Australian Government | eSafetyCommissioner

eSafety Submission

Privacy Act Review Report

March 2023

Contents

About eSafety **2**

Basic Online Safety Expectations 2

Industry codes 2

Safety by Design 3

Online safety and privacy **3**

eSafety's comments on report proposals **5**

Child-appropriate practices 5

Children's Online Privacy Code 5

Fair and reasonable test 6

Privacy impact assessment 7

Facial recognition technology 7

Proposed rights of the individual 8

Automated decision making 9

Direct marketing, targeting and trading proposals 9

Individuals exercising their privacy rights 9

Increased enforcement powers 9

About eSafety

The eSafety Commissioner (eSafety) welcomes the opportunity to provide feedback on the Attorney-General's Privacy Act Review Report (the Review).

eSafety is Australia's national independent regulator for online safety. Our purpose is to help safeguard Australians from online harms and to promote safer, more positive online experiences. While eSafety's primary focus is online safety, we also deal with some privacy issues in the context of promoting the safe and responsible use of digital technologies for Australians.

eSafety has a range of regulatory powers and functions provided by the *Online Safety Act 2021* that enables it to coordinate, support and promote online safety activities across the Australian Government. This includes administering four regulatory complaints and investigations schemes, including for cyberbullying of children, cyber abuse of adults, the non-consensual sharing of intimate images, and illegal or restricted online content.

Basic Online Safety Expectations

The *Online Safety Act 2021* also provides eSafety with powers to require online service providers to report on the reasonable steps they are taking to comply with any of the Basic Online Safety Expectations. The Expectations include a range of steps that providers are expected to take to ensure safety for their users and to protect Australian users from harm.

The Expectations are intended to increase transparency and accountability of online service providers and ensure users can use a service in a safe manner. Although the Expectations are not enforceable, the obligation for platforms to respond to a reporting notice is enforceable and backed by civil penalties and other enforcement mechanisms.

Industry codes

Additionally, the *Online Safety Act 2021* provides for the development of industry codes by sections of the online industry to deal with illegal and restricted content across the digital ecosystem. This includes providers of social media, messaging, search engine and app distribution services, as well as internet and hosting service providers, manufacturers and suppliers of equipment used to access online services and those that install and maintain the equipment.

The first phase of industry codes, which will address class 1 content (including child sexual abuse material and pro-terror material) is well underway. After consulting publicly and with industry, the industry groups tasked with developing the industry codes submitted eight draft codes to the eSafety Commissioner in November 2022.

In February 2023, eSafety identified concerns with industry's draft codes and revised versions of the draft codes were provided to eSafety on 31 March 2023. eSafety is currently considering whether the draft industry codes meet the statutory requirement for registration, including providing adequate community safeguards.

If registered, compliance with these industry codes will be mandatory and enforceable, and eSafety will have the power to investigate potential breaches and direct platforms to comply. The eSafety Commissioner has the power to determine industry standards if industry codes are

not registered and it is considered necessary or convenient to do so to provide appropriate community safeguards.

The second phase of industry codes will address children and young people's access to restricted content, such as online pornography. The development of these codes will follow the registration of Phase 1 industry codes or the determination of industry standards.

Safety by Design

In addition to our legislative functions, we also guide and support industry to enhance online safety measures through our Safety by Design initiative.

Safety by Design focusses on the ways online services can minimise harms by anticipating, detecting and eliminating threats before they occur. It includes a range of guidance, risk-mitigation tools and transparency measures for online services to use throughout the design, development and deployment of a product or service.

The initiative promotes online safety through 3 guiding principles:

1. *Service provider responsibility* – that online services are responsible for the safety of users.
2. *User empowerment and autonomy* – that users should be empowered with safety tools and provided with autonomy.
3. *Transparency and accountability* – that online services should be transparent and held accountable for their actions and to the community.

Safety by Design and a 'privacy by design' framework share a common goal of creating products and services that are safe, secure, user-friendly, while also considering the potential risks and challenges that may arise.

eSafety also conducts educational and community awareness programs, including promoting good privacy practices for children, young people, classrooms, and those experiencing domestic and family violence.

Further detail of eSafety's operations and areas of focus can be found in our Regulatory Posture and Regulatory Priorities 2021-22, our inaugural corporate plan 2022-23, as well as our four-year strategy for 2022-25.

Online safety and privacy

Online safety and privacy are two related but distinct concepts that intersect in several ways.

Online safety relates to the broad protection of individuals, groups and communities from online harms and threats, such as exposure to illegal and harmful content and engagement with bad actors who are looking to threaten or harass individuals. It involves online services and governments taking measures to ensure that an individual's online activity does not put them at risk and that they are able to navigate online spaces safely.

Privacy, on the other hand, broadly relates to how an individual's personal information – including sensitive information- is collected, used and disclosed, protected and destroyed by

entities such as organisations and government agencies. Robust and enforceable privacy protections are crucial to protect individuals from online harms such as data breaches, identity theft, grooming for sexual exploitation, and inappropriate targeted advertising or recommended content.

There are a number of instances where these two areas may overlap. For example, safety risks can arise when personal information about an individual is collected, used and disclosed for improper, unlawful or harmful purposes, or where personal information is not properly protected or destroyed, such as when a service's default setting enables geolocation tracking of an individual users. This can result in significant safety risks – such as inappropriate surveillance by others and physical risks of information is compromised in a data breach. These risks are often heightened in relation to children and young people. Additionally, where excessive and sensitive information is collected about an individual, including by inferring insights about that individual, this can lead to risks of that information being misused in ways that are harmful – such as the recommendation or promotion of harmful content, discrimination and manipulation.

Likewise, an individual's right to privacy may be compromised if an online service does not embed adequate safety protections within their products and services, such as detecting bots and trolls who are scamming vulnerable users for their personal information.

Given the close intersection of online safety and privacy, eSafety encourages a holistic and coordinated approach to address related issues. We support increased transparency and accountability from online services of how they handle personal information as well as support for greater empowerment for individuals to exercise choice and control over their data. These approaches are strongly aligned to our Safety by Design initiative and the objectives of the *Online Safety Act 2021*.

Some of the Review's proposals may also support an organisation's compliance with online safety obligations. For example, the Basic Online Safety Expectations set out the Government's expectations that services are already taking reasonable steps to ensure users can use a service in a safe manner, such as making sure the default privacy and safety settings of services targeted at, or used by children, are robust and set to the most restrictive level.

It is also worth noting that the draft industry codes under the *Online Safety Act 2021*, while primarily focused on regulating the accessibility, distribution and storage of illegal and restricted content, include provisions that are directly relevant to the privacy of users. For example, Minimum Compliance Measure (MCM) 7 of the draft social media service code provides that Tier 1 social media service providers "must at a minimum have default settings that are designed to prevent a young Australian child from unwanted from unknown end-users, including settings which prevent the location of the child being shared with other accounts by default". A young Australian child is defined in the draft code as an Australian end-user under the age of 16 years. Similar provisions are proposed under MCM 6 iii) of the draft code for relevant electronic services.

Additionally, fair and reasonable collection of personal information by online services, such as the age of a user may support positive privacy and safety outcomes – such as ensuring that children's best interests are considered and their online experience is positive and age appropriate. By identifying users who are children and young adults through supplied age data,

online services can take steps to protect those users online, such as by blocking any incoming messaging from unknown adults who may be looking to engaged in harmful or illegal activity, such as grooming.

There are also emerging risks to Australians' online safety and privacy with the increasing use of new technologies such as artificial intelligence and the metaverse. As these technologies continue to evolve, it will be important to ensure that they are designed and developed in a way that prioritises both user safety and privacy, and that Australia's national regulatory frameworks contain robust and adaptable standards.

We would encourage the Review to form part of a broader response by the Australian Government to support and educate individuals to know how to exercise their rights online, what risks are involved with their online participation, and how they can navigate their way online when seeking help.

eSafety's comments on report proposals

While the overlap of online safety and privacy is extensive, this submission will provide eSafety's comments on certain proposals that could have a prominent impact on our work program.

We would welcome further discussions with the Attorney-General or Government on matters raised in this submission.

Child-appropriate practices

eSafety supports **Proposal 16.3** which would require entities to ensure their privacy information, including data collection notices and privacy policies, that are addressed to a child be child appropriate.

We would welcome being consulted during the implementation of this proposal. eSafety has extensive experience in providing educational programs and resources on online safety issues that are specifically tailored for children and young people.

This proposal would also align with Section 17 of the Basic Online Safety Expectations Determination 2022, which includes an expectation that online services' terms of use, policies and complaints are written in plain language and readily accessible.

Children's Online Privacy Code

We note that **Proposal 16.5** provides for the introduction of a Children's Online Privacy Code (COPC) that would apply to online services that are 'likely to be accessed by children', and that eSafety is consulted during the development of the code.

eSafety is well-placed to provide its expertise for this process. As part of our age verification roadmap project, eSafety has already been closely monitoring the design and operation of the UK Age Appropriate Design Code and considering how it could apply in an Australian context.

We consider the COPC and the UK Age Appropriate Design Code could share a number of common standards and principles, including:

- Best interests of the child: The best interests of the child should be a primary consideration when designing online services that are likely to be accessed by children.

- Age-appropriate application: The content, design, and settings of online services should be appropriate to the age of the child.
- Transparency: Children should be given clear information about how their personal data will be used, and any privacy settings should be easy for them to understand and use.
- Detrimental use: Online services should not be allowed to use children's personal data in ways that could be detrimental to their wellbeing.
- Policies and community standards: Online services should have policies and community standards that are designed to protect children from harm.
- Default settings: Privacy settings should be set to "high" by default.
- Data minimisation: Online services should collect and retain only the minimum amount of personal data necessary to provide their services.
- Parental controls: Online services should provide parental controls that are appropriate to the age of the child.
- Online tools: Online services should provide tools to help children protect their privacy, and to help them understand the risks and benefits of online activity.
- Harmful content: Online services should take steps to ensure that children are not exposed to harmful content, and should have systems in place to enable users to report and flag inappropriate content.

eSafety could also provide the COPC developer with relevant insights from its age verification roadmap consultations with industry and other key stakeholders.

The proposed COPC would also be developed against the backdrop of industry codes or industry standards regulating harmful online content, expected to be in place in 2023. eSafety considers it important that there is regulatory coherence in relation to these codes given the intersecting issues and their application in many cases to the same group of stakeholders.

Fair and reasonable test

eSafety supports the introduction of a 'fair and reasonable' test for the collection, use and disclosure of personal information (**Proposal 12.1** and **12.2**).

This test would ensure that handling of personal information is subject to consideration upfront on important matters, including the kind, sensitivity and amount of personal information being collected and handled, any risk of unjustified adverse impact or harm and, if the personal information relates to a child, whether it is in the best interests of the child.

This would encourage and enforce a Safety by Design approach, as well as a privacy by design approach, as organisations will need to consider these matters and either adjust their practices accordingly to ensure their actions are fair and reasonable.

It would also ensure that organisations and agencies cannot rely on consent as a basis for engaging in a data handling practice that is unfair and unreasonable.

eSafety has expertise in applying the best interests of the child in a practical sense, such as through our Safety by Design initiative, and would be keen to share this expertise with the Attorney-General's Department, Office of the Australian Information Commissioner (OAIC), and other relevant Australian Government organisations.

Privacy impact assessment

Proposal 13.1 would require all regulated entities to undertake a privacy impact assessment for high-risk activities.

Many of the high-risk activities outlined in the Review can also pose a substantial threat to a user's online safety. This includes collection, use or disclosure of sensitive information or children's personal information on a large scale, real-time tracking of an individual's geolocation, and the profiling and delivery of personalised content and advertising.

As a practical example, a dating app may need to undertake a privacy impact assessment on how it is handling sensitive information of its users and what is being shared with third-party advertisers. This assessment could help identify gaps in privacy safeguards that could be exploited by bad actors wishing to engage in stalking or harassing, both online and offline.

The privacy impact assessment would also align to our Safety by Design initiative which similarly provides a risk assessment of safeguards that are intended to be utilised by organisations before their products and services are used by individuals.

Additionally, this proposal aligns with Section 6 of the Basic Online Safety Expectations Determination 2022, which states that providers are expected to take reasonable steps to ensure safe use of their services and to take reasonable steps to proactively minimise the extent to which material or activity on the service is unlawful or harmful. Section 6(3) provides a list of examples of reasonable steps that may be taken to comply with this Expectation, including ensuring assessments of safety risks and impacts are undertaken, and safety review processes are implemented throughout the design, development, deployment and post-deployment stages for the service.

eSafety therefore supports this proposal as it would ensure that organisations consider privacy risks up front before undertaking certain data-handling activities, thereby mitigating potential safety risks.

Facial recognition technology

eSafety also supports further considerations on how an enhanced risk assessment requirement for facial recognition technology and other uses of biometric information may be adopted as part of the proposal to require privacy impact assessments for high privacy risks activities (**Proposal 13.2**).

eSafety has recently been monitoring the use of age verification and age assurance technologies, including facial recognition technologies, as part of its age verification roadmap project. Given our engagement in this area, we would be interested in contributing to further discussions on this proposal.

Proposed rights of the individual

Chapter 18 of the Review puts forward a series of proposals for individuals to have new rights in relation to their personal information that are aimed at providing them with greater transparency and control.

- Right to access and explanation (**Proposal 18.1**): This proposal would likely allow individuals to request organisations to explain how their personal and sensitive information and data is being used to recommend content to them, or otherwise shape their online experience. eSafety supports this proposal given its intent to increase transparency and accountability.
- Right to objection (**Proposal 18.2**): This proposal would enable individuals to object to the collection, use or disclosure of personal information, with an entity required to provide a written response to an objection. eSafety supports this proposal as it allows individuals to exercise increased control over how their information is used and control of their online experience.
- Right to erasure (**Proposal 18.3**): eSafety acknowledges the concerns raised in the report around the potential for offenders to utilise this right to erase any trail of their activity or presence on a platform.

  However, we consider it important that organisations preserve information about their users in circumstances where a user is posing or creating a safety risk, such as sharing or storing illegal or harmful material. This information can be incredibly valuable when reporting issues to law enforcement or other relevant bodies, as well as responding to any reports or complaints about the user.

  We also note that some organisations have responsibilities under the Basic Online Safety Expectations that may require certain information to be quarantined or preserved in order to ensure safe user of their online services.[1]

  eSafety would welcome to engage further on this issue.

[1] Section 19 of the Basic Online Safety Expectations Determination 2022 states that providers will 'keep records of reports and complaints about the material mentioned in Section 13 provided on the service for 5 years after the making of the report or complaint to which the record relates'. Section 13 sets out Expectations in relation to reports and complaints about certain material including cyber-bullying material targeted at an Australian child, cyber-abuse material directed at an Australian adult, a non-consensual intimate image of a person, class 1 and class 2 material, and material that promotes, incites, instructs or depicts abhorrent violent conduct.

Automated decision making

eSafety supports **Proposal 19.1** and **19.2** that privacy policies should set out the type of personal information that will be used in substantially automated decisions, which have legal or similarly significant effect on an individual's rights.

eSafety would welcome the opportunity to provide additional input on how online harms may constitute a 'similarly significant effect' on an individual's rights.

Direct marketing, targeting and trading proposals

eSafety supports the proposals to provide individuals with rights to opt-out of receiving direct marketing and targeted advertising (**Proposals 20.1 – 20.9**).These proposals will allow individuals to exercise greater choice and control over harmful or unwanted material being recommended or promoted to them and thereby offering individuals a more positive online experience.

We also support the proposal that targeting should be fair and reasonable, and that targeting based on sensitive information should be prohibited except for socially beneficial content (**Proposal 20.8**). This would likely reduce instances of individuals being targeted with material that is harmful to them, such as targeted based on knowledge of a health issue or vulnerability.

Additionally, eSafety supports **Proposal 20.9** to require entities to provide information about targeting, including clear information on the use of algorithms and profiling to recommend content to individuals. This would benefit individuals if choices were provided at sign up, and through in service prompts, nudges or warnings. Such interventions should always provide users with opportunities to clearly and simply report content, as well as links to manage settings.

Individuals exercising their privacy rights

eSafety welcomes proposals for increased options for individuals to exercise their privacy rights, such as through a direct right of action or statutory tort for invasion of privacy (**Proposal 26.1 – 27.1**).

We would encourage coordination and communication to individuals to explain what these rights are and how they can be exercised. This could include, for example, clarity on when an individual should use eSafety's complaints scheme or should seek relief from an online harm through the privacy framework. Further consultation and coordination with eSafety may be needed.

Increased enforcement powers

Finally, eSafety support the proposals for the OAIC to be provided with greater enforcement powers and more options to deal with situations where people's privacy has been impacted **Proposal 25.3 – 25.4**).

With eSafety recently being provided with a suite of new powers under the *Online Safety Act 2021*, these proposed powers would align the OAIC and eSafety to better coordinate their approaches to online safety and privacy issues.

We would also support a balance of available penalties and enforcement responses between the *Online Safety Act* and the *Privacy Act* to ensure that safety or privacy are equally prioritised by industry.