating an evolving choice and future opportunities for developers. We found private-sector investment and opportunities for growth and economic development.

6. **We found robust, appropriate, secure data handling practices.**

We found deep understanding and appropriate policy decisions regarding the handling of personal data – particularly by independent age assurance service providers, where no evidence of exploitative data practices was found. Separating age assurance services from those of relying parties was useful in maintaining appropriate data handling practices.

7. **There is broad demographic consistency in the operation of the systems.**

The systems under test performed broadly consistently across demographic groups and despite an acknowledged deficit in training age analysis systems with data about indigenous populations, we found no discernible difference in the outcomes for First Nations and Torres Straights Islander Peoples using the age assurance systems. We found variances across race and gender were within tolerable parameters.

8. **There is room for continuous technical improvement including emerging technologies.**

We found opportunities for technological improvement of age assurance systems including through one-way blind access to government verification; enabling connection to data holder services (like digital wallets); and improving the accreditation, certification, continuous monitoring, testing and analysis of the systems in accordance with the evolving international standards.

9. **There are limitations to parental control systems particularly during adolescence.**

Although we found that parental control and consent systems were initially effective, we found limited evidence that they could cope with the evolving capacity of children

(particularly through adolescence), were able to enhance the rights of children to participate in the breadth of digital experiences or were effective and secure in the management of a child's digital footprint.

10. **There are innovative, interoperable age token management systems emerging into the marketplace with future potential.**

We found opportunities for holding and managing age assurance results (tokens) at different levels of the technology stack, but none of the solutions offered for the trial have yet reached an appropriate technology readiness level to be able to demonstrate this in practice. This we anticipate will improve as holder services (like digital wallets) enhance their capabilities. The emerging concept of 'app-store' level or 'device' level age assurance was explored and found to lack effective thinking about risks and unintended consequences.

11. **Proximity to risk builds user trust and understanding of the need for age assurance.**

Age assurance activities deployed at or near to the age-related risk provided a clearer linkage for users on the need for the age assurance process. This proximity to risk is an important factor in making the age assurance process trustworthy, transparent and proportionate. We found the potential for collateral intrusion to individual privacy the less proximate age assurance systems were to the risk identified.

12. **Systems demonstrated cybersecurity compliance and most actively counter AI-driven threats.**

We found that the systems tested were secure, well-built and established in accordance with information security management standards. We found an industry that is acutely aware of, planning for and actively defeating artificial intelligence generated threat vectors – such as presentation attack, video injection attack and document or record forgeries and counterfeits.

13. **We caution against inadvertently promoting unnecessary data retention through audit trails driven by anticipating the future needs of regulators or judicial processes (such as Coroners).**

We found some concerning evidence that service providers were over-anticipating the eventual needs of regulators or judicial processes about providing data for future investigations. Some providers were found to be building tools to enable Regulators, Law Enforcement or Coroners to retrace the actions taken by individuals to verify their age which could lead to potential security vulnerabilities without clear guidance and policy decisions.

14. **Accreditation and certification, enduring system monitoring and recertification of age assurance systems is essential to enhancing public trust.**

The standards-based approach adopted by the Trial, including through the ISO/IEC 27566 Series, the IEEE 2089.1 and the Systems and Software Engineering - Product Quality Model all provide a strong basis for the development of accreditation of conformity assessment and subsequent certification of individual age assurance providers in accordance with

Australia's National Quality Infrastructure.
I hope that makes for interesting reading and I look forward to meeting with your team next Monday.
Best Regards
s47F

From:
Sent: Sunday, April 13, 2025 12:37 PM
Subject: Age Assurance Technology Trial - OAIC Preliminary Findings Discussion

---

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 327 692 370 922 8
Passcode: 9BU2rN3Y

For organisers: Meeting options

From: s47F
To: s47F s47F
Cc: s47F s47F
Subject: RE: For review by 11am 25/6 - Notes from OAIC x eSafety SMMA session [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]
Date: Wednesday, 25 June 2025 9:18:50 AM
Attachments: image012.png
image013.png
image014.png
image015.png
image016.png
image017.png
image018.png
image019.png

OFFICIAL: Sensitive//Legal Privilege

Hi s47F

Thanks for sharing this helpful summary of our conversation and it will be good grounding for the meeting tomorrow, our suggested edits are below in purple (comments in Italics)

s47F

Implementation of the SMMA for new vs existing users

New users:

- Must undergo an age assurance (AA) check at onboarding (Notice applies. Consent applies if collecting sensitive information for the check. Collection should be limited to only reasonably necessary personal or sensitive information. Destruction applies per s63F).

Existing users:

- Platforms may:
  - Do a one-off AA check (Notice applies. Consent applies if collecting sensitive information for the check. Collection should be limited to only reasonably necessary personal or sensitive information. Destruction applies per s63F).
  - Infer age from existing data (Notice applies. User consent applies due to the likely handling of sensitive information to infer age). Collection should be limited to only reasonably necessary personal information i.e. inferred age. Ideally the inference should just be <16 or >16. Destruction applies per s63F.
  - Users with verified age information or a prior verified AA check on the platform may not require re-engagement. (Notice still applies to secondary use of this age information for SMMA purposes. Consent would apply if this involved secondary use of sensitive information. s63F does not apply because this would be a secondary use rather than a collection).

Age assurance checks

- Platforms may implement AA either internally or through third-party providers.
- Section 63F of the *Online Safety Act 2021* applies where an ~~platform~~entity holds personal information about an individual that was collected for the purpose of taking reasonable steps to prevent age-restricted users having an account.
- A simple, de-identified 'verified' or 'not verified' outcome or token from an age assurance process is not considered personal information if it is not linked to an identified individual, or an individual who is reasonably identifiable.
- However, if the data includes or can be linked to a specific individual's age, it may become personal information. The platform would be required to destroy this information under s63F(3).

Age inference from existing user data

- If a platform sought to use existing information about a user (e.g. posts, account information) to infer or generate the users age for the purposes of the SMMA obligation, consent would need to be obtained from the user. As above - Notice applies. User consent applies due to the likely handling of sensitive information to infer age. Collection should be limited to only reasonably necessary personal information i.e. inferred age. Ideally the inference should just be <16 or >16. Destruction applies per s63F.
- The collected age inference data would be considered 'personal information', and s63F would apply.
- The collected age inference data would need to be destroyed under s63F(3) however the original data would not need to be destroyed and could be kept for its original purposes.
  - An example of this would be if a platform originally collected a user's behavioural data for the purposes of targeted advertising, and then used it for the secondary purpose of age assurance under the SMMA obligation.
  - The age inference data would need to be destroyed, but the behavioural data could continue to be held and used for their original advertising purposes.

Users with existing verified age information

- If a platform has previously collected verified age-related information about a user for a different purpose, and this same information is then used ~~to infer the user's age~~ for the purposes of the SMMA obligation (i.e. secondary purpose), s63F does not apply because the obligation can be met through a use not a collection.
  - Consent may not be required from users for platforms to verify age using this method. Under Australian Privacy Principle 6, an organisation can use or disclose personal information for a secondary purpose if the

individual would reasonably expect it AND the secondary purpose is related to the primary purpose of collection (or **directly** related in the case of sensitive information). Age-related information could therefore be used for AA purposes, without requiring user consent. Notice still applies.

- Note that the age-related information must be verified, such as an identity document or the outcome of a previous AA check. Self-declaration of age will not be sufficient under the reasonable steps.

Data retention

- Platforms must retain evidence that they have taken reasonable steps to prevent age-restricted users from having accounts.
- The OAIC ~~recommends that~~ agrees the evidence retained should include the AA method used, the AA provider, and the outcome (i.e. verified/not verified) - if it is not linked to an identified individual, or an individual who is reasonably identifiable.
- Retention of tokens or verification outcomes is permissible if information is de-identified.
- Separation principles are recommended; it is best to store data and keys separately to avoid re-identification.

s47C [redacted]

- Compliance under Section 63F *do you mean 63D?* is not a one-time obligation. Platforms are expected to engage in ongoing monitoring to ensure users remain over the minimum age - *is this the same purpose as guarding against circumvention?*
- This includes removing underage users if discovered, re-verifying users if behavioural data suggests they may be underage, and ensuring that users who were verified as over 16 continue to meet that threshold.
- User reporting mechanisms must strike a balance between being effective and not overly burdensome, as overly frictionless systems may be abused for malicious reporting.
  - User reporting may trigger an AA process.

Circumvention

Circumvention of age assurance can occur in two primary ways: age-based and location-based:

- Age-based circumvention includes tactics like spoofing, account selling, or collusion (e.g. family members assisting with facial scans).
- Location-based circumvention may involve users masking their location using VPNs or other tools, which means platforms must rely on more than just IP addresses—such as phone numbers or device signals—to verify user location.
  - The OAIC will further consider the types of location data that may be considered personal information. We will consider and get back to you

Consent

- While the Privacy Act does not require consent for the secondary use of or collection of personal information, it does for sensitive information.
- Section 63F(2) introduces a higher consent threshold than the Privacy Act, which the OAIC supports for the purposes of the SMMA.
- Determining a child's capacity to consent is challenging under the SMMA, as platforms may not know the user's age.
- Co-consent models involving parents may be a potential solution.

s47F [redacted]
Director, Privacy Reform Implementation
Office of the Australian Information Commissioner
Melbourne
P s47E(d) [redacted] E s47E(d) [redacted] @oaic.gov.au
Working remotely from Melbourne, Monday to Friday
The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.
Subscribe to Information Matters

OFFICIAL: Sensitive//Legal Privilege

From: s47F [redacted]
Sent: Tuesday, June 24, 2025 6:07 PM
To: s47F [redacted] ; s47F [redacted]
Cc: s47F [redacted] ; s47F [redacted]
Subject: For review by 11am 25/6 - Notes from OAIC x eSafety SMMA session [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]
Importance: High

OFFICIAL: Sensitive//Legal Privilege

the sender and know the content is safe.

OFFICIAL: Sensitive
Legal Privilege

Hi s47F ,

Thanks for your time today – it was really valuable running through some of the SMMA privacy considerations together. We wanted to run our notes from today's meeting by you both to ensure we have accurately captured the key points. Apologies for the time crunch, but we would appreciate if you could review the below notes and get back to us with any edits **ASAP tomorrow morning, before 11am** if possible. We need to progress a brief to senior exec before COB.

Implementation of the SMMA for new vs existing users

New users:

- Must undergo an age assurance (AA) check at onboarding.

Existing users:

- Platforms may:
  - Do a one-off AA check.
  - Infer age from existing data (with user consent).
  - Users with verified age information or a prior verified AA check on the platform may not require re-engagement.

Age assurance checks

- Platforms may implement AA either internally or through third-party providers.
- Section 63F of the *Online Safety Act 2021* applies where a platform holds personal information about an individual that was collected for the purpose of taking reasonable steps to prevent age-restricted users having an account.
- A simple, de-identified 'verified' or 'not verified' outcome or token from an age assurance process is not considered personal information.
- However, if the data includes or can be linked to a specific age, it may become personal information. The platform would be required to destroy this information under s63F(3).

Age inference from existing user data

- If a platform sought to use existing information about a user (e.g. posts, account information) to infer the users age for the purposes of the SMMA obligation, consent would need to be obtained from the user.
- The age inference data would be considered 'personal information', and s63F would apply.
- The age inference data would need to be destroyed under s63F(3) however the original data would not need to be destroyed and could be kept for its original purposes.
  - An example of this would be if a platform originally collected a user's behavioural data for the purposes of targeted advertising, and then used it for the secondary purpose of age assurance under the SMMA obligation.
  - The age inference data would need to be destroyed, but the behavioural data could continue to be held and used for their original advertising purposes.

Users with existing verified age information

- If a platform has previously collected verified age-related information about a user for a different purpose, and this information is then used to infer the users age for the purposes of the SMMA obligation (i.e. secondary purpose), s63F does not apply.
  - Consent may not be required from users for platforms to verify age using this method. Under Australian Privacy Principle 6, an organisation can use or disclose personal information for a secondary purpose if the individual would reasonably expect it. Age-related information could therefore be used for AA purposes, without requiring user consent.
  - Note that the age-related information must be verified, such as an identity document or the outcome of a previous AA check. Self-declaration of age will not be sufficient under the reasonable steps.

Data retention

- Platforms must retain evidence that they have taken reasonable steps to prevent age-restricted users from having accounts.
- The OAIC recommends that the evidence retained should include the AA method used, the AA provider, and the outcome (i.e. verified/not verified).
- Retention of tokens or verification outcomes is permissible if information is de-identified.
- Separation principles are recommended; it is best to store data and keys separately to avoid re-identification.

Ongoing compliance and monitoring

- Compliance under Section 63F is not a one-time obligation. Platforms are expected to engage in ongoing monitoring to ensure users remain over the minimum age.
- This includes removing underage users if discovered, re-verifying users if behavioural data suggests they may be underage, and ensuring that users who were verified as over 16 continue to meet that threshold.
- User reporting mechanisms must strike a balance between being effective and not overly burdensome, as overly

frictionless systems may be abused for malicious reporting.
  - User reporting may trigger an AA process.

Circumvention

Circumvention of age assurance can occur in two primary ways: age-based and location-based:

- Age-based circumvention includes tactics like spoofing, account selling, or collusion (e.g. family members assisting with facial scans).
- Location-based circumvention may involve users masking their location using VPNs or other tools, which means platforms must rely on more than just IP addresses—such as phone numbers or device signals—to verify user location.
  - The OAIC will further consider the types of location data that may be considered personal information.

Consent

- While the Privacy Act does not require consent for the collection of personal information, it does for sensitive information.
- Section 63F(2) introduces a higher consent threshold than the Privacy Act, which the OAIC supports for the purposes of the SMMA.
- Determining a child's capacity to consent is challenging under the SMMA, as platforms may not know the user's age.
- Co-consent models involving parents may be a potential solution.

Thanks again,

s47F
Assistant Manager, Social Media Age Restriction
Industry Compliance and Enforcement
She | Her
s47E(d)
esafety.gov.au

signature_4012186592

eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses — land, waters and community. We pay our respects to First Nations people, and to Elders past, present and future.