



Meeting brief

File ref	D2023/018923
Subject	Monthly Meeting OAIC and eSafety

Meeting details

Day and Date	Monday, 14 August 2023
Time	2:30pm – 3:00pm
Location	Teams
Contact person	Isla Gibson
Contact number	02 9942 4233

Attendees

Name	Position
Julie Inman Grant	eSafety Commissioner

OAIC

Name	Position
Angelene Falk	Australian Information Commissioner and Australian Privacy Commissioner

Table of Contents

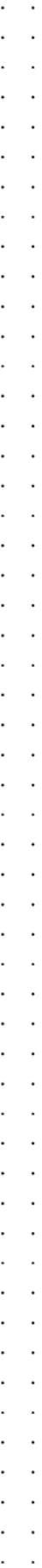


Key messages/points from DR

Key messages/points from R&S

s 22

s 22



S 22

ii) Online Safety Codes

On **30 May 2023**, the Law Reform & Digital Platforms team was briefed by eSafety ([D2023/015709](#)) in relation to the eSafety Commissioner's decision on industry's second attempt to develop Online Safety Codes. The eSafety Commissioner's decision was formally [announced](#) on 1 June 2023.

The eSafety Commissioner decided to **register five of the eight** industry codes:

- Internet Carriage Services (i.e. ISPs)
- Hosting Services (e.g. Amazon Web Services, Azure)
- Equipment Services (e.g. manufacturers of devices, operating systems)
- App Distribution Services (i.e. App stores)
- Social Media Services.

Two of the industry codes were rejected on the basis that they failed to provide appropriate community safeguards to deal with illegal and harmful content online. eSafety will now move to develop mandatory and enforceable industry standards for these two industry sectors:

- Relevant Electronic Services (i.e. messaging services, SMS, email, online gaming)
- Designated Internet Services (a miscellaneous category which includes websites, apps, and user hosting services such as iCloud and Dropbox)

When briefing the Law Reform & Digital Platforms team, eSafety noted that the decision to reject the Relevant Electronic Services and Designated Internet Services codes was largely based on the lack of commitments by certain services to deploy systems, processes or technologies to proactively detect known CSAM (i.e. material that has already been vetted as CSAM) and pro-terror content. In particular, the Relevant Electronic Services code did **not make a commitment in relation to email or encrypted messages**.

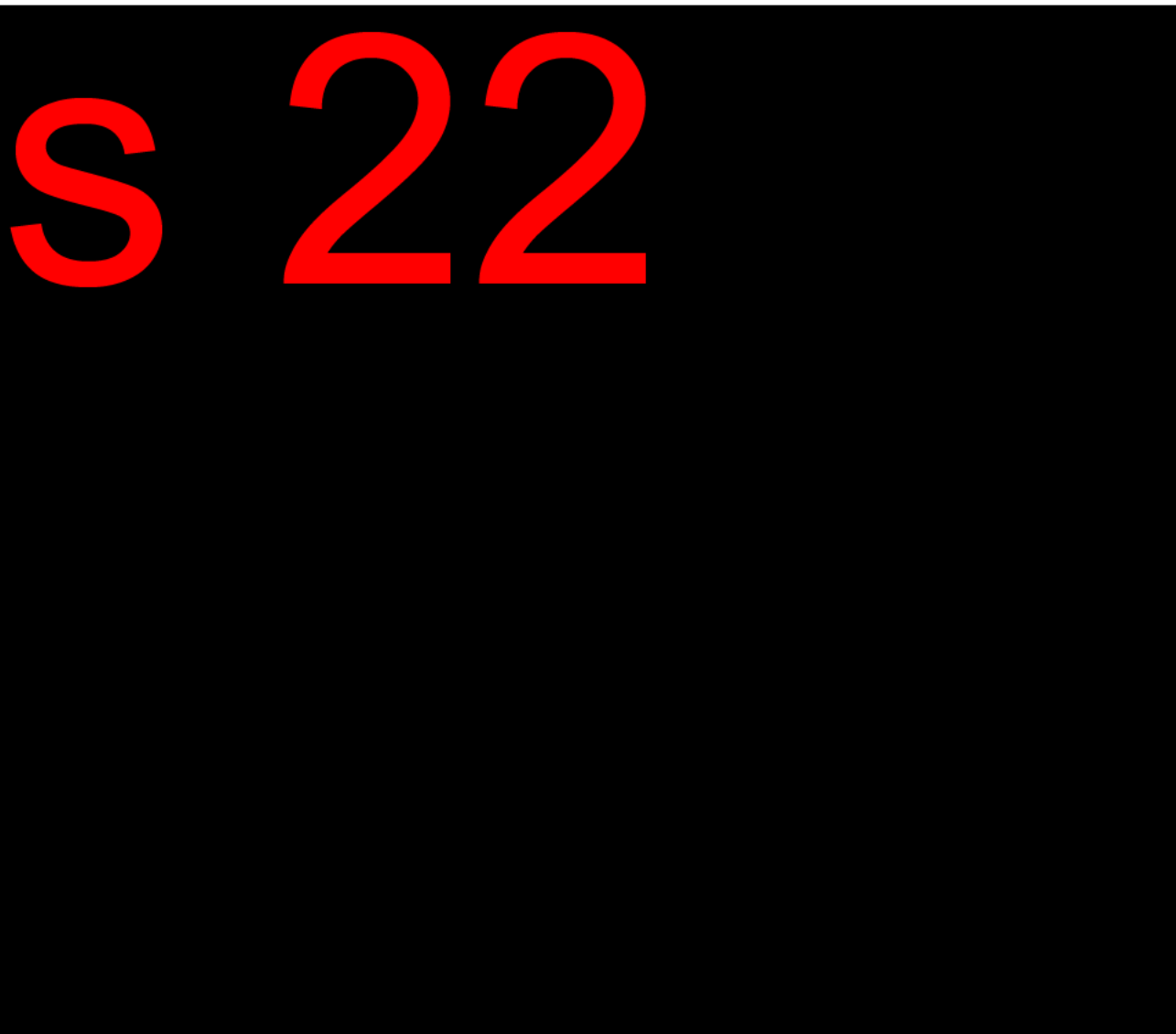
eSafety noted that industry was concerned about privacy in relation to consumer facing content hosting services and technical limitations when it comes to encrypted messages. It

plays into the larger debate seen overseas (e.g. UK Online Safety Bill) in relation to end to end encryption.

In the briefing, eSafety stressed that they are not suggesting that encryption be 'broken'. They noted that, for example, WhatsApp is already scanning non-encrypted materials, including the names of group messages and profile pictures to detect whether CSAM is likely being shared in that message thread. Proportionate measures can be taken to proactively detect CSAM. In contrast to the rejected codes, the Social Media Services code clearly made this commitment.

The eSafety Commissioner requested that the **final industry code (search engine services) be further updated** to reflect the integration of generative AI into certain search services (e.g. Google and Bing). When briefing the OAIC, eSafety noted that they are particularly concerned about the use of generative AI for deep fake image generation (e.g. generation of CSAM or pro-terror content).

In terms of **next steps**, the registered industry codes will commence in **December 2023**. eSafety hopes to develop the mandatory standards for Relevant Electronic Services and Designated Internet Services within 4 months, but this may be an optimistic timeframe given that they will have to draft them and consult.



s 22

iv) eSafety Submission to Privacy Act Review Final Report

In **March 2023**, the Office of the eSafety Commissioner made a submission in response to the Privacy Act Review Final Report which is available [here](#). eSafety's submission notes the intersection between safety and privacy (which it defines as informational privacy) and highlighted the following:

- s22 [redacted]
- There are some synergies with protections under eSafety legislation such as the BOSE (expectation of reasonable steps for privacy defaults in services targeted at children) and industry codes (default settings to prevent unwanted contact including settings which prevent location of the child being shared by default)
- s22 [redacted]

s 22

s 22

s 22



s 22



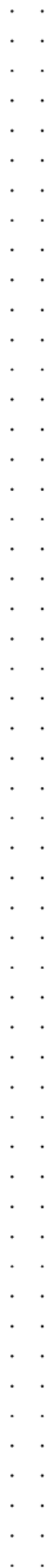
s 22



s 22



s 22



s 22



s 22



s 22





Meeting brief

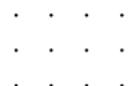
File ref	D2023/009514
Subject	Monthly Meeting – OAIC and eSafety

Meeting details

Day and Date	Tuesday, 9 May 2023
Time	3:00pm – 3:30pm
Location	Teams
Contact person	Samantha Lidbetter
Contact number	02 9942 4238

Attendees

Name	Position
Julie Inman Grant	eSafety Commissioner
Angelene Falk	Australian Information Commissioner and Australian Privacy Commissioner



Recent work of eSafety and key online safety initiatives

A large, stylized graphic consisting of a red letter 'S' followed by the number '22', all set against a solid black background.

ii) Online Safety Codes

In **February 2023**, the eSafety Commissioner rejected proposed industry-developed [Online Safety Codes](#) that had been put forward by several industry associations, including DIGI, the Communications Alliance and the Interactive Games and Entertainment Association.

The Commissioner determined that the codes were unlikely to provide the appropriate level of community safeguards that was required for them to be registered. eSafety's concerns included inadequate reporting timeframes and insufficient measures to detect and remove class 1A material (including CSAM, pro-terror content and content that depicts extreme crime or violence).

Revised versions of the industry Online Safety Codes were due to be re-submitted to the eSafety Commissioner by **31 March 2023**. As at 4 May, we are not aware as to whether a decision has been reached on the final draft codes.

A large, stylized graphic consisting of a red letter 'S' followed by the number '22', all set against a solid black background.

S 22

S 22

S 22

S 22

Attachment B – eSafety Senate Estimates Appearance (February 2023)

Date: Tuesday 14 February 2023

Committee: Environment and Communications Legislation Committee

Appearing: Ms Julie Inman Grant, Mr Toby Dagg, Ms Morag Bond

Senators: Senator Sarah Henderson (LNP), Senator David Shoebridge (Greens)

A large, bold, red graphic consisting of the letter 'S' followed by the number '22', set against a solid black rectangular background.

Industry Codes and Online Safety Act:

- Senator Henderson noted the recent murder of two police officers in Queensland and the online video posted by the offenders, and sought eSafety’s views on the responsibility of tech platforms to ensure that these videos do not make it online.
- Ms Inman Grant noted that the industry codes seek to address this, and the first tranche of codes examine the proactive detection of CSAM and terrorist and violent extremist content (TVEC). She acknowledged it can be challenging but that the major companies have access to technology such as AI and image clustering, and should be investing more into these technologies.
- Mr Dagg noted that Google publishes transparency stats on proactive detection of TVEC on Youtube. The eSafety Commissioner has expressed a strong expectation that industry commit to, through the codes, a strong stance in relation to detection of that kind of material proactively.
- Ms Inman Grant noted that transparency powers help eSafety to understand the scale and scope of the problem - it was only through legally enforceable notices that they got

the information they needed. Government has been supportive and powers in Online Safety Act help the commissioner to hold the companies to account.

- Mr Dagg noted that there will be a three-year statutory review of the Online Safety Act and that eSafety is reaching findings in the course of applying their powers which will inform recommendations to Government.

S 22

Industry Codes:

- Senator Shoebridge asked questions about the status of the industry codes, and why eSafety's preliminary view is that the draft codes do not provide appropriate community safeguards.
- Ms Inman Grant noted that the industry associations did not make their final draft codes public. Specific feedback has been provided by eSafety in relation to each of the industry codes. The first tranche of codes specifically deal with CSAM and TVEC content – companies should be doing more to use technologies such as PhotoDNA to proactively detect 'known'/triple vetted CSAM material.
- Ms Bond stated that it would be inappropriate for eSafety to go into detail about their concerns as industry never published the final draft codes as at November 2022 (industry only published an earlier draft from September 2022). eSafety made it clear to industry that they wished to see a broader commitment to deploy technology to detect known CSAM, not just in relation to certain businesses/online services.
- Senator Shoebridge asked whether it would be appropriate for the final draft codes (as at November 2022) be made public.
- Ms Inman Grant noted that eSafety is following the letter of the law which states that they are industry's codes and it's ultimately their determination. If and when eSafety makes a final determination, it will be appropriate to release the codes in their entirety.
- Senator Shoebridge asked whether the draft November 2022 code can be provided to the Committee.
- Ms Inman Grant took this on notice and indicated she would discuss with the department.
- Senator Henderson asked whether all correspondence between industry and eSafety could be tabled.
- Ms Bond and Inman Grant noted this would be a lot of correspondence, but would take it on notice.



Meeting brief

File ref	File ref
Subject	Monthly Meeting OAIC and eSafety

Meeting details

Day and Date	Tuesday, 1 November 2022
Time	9.30am-10.00am
Location	Teams
Contact person	Samantha Lidbetter
Contact number	02 9942 4238

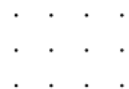
Attendees

Name	Position
Julie Inman Grant	eSafety Commissioner

OAIC

Name	Position
Angelene Falk	Australian Information Commissioner and Australian Privacy Commissioner

Key messages/points



S 22

S 22

S 22

eSafety Online Safety codes

- No update from last meeting. The following is included for background information.
- Eight industry codes were released for public consultation on **1 September 2022**, and the consultation is closed on **2 October 2022**.
- The consultation is the responsibility of the six industry associations that formed a steering group to oversee the development of the codes for the 8 industry sections outlined under the Online Safety Act (OSA).
- These industry associations are: the Australian Mobile Telecommunications Association, BSA – The Software Alliance, Communications Alliance, Consumer Electronics Suppliers' Association, Digital Industry Group Inc, Interactive Games and Entertainment Association.
- eSafety has not endorsed the draft codes at this stage and will undertake an assessment of whether they meet the statutory requirements when industry submits them for registration in late 2022.
- We are still considering the codes but do not intend to make a formal submission at this stage. We will look to engage with eSafety at the officer-level.

Background on eSafety codes

- The OSA provides for industry bodies or associations to develop, and eSafety to register, new industry codes to regulate harmful online content.
- This material, referred to as 'class 1' and 'class 2' material, ranges from material of the highest and most serious harm, such as videos of the sexual abuse of children or terrorism, through to material which is inappropriate for children, such as online pornography.
- eSafety's [position paper](#) for the development of the codes encouraged:
 - industry associations to adopt an outcomes and risk-based approach when developing the codes.
 - industry to adopt a two-phased approach to industry codes, where separate codes are developed for:

- high end class 1 material (1A and 1B), including CSEM and pro-terror content (first phase – the current draft codes out for consultation address this material)
 - online pornography and class 2 material (second phase – will take place after the first phase is completed).
- The draft [Codes](#) (phase 1) outline steps that online industry participants must take to enhance online protections by reducing access and exposure to Class 1A and Class 1B material.
 - The draft codes have been developed that will apply to the following sections of the online industry as set out in the OSA:
 1. **social media services** (e.g. Facebook, Instagram, TikTok);
 2. **relevant electronic services** used for messaging (including SMS and MMS) services, **email, and online gaming services** (e.g. Gmail, WhatsApp, services);
 3. **designated internet services** that include websites and end-user online storage and sharing services (e.g. Dropbox, Google Drive);
 4. **internet search engine services** (e.g. Google Search);
 5. **app distribution services** used to download apps (e.g. Apple IOS and Google Play stores);
 6. **hosting services** (e.g. Amazon Web Services, NetDC).
 7. **internet carriage services** (e.g. Telstra, iiNet, Optus, TPG Telecom); and
 8. **manufacturers and suppliers of any equipment that connects to the internet, and those who maintain and install it** (e.g. of modems, televisions, phones, tablets, smart home devices, e-readers etc).
 - the Codes have adopted a risk and outcomes based approach and are not proscriptive in how industry achieves those outcomes.
 - **Areas of intersection – age assurance:**
 - The Codes state that age assurance measures may be part of reasonable steps that organisations can take to limit children from accessing content.
 - The [Social Media Services Online Safety Code provides](#) that a social media provider must take reasonable steps to prevent an Australian child that is known to be under the minimum age permitted on the service from holding an account on the service (see 6(6)). The guidance provides that reasonable steps could include age estimation tools or AI tools that help understand a person’s real age.
 - The [Internet Search Engine Services Code](#) provides that an internet search engine service should provide “age appropriate safety settings” (see 7(10)).
 - The OAIC have previously recommended to eSafety that such age estimation tools should be privacy-preserving (see for example our comments on the Restricted Access System: [D2022/017937](#)). Age estimation tools should limit the scope of information

collected by the system to ensure the only attribute being tested is the age of the applicant.

- Given the Codes are not proscriptive in terms of the types of age estimation tools that could be used, the Codes would not prevent the OAIC from issuing further guidance on the privacy considerations of age estimation technologies.

A large, bold, red serif font displays the text "S 22" against a solid black rectangular background. The "S" is on the left, and the "22" is to its right, with a small gap between them. The text is positioned in the upper left quadrant of the page.

S 22

s 22

s 22

s 22

s 22

S 22

S 22

s 22

S 22

s 22

S 22

S 22

S 22

S 22

s 22

S 22

S 22

Office of the eSafety Commissioner ([transcript](#))

Committee: Environment and Communications Legislation Committee

Appearing: Ms Julie Inman Grant, Mr Toby Dagg, Ms Morag Bond

Senators asking about the issue: Senator Sarah Henderson (Greens)

S 22

Industry Codes and Online Safety Act:

- Senator Henderson noted the recent murder of two police officers in Queensland and the online video posted by the offenders, and sought eSafety's views on the responsibility of tech platforms to ensure that these videos do not make it online.
- Ms Inman Grant noted that the industry codes seek to address this, and the first tranche of codes examine the proactive detection of CSAM and terrorist and violent extremist content (TVEC). She acknowledged it can be challenging but that the major companies have access to technology such as AI and image clustering, and should be investing more into these technologies.
- Mr Dagg noted that Google publishes transparency stats on proactive detection of TVEC on Youtube. The eSafety Commissioner has expressed a strong expectation that industry commit to, through the codes, a strong stance in relation to detection of that kind of material proactively.
- Ms Inman Grant noted that transparency powers help eSafety to understand the scale and scope of the problem - it was only through legally enforceable notices that they got the information they needed. Government has been supportive and powers in Online Safety Act help the commissioner to hold the companies to account.
- Mr Dagg noted that there will be a three-year statutory review of the Online Safety Act and that eSafety is reaching findings in the course of applying their powers which will inform recommendations to Government.

A large, stylized red logo consisting of the letter 'S' followed by the number '22', set against a solid black rectangular background.

Senator asking about the issue: Senator David Shoebridge (Greens)

Issues:

- **Industry Codes:**

- Senator Shoebridge asked questions about the status of the industry codes, and why eSafety's preliminary view is that the draft codes do not provide appropriate community safeguards.
- Ms Inman Grant noted that the industry associations did not make their final draft codes public. Specific feedback has been provided by eSafety in relation to each of the industry codes. The first tranche of codes specifically deal with CSAM and TVEC content – companies should be doing more to use technologies such as PhotoDNA to proactively detect 'known'/triple vetted CSAM material.
- Ms Bond stated that it would be inappropriate for eSafety to go into detail about their concerns as industry never published the final draft codes as at November 2022 (industry only published an earlier draft from September 2022). eSafety made it clear to industry that they wished to see a broader commitment to deploy technology to detect known CSAM, not just in relation to certain businesses/online services.
- Senator Shoebridge asked whether it would be appropriate for the final draft codes (as at November 2022) be made public.
- Ms Inman Grant noted that eSafety is following the letter of the law which states that they

are industry's codes and it's ultimately their determination. If and when eSafety makes a final determination, it will be appropriate to release the codes in their entirety.

- Senator Shoebridge asked whether the draft November 2022 code can be provided to the Committee.
- Ms Inman Grant took this on notice and indicated she would discuss with the department.
- Senator Henderson asked whether all correspondence between industry and eSafety could be tabled.
- Ms Bond and Inman Grant noted this would be a lot of correspondence, but would take it on notice.

Next steps: For noting only.

A large, bold, red graphic consisting of the letter 'S' followed by the number '22', set against a solid black rectangular background. The text is positioned in the upper left quadrant of the page.

s 22

From: [MACKIE, Tom](#)
To: [LAMPE, Naomi](#); [CORBETT, Jason](#)
Cc: [BROWN, Rebecca](#)
Subject: eSafety Industry Codes Briefing
Date: Tuesday, 30 May 2023 12:42:00 PM
Attachments: [image001.jpg](#)

Hi Naomi and Jason,

For your visibility, below are my notes from the briefing we received from eSafety about their upcoming decision on the online safety codes.

eSafety Industry Codes Briefing (30 May 2023)

- The decision will be announced this week or next Monday at the latest.
- Industry have made significant improvements to many of the codes since February.
- The Commissioner will **register five of the eight** industry codes:
 - Internet carriage services (i.e. ISPs)
 - Hosting services (e.g. Amazon Web Services, Azure)
 - Equipment services (e.g. manufacturers of devices, operating systems)
 - App distribution services (i.e. App stores)
 - Social media services.
- The Commissioner will **reject two** of the industry codes and will move to develop mandatory standards:
 - Relevant electronic services (i.e. messaging services, SMS, email, online gaming)
 - Designated internet services (a bit of a miscellaneous category which includes websites, apps, and user hosting services such as iCloud and Dropbox)
- The Commissioner will request that the **final industry code (search engine services) be further updated** to reflect the integration of generative AI into certain search services (e.g. Google and Bing).
 - eSafety is particularly concerned about the use of generative AI for deep fake image generation (e.g. generation of CSAM or pro-terror content).
- The decision to reject the 'relevant electronic services' and 'designated internet services' codes was largely based on the lack of commitments by certain services to deploy systems, processes or technologies to proactively detect known CSAM (i.e. material that has already been vetted as CSAM) and pro-terror content.
 - For example, the relevant electronic services code did not make that commitment in relation to email or encrypted messages.
 - Industry is concerned about privacy in relation to consumer facing content hosting services and technical limitations when it comes to encrypted messages. It plays into the larger debate seen overseas (e.g. UK Online Safety Bill) in relation to encrypted messages.
 - To be clear, eSafety is not suggesting that encryption be 'broken'. For example, WhatsApp is already scanning non-encrypted materials, including the names of group messages, profile pictures, to detect whether CSAM is likely being shared. There are other measures that can be taken. By contrast to the rejected codes, the draft social media services code clearly made the commitment.
- eSafety does expect some pushback from certain industry bodies once the decisions are released.
- The social media services code will require privacy settings to be implemented for child users by default, with an emphasis on ensuring that children do not receive unwanted contact from other users, and preventing their location from being shared with other users by default.

- The code defines a 'young Australian' as under 16 years of age. Child rights orgs expressed concerns. eSafety accepted rather than pushing for 18 years, not a red line issue in light of other issues. eSafety notes that in accepting this, they do not think it would prevent a future children's online privacy code from being developed and setting a higher age limit of 18 years of age.
- The registered industry codes will commence within 6 months.
- eSafety hopes to develop the mandatory standards within 4 months, but this may be an optimistic timeframe given that they will have to draft them and consult.

Best,



Tom Mackie | Assistant Director, Law Reform and Digital Platforms
Regulation and Strategy Branch
Office of the Australian Information Commissioner
GPO Box 5228 Sydney NSW 2001 | [oaic.gov.au](https://www.oaic.gov.au)
+61 02 9942 4258 | tom.mackie@oaic.gov.au

From: [GHALI,Sarah](#)
To: s 47E(d); s 47E(d)
Cc: s 47E(d); [HAMPTON,Elizabeth](#); [BROWN,Rebecca](#); [MACKIE,Tom](#)
Subject: RE: Briefing note - online safety industry codes decision [SEC=OFFICIAL]
Date: Friday, 2 June 2023 3:50:00 PM
Attachments: [image009.jpg](#)
[image010.jpg](#)
[image012.png](#)
[image013.png](#)
[image014.png](#)
[image015.png](#)
[image016.png](#)
[image017.png](#)
[image018.png](#)
[image019.jpg](#)
[image001.jpg](#)

Hi s 47E(d) and s 47E(d)

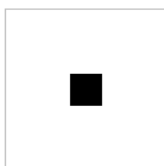
Thank you again for the briefing on Tuesday and for sharing those materials with us.

We don't have concerns with the messaging around consultation with the OAIC on the relevant standards. We appreciate the opportunity to provide input on the standards at the appropriate time.

Please feel free to reach out to Beck or myself directly if we can be of assistance as this process progresses, or in relation to any other privacy-related matters.

Thanks

Sarah



Sarah Ghali

Assistant Commissioner

Regulation and Strategy

Office of the Australian Information Commissioner

P +61 2 9942 4208 M s 47E(d) E sarah.ghali@oaic.gov.au

Please note I work part time and I am not available on Wednesday

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: s 47E(d)
Sent: Wednesday, May 31, 2023 12:26 PM
To: s 47E(d); [HAMPTON,Elizabeth](#)
<Elizabeth.Hampton@oaic.gov.au>; [GHALI,Sarah](#) <Sarah.Ghali@oaic.gov.au>; [BROWN,Rebecca](#)
<Rebecca.Brown@oaic.gov.au>; [MACKIE,Tom](#) <Tom.Mackie@oaic.gov.au>
Cc: s 47E(d)
Subject: RE: Briefing note - online safety industry codes decision [SEC=OFFICIAL]

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

Thanks ,




I will just add that we have indicated that we will consult with the OAIC in relation to the development of industry standards for the Designated Internet Services and Relevant Electronic Services sections of the online industry.

Apologies for not mentioning this to you yesterday.

Please let me know if you have any concerns with this.

Kind regards



From:  **Sent:** Wednesday, 31 May 2023 12:22 PM
To: HAMPTON,Elizabeth <Elizabeth.Hampton@oaic.gov.au>; GHALI,Sarah <Sarah.Ghali@oaic.gov.au>; Rebecca.Brown@oaic.gov.au; MACKIE, Tom <Tom.Mackie@oaic.gov.au>
Cc:  
Subject: Briefing note - online safety industry codes decision [SEC=OFFICIAL]

OFFICIAL


Dear Libby, Sarah, Bec and Tom,

Thank you very much for your time yesterday.


Please see attached for the promised briefing – we have also added our key media messages as promised.

All the best,



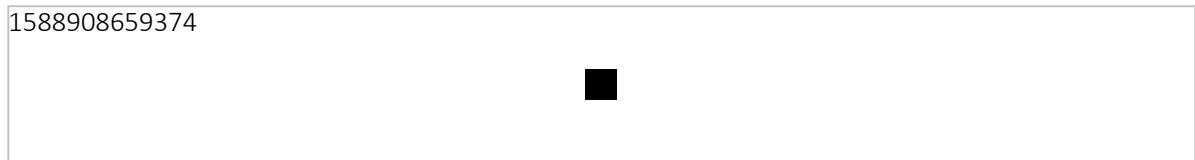
 (she/her)
A/g Manager – Industry Codes
[eSafety logo Email-Signautre](#)



 
 [eSafety.gov.au](https://www.esafety.gov.au)



1588908659374



eSafety acknowledges the Traditional Custodians of Country throughout Australia and their continuing connection to land, waters and community. We pay our respects to Aboriginal and Torres Strait Islander cultures, and to Elders past and present.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

From: s 47E(d)
To: HAMPTON,Elizabeth; GHALI,Sarah; BROWN,Rebecca; MACKIE,Tom
Cc: s 47E(d)
Subject: Briefing note - online safety industry codes decision [SEC=OFFICIAL]
Date: Wednesday, 31 May 2023 12:23:47 PM
Attachments: [image001.png](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[image006.png](#)
[image007.png](#)
[image008.jpg](#)
[OAIC Briefing Note - online safety codes decision - 310523.docx](#)

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

Dear Libby, Sarah, Bec and Tom,
Thank you very much for your time yesterday.
Please see attached for the promised briefing – we have also added our key media messages as promised.
All the best,

s 47E(d)
s 47E(d)
Avg Manager – Industry Codes
[eSafety logo Email-Signautre](#)

s 47E(d)
eSafety.gov.au



1588908659374

eSafety acknowledges the Traditional Custodians of Country throughout Australia and their continuing connection to land, waters and community. We pay our respects to Aboriginal and Torres Strait Islander cultures, and to Elders past and present.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

Briefing Note

To	Elizabeth Hampton, Sarah Ghali, Rebecca Brown
From	eSafety (s 47E(d) [REDACTED])
Date	30/05/23
Subject	OAIC briefing – online safety codes decision
Purpose	To brief the OAIC on key privacy and safety intersections and eSafety’s decision in relation to online safety codes

eSafety’s key messages

- Under Australia’s Online Safety Act 2021 which commenced on 23 January 2022, the online industry is required to develop world-first mandatory codes requiring them to take adequate steps to reduce the availability of seriously harmful online content, such as child sexual abuse and pro-terror material.
- Under the Act, the draft codes are required to be submitted to the eSafety Commissioner for registration.
- eSafety has been engaging closely with industry associations and industry participants throughout the development of the codes since mid-2021.
- In November last year, industry submitted final drafts of eight codes for registration covering the full online ecosystem including social media services, websites, search engines, app stores, internet service providers, device manufacturers, hosting services, and services such as email, messaging, gaming and dating services.
- In February, the Commissioner informed industry that she did not intend to register any of the eight codes submitted last November and asked them to resubmit amended codes which provided appropriate community safeguards required under the Act. Substantially revised codes were submitted to eSafety on 31 March this year.
- Today, the eSafety Commissioner has determined that five codes including the Social Media Services, Internet Carriage Services, App Distribution Services, Hosting Services, and Equipment codes, contain appropriate community safeguards as required under the Act to be registered.
- But two key codes fail to meet this high bar and eSafety will be rejecting them.
- These codes include the Designated Internet Services code, covering apps, websites, and file and photo storage services like Apple iCloud, Google Drive and Microsoft OneDrive;

and the Relevant Electronic Services code, covering dating sites, online games, direct and instant messaging services including encrypted services.

- These two codes have been rejected for failing to include adequate protections, including a broadly applicable commitment to proactively detect and remove known child abuse material.
- We know file and photo storage services like iCloud, Google Drive, and OneDrive are used by predators to store and share child sexual abuse material. And we also know that email services and partially encrypted messaging services are widely used by these predators to share this illegal content.
- eSafety will now draft mandatory and enforceable standards for those sections of the online industry. eSafety will consult with the OAIC in the development of these standards.
- The Commissioner will reserve her decision on a third draft code covering search engines. This code, re-submitted by industry to eSafety in late March is no longer fit for purpose following recent announcements to integrate generative AI into search engine functions.
- The Commissioner has requested that a revised search engine code be submitted within the next four weeks to address the specific concerns raised by eSafety, including the ability of the code to protect against the production of deepfake child sexual abuse material and terrorist and extremist propaganda material.
- Until now, most of the world's biggest tech companies, of which almost are headquartered in the US, have only been required under US legislation to report images of child abuse to the not-for-profit US National Center for Missing and Exploited Children (NCMEC). But they are not actually required to proactively look for these images.
- Once these codes and standards are in place, Australia will be leading the world in requiring tech companies to proactively detect, remove and prevent the spread of illegal and harmful content, including child sexual abuse and pro terrorist material.

Key points re privacy and safety intersection

- A key concern for eSafety was the absence of a commitment by key categories of online services (end-user managed hosting services, closed communication services such as email and encrypted services) to deploy technology, systems or processes to detect known (pre-identified) child sexual abuse material or pro-terror material.
- Privacy protective tools are widely available and commonly used by many industry participants. Tools such as hash matching protect both the privacy of end-users, but also, importantly, of child victims, whose privacy is repeatedly infringed when child sexual exploitation material is shared online. The trauma from materials being re-shared resulting in repeat victimisation is well-documented.
- eSafety is not asking industry participants to break end-to-end encryption. However, encryption does not mean services should be able to avoid taking steps to protect online safety and prevent the dissemination of child sexual abuse material. There are systems and processes that can be and are adopted by encrypted services to prevent the distribution of child sexual abuse material.

- eSafety will consult with the OAIC in the preparation of industry standards for Relevant Electronic Services and Designated Internet Services. eSafety wishes to ensure the industry standards for these sections of the online industry appropriately balance safety and privacy considerations.

A large, stylized graphic consisting of a red letter 'S' followed by two red numbers '22', all set against a solid black rectangular background.

If an industry code does not meet the statutory requirements including the requirement that it provides appropriate community safeguards, eSafety can determine a mandatory industry standard.

Under the Online Safety Act, industry codes or industry standards are to apply to the participants of eight key sections of the online industry, including providers of social media, messaging, websites, file and photo storage services, 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.

eSafety has been working closely with industry associations and industry participants throughout the development of the codes since mid-2021. The industry associations submitted eight codes to eSafety on 18 November 2022. eSafety provided industry with its Statements of Preliminary Views in relation to the eight draft codes and significant amendments were made to those versions before revised codes were submitted on 31 March 2023.

eSafety's decision

The five codes covering Social Media Services (SMS), Internet Carriage Services, App Distribution Services, Hosting Services, and Equipment, will be registered shortly and will come into effect six months after registration.

eSafety has decided not to register the following three codes:

- the Designated Internet Services code, covering apps, websites, and file and photo storage services like Apple iCloud and Microsoft One Drive,
- the Relevant Electronic Services code, covering dating sites, online games and other messaging services, and

- the Internet Search Engine Services code, covering search engines.

Privacy and safety intersections

A number of issues have arisen during the code development process which involve intersections between online safety and some industry participants' views of users' privacy expectations. The key issue is the proactive detection of 'known' material.

Tools to proactively detect 'known' child sexual abuse material and pro-terror material

1. A key sticking point for eSafety is the absence of a requirement on certain services covered by the RES or DIS codes to use systems, processes and/or technologies to detect and remove *known* child sexual abuse material and known pro-terror material.
2. Known child sexual abuse material and known pro-terror material is material that has been previously identified and verified as child sexual abuse material or pro-terror material, by a well-recognised non-government organisations that are legally able to view and verify the material.
3. Such material, once verified is typically then 'hashed' (ascribed a unique digital fingerprint). Online services are then able to use hash matching tools to find and prevent the re-sharing of copies of the same image or video. These tools operate without reviewing the specific content of messages.
4. The most widely known and used hash matching tool is Microsoft's PhotoDNA, which was developed in 2009 and is in use by over 200 organisations. Collisions (false positives) are theoretically possible but extremely unlikely. PhotoDNA is reported to have an expected error rate of approximately 1 in 50 billion. PhotoDNA also maintains privacy as, if a hash is not recognised, no information is kept. Microsoft itself refers to this tool as privacy protective¹.
5. While this is a common tool, the codes were drafted broadly to allow the use of "systems, processes and/or technologies" to achieve the objective of detecting and removing known child sexual abuse material and pro-terror material. Services can use alternate methods that may be more appropriate to their services.
6. Across the Social Media Services, Relevant Electronic Services and Designated Internet Services codes, a range of services undertook to follow this commitment, while others were excluded:

Table 1: Code requirements on service providers to proactively detect 'known' material

	'Known' child sexual abuse material	'Known' pro-terror material
Services required to detect and remove material	'Tier 1' social media services Certain relevant electronic services ² namely Dating services, gaming services with	'Tier 1' social media services Certain relevant electronic services ³ : Open communication RES and Tier 1 RES

¹ [\(3\) Post | Feed | LinkedIn](#)

² To the extent that they are 'capable of reviewing, assessing and removing material'

³ To the extent that they are 'capable of reviewing, assessing and removing material'

under the proposed codes	communications functionality, open communication RES, Tier 1 RES 'Tier 1' designated internet services including pornography sites	
Services not required to detect and remove material under the proposed codes	End-user managed hosting services (file and photo storage) Closed communication relevant electronic services (e.g. email) Encrypted relevant electronic services with capability to detect material (e.g. WhatsApp, iMessage)	Designated internet services, including end-user managed hosting services (file and photo storage) Closed communication relevant electronic services (e.g. email) Encrypted relevant electronic services with capability to detect material (e.g. WhatsApp)

7. eSafety's key concerns are with:

- the exclusion of end-user managed hosting services (e.g. OneDrive),
- closed communication relevant electronic services (e.g. iCloud email) and
- encrypted relevant electronic services (e.g. WhatsApp)

from this requirement. These services are known to be high risk for storage and distribution of child sexual abuse material and pro-terror material.

8. In some cases, industry has proposed commitments that require providers to take action or invest in systems which 'disrupt or deter' child sexual abuse material and pro-terror material. This broader commitment, which will require less specific steps from providers does not address the concern that many online services which do have the capability to deploy technology to detect child sexual abuse material have not committed to do so.

9. Industry associations have argued that these exclusions from the requirement to proactively detect child sexual abuse material are due to user privacy expectations and technical limitations on end-to-end encrypted services.

10. eSafety's view is that privacy and safety objectives are not mutually exclusive and it is possible to strike a balance between the two. Risks to privacy can be managed and mitigated with the appropriate tools. As set out above, hash matching is widely considered privacy protective.

11. We do not agree that users' privacy expectations are such that closed communication and encrypted RES Providers are precluded from taking reasonable steps to detect and prevent the distribution and online storage of known CSAM and known pro-terror material on their services.

12. We also know that several of these services – including Dropbox, OneDrive, iCloud email – use hash matching on their services. WhatsApp uses hash matching on unencrypted surfaces (e.g. group names and profile photos). The absence of a commitment from these services does not match current practice by many services.

13. We consider that tools such as hash matching protect both the privacy of end-users, but also, importantly, of child victims, whose privacy is repeatedly infringed when child sexual exploitation material is shared online. The trauma from materials being re-shared resulting in repeat victimisation is well-documented.

S 22

From: s 47E(d)
To: s 47E(d) HAMPTON,Elizabeth; GHALI,Sarah; BROWN,Rebecca; MACKIE,Tom
Cc: s 47E(d)
Subject: RE: Briefing note - online safety industry codes decision [SEC=OFFICIAL]
Date: Wednesday, 31 May 2023 12:26:36 PM
Attachments: [image001.png](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[image006.png](#)
[image007.png](#)
[image008.jpg](#)

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

Thanks s 47E(d)

I will just add that we have indicated that we will consult with the OAIC in relation to the development of industry standards for the Designated Internet Services and Relevant Electronic Services sections of the online industry.

Apologies for not mentioning this to you yesterday.

Please let me know if you have any concerns with this.

Kind regards

s 47E(d)

From: s 47E(d)
Sent: Wednesday, 31 May 2023 12:22 PM
To: HAMPTON,Elizabeth <Elizabeth.Hampton@oaic.gov.au>; GHALI,Sarah <Sarah.Ghali@oaic.gov.au>; Rebecca.Brown@oaic.gov.au; MACKIE,Tom <Tom.Mackie@oaic.gov.au>
Cc: s 47E(d) s 47E(d)
Subject: Briefing note - online safety industry codes decision [SEC=OFFICIAL]

OFFICIAL

Dear Libby, Sarah, Bec and Tom,

Thank you very much for your time yesterday.

Please see attached for the promised briefing – we have also added our key media messages as promised.

All the best,

s 47E(d)

(she/her)
A/g Manager – Industry Codes
[eSafety logo Email-Signautre](#)

s 47E(d)
eSafety.gov.au



1588908659374

eSafety acknowledges the Traditional Custodians of Country throughout Australia and their continuing connection to land, waters and community. We pay our respects to Aboriginal and Torres Strait Islander cultures, and to Elders past and present.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.