JIM JORDAN, Ohio
CHAIRMAN

JAMIE RASKIN, Maryland
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–6906
judiciary.house.gov

November 18, 2025

Ms. Julie Inman Grant
Australian eSafety Commissioner

via email

Dear Ms. Inman Grant:

The Committee on the Judiciary of the U.S. House of Representatives is conducting oversight of how and to what extent foreign laws, regulations, and judicial orders compel, coerce, or influence companies to censor speech in the United States.[1] To develop effective legislation, such as new statutes to ensure that foreign laws cannot silence Americans in the United States or severely burden American companies, the Committee must first understand the nature of the harms imposed by these foreign laws. As the Australian eSafety Commissioner, you are the official primarily responsible for enforcing Australia's Online Safety Act (OSA), which imposes obligations on American companies and threatens speech of American citizens.[2] In addition, you have been working with U.S.-based organizations and universities to facilitate and encourage cooperation with foreign censorship regimes, including the OSA.[3] As such, we respectfully request your testimony at a transcribed interview to inform the Committee's oversight.

Your expansive interpretation and enforcement of Australia's OSA—including your claim of extraterritorial jurisdiction to censor speech outside of Australia—directly threatens

[1] *See, e.g.*, STAFF OF THE H. COMM. ON THE JUDICIARY, 119TH CONG., THE FOREIGN CENSORSHIP THREAT: HOW THE EUROPEAN UNION'S DIGITAL SERVICES ACT COMPELS GLOBAL CENSORSHIP AND INFRINGES ON AMERICAN FREE SPEECH (Comm. Print July 25, 2025); Press Release, H. Comm. on the Judiciary, Chairman Jordan Subpoenas Big Tech for Information on Foreign Censorship of American Speech (Feb. 26, 2025).
[2] *See Our Commissioner*, ESAFETY COMMISSIONER, https://www.esafety.gov.au/about-us/about-the-commissioner (last accessed Oct. 30, 2025); *What we do*, ESAFETY COMMISSIONER, https://www.esafety.gov.au/about-us/what-we-do (last accessed Oct. 30, 2025).
[3] *See e.g.,* Compliance and Enforcement in a Rapidly Evolving Landscape Agenda and Attendee List (Sep. 24, 2025) (on file with Comm.).

American speech.[4] Global content takedown orders are concerning because they harm the free speech rights of those outside of Australia's jurisdiction and set the precedent that other governments may do the same. For example, in 2024, your Commission sought to compel X to remove content globally, arguing that its geo-blocking of the content was insufficient because Australians could use VPNs to access the content.[5] Other censorship regimes, like the one in Brazil, have used similar justifications when ordering global takedowns of content and threatening fines for VPN use.[6]

The Committee has also learned that you have colluded with pro-censorship entities in the United States to facilitate Australia's, and other, global censorship regimes. According to documents obtained by the Committee, you recently gave the "keynote" at a non-public event at Stanford University on September 25, 2025.[7] Other attendees and panelists included officials from some of the entities with the worst track records of extraterritorial censorship, including the European Union and Brazil.[8] The stated purpose of this event was to "bring[] together policy makers, academics, and experienced Silicon Valley experts to discuss the state of compliance and enforcement of existing regulations related to online trust and safety."[9] Put plainly, the roundtable sought to facilitate cooperation with global censorship by bringing together foreign officials who have directly targeted American speech and represent a serious threat to the First Amendment.

On the same day you appeared at Stanford's censorship roundtable, your Commission announced that an academic panel from Stanford's Social Media Lab would "support the eSafety Commissioner"—you—in examining how to implement social media laws and evaluate their

---

[4] *See e.g.,* Letter from Australia's eSafety Commission requiring X to take down content worldwide because it can be accessed via VPN (Apr. 18, 2024) (on file with Comm.); Tom Crowley, *'Silly' to demand global takedowns: Dutton weighs in on eSafety case*, AUSTRALIAN BROADCASTING CORP. (Apr. 25, 2024).

[5] *Id*. In April 2024, you, as eSafety Commissioner, issued orders to X and other platforms to remove certain content. X ultimately complied with this order by making the posts unavailable to Australian users while allowing the posts to remain on the site. You then sought a legal order to compel X to takedown the content globally, which X challenged. Tom Crowley, *'Silly' to demand global takedowns: Dutton weighs in on eSafety case*, AUSTRALIAN BROADCASTING CORP. (Apr. 25, 2024).

[6] *Fact Check: Brazilians Can Be Fined for Using VPN to Access X*, REUTERS (Sept. 6, 2024) (last updated Sept. 9, 2024).

[7] Compliance and Enforcement in a Rapidly Evolving Landscape Agenda and Attendee List (Sep. 24, 2025) (on file with Comm.).

[8] *See, e.g.*, STAFF OF THE H. COMM. ON THE JUDICIARY, 119TH CONG., THE FOREIGN CENSORSHIP THREAT: HOW THE EUROPEAN UNION'S DIGITAL SERVICES ACT COMPELS GLOBAL CENSORSHIP AND INFRINGES ON AMERICAN FREE SPEECH (Comm. Print July, 25, 2025); STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION'S SILENCE: THE CASE OF BRAZIL (Comm. Print Apr. 17, 2024); STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION'S SILENCE: THE CASE OF BRAZIL, PART II (Comm. Print May 7, 2024); Rep. Jim Jordan (@Jim_Jordan), X (July 28, 2025, 10:58 AM), https://x.com/Jim_Jordan/status/1949846809238446237; Rep. Jim Jordan (@Jim_Jordan), X (July 29, 2025, 9:30 PM), https://x.com/Jim_Jordan/status/1950368307372020086.

[9] Compliance and Enforcement in a Rapidly Evolving Landscape Agenda and Attendee List (Sep. 24, 2025) (on file with Comm.).

effectiveness.[10] These close ties with Stanford are troubling given the university's past efforts to facilitate U.S. government censorship of lawful American speech.[11] As the Committee found in the 118th Congress, the Stanford Internet Observatory played a key role in laundering government censorship requests to social media platforms, enabling officials in the U.S. government to covertly silence American voices to influence the 2020 U.S. presidential election.[12]

As a primary enforcer of Australia's OSA and noted zealot for global takedowns, you are uniquely positioned to provide information about the law's free speech implications—both in the U.S. and abroad. This information will inform the Committee's legislative reforms aimed, in part, at ensuring that foreign censors cannot silence protected American speech. Accordingly, we respectfully request your cooperation and ask that you make yourself available for a transcribed interview with the Committee. Please contact Committee staff to schedule your transcribed interview as soon as possible but no later than 10:00 a.m. ET on December 2, 2025.

The Supreme Court has recognized that Congress has a "broad and indispensable" power to obtain information and conduct oversight, which "encompasses inquiries into the administration of existing laws, studies of proposed laws, and surveys of defects in our social, economic or political system for the purpose of enabling the Congress to remedy them."[13] Pursuant to the Rules of the House of Representatives, the Committee on the Judiciary has jurisdiction to conduct oversight of matters concerning "[c]ivil liberties" to inform potential legislative reforms.[14]

If you have any questions, please contact Committee staff at +1 (202) 225-6906. Thank you for your prompt attention to this matter.

Sincerely,

Jim Jordan
Chairman

cc: The Honorable Jamie Raskin, Ranking Member

---

[10] Press Release, Australian eSafety Commissioner, eSafety appoints Stanford University-led academic advisory group to assess the impacts of the Social Media Minimum Age obligation (Sep. 25, 2025), https://www.esafety.gov.au/newsroom/media-releases/esafety-appoints-stanford-university-led-academic-advisory-group-to-assess-the-impacts-of-the-social-media-minimum-age-obligation.

[11] *See* STAFF OF THE H. JUDICIARY COMM. & THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, THE WEAPONIZATION OF 'DISINFORMATION' PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS' FREE SPEECH, (Nov. 6, 2023).

[12] *Id*.

[13] *Trump v. Mazars USA, LLP*, 591 U.S. 848, 862 (2020) (citation and internal quotation marks omitted).

[14] Rules of the House of Representatives, R. X, cl. 1(*l*)(5) (2025).

2 December 2025 CC25-0191

Congressman Jim Jordan
Chairman, Committee on the Judiciary
United States House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

CC: The Honorable Jamie B. Raskin, Ranking Member, Committee on the Judiciary

Dear Mr Jordan

I refer to your letter dated 18 November 2025 in which you invited me to voluntarily provide testimony at a transcribed interview before the Committee about Australia's *Online Safety Act 2021* (Cth) (the Act) and my role as eSafety Commissioner, enforcing compliance with the Act.

While I am not in a position to attend an interview, in response to your letter, I provide the following summary of our approach.

As you would understand, all businesses operating in Australia, including technology platforms, must comply with Australian laws, including the Act. Australian laws have been enacted in response to increasing online harms and the decreasing efforts and effectiveness of the steps online platforms are taking to mitigate those harms to Australians.

eSafety's current approach to responding to illegal and restricted content, particularly Class 1 material, builds on the Court's guidance on the interpretation and application of the relevant illegal and restricted removal powers in the Act, particularly around what would constitute "removal" for the purposes of the Act.

While that means that it is unlawful for businesses to display or distribute in Australia material classified as 'refused classification' under Australian law, it would not prevent a business from displaying or distributing material of that kind in other jurisdictions that is not child sexual abuse material.

In other words, nothing we do here in Australia prevents American companies from displaying non-child sexual abuse material to Americans.

This was most recently demonstrated through our acceptance of geo-blocking of graphic video footage of the Charlie Kirk, Iryna Zarutska, and Chandra Mouli Nagamallaiah murders. In each case, the independent Classification Board classified certain material containing

violent graphic imagery as 'refused classification', which is the highest possible rating and is given to material that is outside generally accepted community standards.

Based on the Classification Board's decisions, eSafety issued removal notices for that and similar material. eSafety accepted geo-blocking, so the material is not displayed to users in Australia, as compliance with the statutory removal notice.

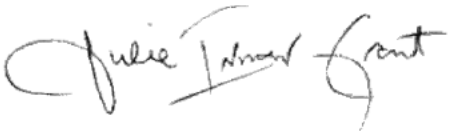
As the laws are relatively new, many of the provisions are only now being tested and interpreted by the courts. eSafety continues to update its processes to reflect judicial and administrative guidance about the provisions.

Finally, I'd like to point out also that there may be more that unites us than divides us in terms of similar approaches to tackling child sexual abuse material and the non-consensual sharing of intimate imagery, noting that the TAKE IT DOWN Act provisions closely resemble Australia's image-based abuse scheme, which has been in operation for 8 years.

Thank you for your interest in the work of eSafety and how legislatures, platforms and regulators around the work can work together to address online harms in both Australia and the United States of America.

We hope this information will assist you and the Committee in your further exploration of these issues.

Yours sincerely,



Julie Inman Grant
eSafety Commissioner

JIM JORDAN, Ohio
CHAIRMAN

JAMIE RASKIN, Maryland
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–6906
judiciary.house.gov

December 30, 2025

Ms. Julie Inman Grant
Australian eSafety Commissioner

via email

Dear Ms. Inman Grant:

The Committee on the Judiciary of the U.S. House of Representatives is conducting oversight of how and to what extent foreign laws, regulations, and judicial orders compel, coerce, or influence companies to censor speech in the United States.[1] To develop effective legislation, such as new statutes to ensure that foreign laws cannot silence Americans in the United States or severely burden American companies, the Committee must first understand the nature of the harms imposed by these foreign laws. For this reason, on November 18, 2025, the Committee requested your testimony at a transcribed interview.[2] On December 2, 2025, you declined to testify, stating that you were "not in a position to attend an interview."[3] We write to reiterate our request for your voluntary testimony.

Your testimony remains vital to the Committee's oversight. We are concerned about the extraterritorial content moderation requirements of Australia's Online Safety Act, eSafety's attempts to mandate global content takedowns, and your collaboration with a U.S. university and other foreign governments to design and implement a global censorship regime.[4] Moreover, new documents indicate that eSafety harassed American companies ahead of the implementation of the Social Media Minimum Age (SMMA) law.[5] Emails and correspondence produced to the Committee show that even before the law's effective date, eSafety directed American platforms

---

[1] *See, e.g.*, STAFF OF THE H. COMM. ON THE JUDICIARY, 119TH CONG., THE FOREIGN CENSORSHIP THREAT: HOW THE EUROPEAN UNION'S DIGITAL SERVICES ACT COMPELS GLOBAL CENSORSHIP AND INFRINGES ON AMERICAN FREE SPEECH (Comm. Print July 25, 2025); Press Release, H. Comm. on the Judiciary, Chairman Jordan Subpoenas Big Tech for Information on Foreign Censorship of American Speech (Feb. 26, 2025).
[2] Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Julie Inman Grant, Australian eSafety Commissioner (Nov. 18, 2025).
[3] Letter from Ms. Julie Inman Grant, Australian eSafety Commissioner, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Dec. 2, 2025).
[4] *See* Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Julie Inman Grant, Australian eSafety Commissioner (Nov. 18, 2025).
[5] *Online Safety Amendment (Social Media Minimum Age) Bill 2024* (Cth); *see* Enclosure.

to release "public-facing" compliance commitments based on an eSafety "template,"[6] and demanded meetings with platforms that did not immediately comply.[7] Similarly, the Communications Ministry, one of the Australian agencies responsible for the implementation of the SMMA, solicited SMMA "talking points" from each platform to demonstrate that they were "working collaboratively with the government."[8]

In addition, documents show that eSafety formally asked American companies how they planned to "mitigate potential circumvention" of the SMMA law "via VPNs."[9] In 2024, you used concerns about VPNs, which may conceal a user's country of origin, as a pretext to demand global takedowns of social media content.[10] The documents obtained by the Committee suggest that you may be using this playbook again.[11] Testimony about each of these initiatives will inform the Committee's legislative reforms aimed at ensuring that foreign censors cannot silence protected American speech.[12]

We appreciate the limited information you provided in your response letter of December 2; however, that information is not sufficient to satisfy the Committee's oversight. For example, your letter doesn't address eSafety's previous attempts to mandate global takedowns or your participation in a September 2025 roundtable event at Stanford University in which "misinformation" pseudoscientists and censorious foreign government officials discussed how to build and operationalize an effective global internet censorship regime.[13] Your attendance at the Stanford event also undermines the argument that you are "not in a position to attend an interview" in the United States.[14] Clearly, you are willing and able to return to the United States when it suits you.

The Supreme Court has recognized that Congress has broad authority to gather information from U.S. persons and entities to inform legislative reforms.[15] The Court has

---

[6] Letter from eSafety to Platform (Nov. 7, 2025) (enclosed); *see* Template Commitment to Compliance (enclosed).
[7] Email from eSafety to Platform (Nov. 16, 2025) (enclosed).
[8] Email from Communications Ministry to Platform (Nov. 16, 2025) (enclosed).
[9] Letter from eSafety to Platform (Nov. 7, 2025) (enclosed).
[10] *See e.g.,* Letter from Australia's eSafety Commission requiring X to take down content worldwide because it can be accessed via VPN (Apr. 18, 2024) (on file with Comm.); Tom Crowley, *'Silly' to demand global takedowns: Dutton weighs in on eSafety case*, AUSTRALIAN BROADCASTING CORP. (Apr. 25, 2024).
[11] *Cf.* Letter from eSafety to Platform (Nov. 7, 2025) (enclosed); Tom Crowley, *'Silly' to demand global takedowns: Dutton weighs in on eSafety case*, AUSTRALIAN BROADCASTING CORP. (Apr. 25, 2024).
[12] *See* H.R. 1071, No Censors on our Shores Act, 119th Cong. (2025).
[13] *See* Letter from Australia's eSafety Commission requiring X to take down content worldwide because it can be accessed via VPN (Apr. 18, 2024) (on file with Comm.); Tom Crowley, *'Silly' to demand global takedowns: Dutton weighs in on eSafety case*, AUSTRALIAN BROADCASTING CORP. (Apr. 25, 2024); Compliance and Enforcement in a Rapidly Evolving Landscape Agenda and Attendee List (Sep. 24, 2025) (on file with Comm.); *see* Michael Shellenberger, *Obama-Linked Stanford Center Held Secret Meeting with Foreign Governments to Plot Global Internet Censorship*, PUBLIC NEWS (Oct. 28, 2025); Teddy Ganea et al., *Stanford's Cyber Policy Center Coordinates International Internet Censorship*, THE STANFORD REV. (Oct. 29, 2025).
[14] Letter from Ms. Julie Inman Grant, Australian eSafety Commissioner, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Dec. 2, 2025).
[15] *See Trump v. Mazars USA, LLP*, 591 U.S. 848, 862 (2020) (Congress's oversight power "encompasses inquiries into the administration of existing laws, studies of proposed laws, and surveys of defects in our social, economic, or political system for the purpose of enabling the Congress to remedy them." (internal citation omitted)).

explained that compliance with a congressional inquiry is a "public duty, which every person within the jurisdiction of the [U.S.] Government is bound to perform when properly summoned."[16] U.S. citizenship carries with it both benefits and responsibilities, and those, such as yourself, who enjoy the advantages associated with such citizenship should be willing to shoulder the responsibilities as well, including cooperating with congressional investigations. In other contexts, courts have routinely found that U.S. citizens living abroad are within the jurisdiction of the U.S. government and can be compelled to provide testimony.[17]

Accordingly, we reiterate our request for your cooperation and ask that you make yourself available for a transcribed interview with the Committee. Pursuant to the Rules of the House of Representatives, the Committee on the Judiciary has jurisdiction to conduct oversight of matters concerning "[c]ivil liberties" to inform potential legislative reforms.[18] Please contact Committee staff to schedule your transcribed interview as soon as possible but no later than 10:00 a.m. ET on January 13, 2026. The Committee may have to consider, if necessary, additional steps to obtain compliance with our request.

If you have any questions, please contact Committee staff at +1 (202) 225-6906. Thank you for your prompt attention to this matter.

Sincerely,

Jim Jordan
Chairman

cc: The Honorable Jamie Raskin, Ranking Member

Enclosure

[16] *United States v. Bryan*, 339 U.S. 323, 331 (1950).
[17] *See e.g.*, *Blackmer v. United States*, 284 U.S. 421, 439-440 (1932) ("As the Congress could define the obligation, it could prescribe a penalty to enforce it. And as the default lay in disobedience to an authorized direction of the court, it constituted a contempt of court, and the Congress could provide for procedure appropriate in contempt cases."); *see also id*. at 436-37 (A U.S. citizen residing in a foreign country "continue[s] to owe allegiance to the United States." . . . "Nor can it be doubted that the United States possesses the power inherent in sovereignty to require the return to this country of a citizen, resident elsewhere, whenever the public interest requires it, and to penalize him in case of refusal.").
[18] Rules of the House of Representatives, R. X, cl. 1(*l*)(5) (2025).

Enclosure

[redacted]

[redacted]

[redacted]_Correspondence from eSafety Commissioner_[redacted]_Plans for compliance with the Social Media Minimum Age [SEC=OFFICIAL]

1 message

Julie Inman Grant <[redacted]@esafety.gov.au> Fri, Nov 7, 2025 at [redacted]

To: [redacted]

Cc: [redacted], Social Media Minimum Age Restrictions <[redacted]@esafety.gov.au>, eSafety Industry Supervision <[redacted]@esafety.gov.au>, [redacted]@esafety.gov.au>, [redacted]@esafety.gov.au>, [redacted]@esafety.gov.au>, Julie Inman Grant <[redacted]@esafety.gov.au>

OFFICIAL

Dear [redacted]

Please find attached correspondence from the esafety Commissioner regarding [redacted]s plans for compliance with the Social Media Minimum Age.

As outlined in the letter, please also find attached the *Statement of Commitment to Comply* template.

Have a lovely weekend

Kind regards

[redacted] *p.p eSafety Commissioner*

Julie Inman Grant
Commissioner

[redacted]

[redacted]

Executive Assistant [redacted]@esafety.gov.au

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.

2 attachments

[redacted]Correspondence from eSafety Commissioner_[redacted]_Plans for compliance with the Social Media Minimum Age.pdf

Statement of commitment to comply - TEMPLATE .docx
639K

[redacted]

Australian Government | eSafetyCommissioner

7 November 2025 [redacted]

[redacted]

By email: [redacted]

CC: [redacted]; [redacted]; [redacted];

Dear [redacted]:

[redacted]'s plans to comply with the Social Media Minimum Age

Thank you for your engagement with eSafety to date regarding the Social Media Minimum Age (SMMA) obligation. We refer to:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]

Thank you for confirming [redacted]'s intention to comply with the SMMA obligation. With just over a month until the SMMA takes effect on 10 December 2025, we request [redacted] provide:

1. an outline of the steps you intend to take to comply, as well as a short public-facing summary of these steps, and
2. an early indication of the number of accounts likely to be removed or deactivated by 10 December 2025.

eSafety is making the same requests of all services which we have assessed as age-restricted social media platforms.

Our understanding of [redacted]'s current age gating and assurance measures

From eSafety's Behind the Screen Report and our discussions to date, we understand [redacted] currently has the following age gating and assurance measures in place:

- [redacted]

Compliance plans

We request the following information about the steps [redacted] intends to take to comply with the SMMA obligation:

1. **Finding and actioning accounts held by Australian end-users under the age of 16 (age-restricted users)**
    a. [redacted]

[1] See *eSafety's Behind the Screen Transparency Report*

[redacted]

[redacted] How does [redacted] plan to identify which accounts are or may be held by age-restricted users?

b. Based on that methodology, how many accounts does [redacted] anticipate will be impacted by the SMMA obligation on 10 December?
c. What steps does [redacted] intend to take for those accounts on 10 December (e.g. deleting, deactivating, disabling, suspending, etc)?
    i. Under what circumstances (e.g. pending age assurance, moderator review, etc)?
    ii. Will end-users be given a choice about what happens to their account?
d. What information will be provided to those account holders, and when will it be provided? eSafety considers it to be good practice to provide this information to account holders no later than 2 weeks before the SMMA obligation takes effect. eSafety has published resources that we encourage service providers to include in communication with their end-users.
    i. Do you have information or a URL you could provide to eSafety to direct members of the public if they have questions about [redacted]'s approach?

2. Age assurance and user reporting options

a. What age assurance options will [redacted] apply to comply with the SMMA obligation?
    i. Will [redacted] be using [redacted] or another third-party age assurance vendor? If so, which vendor? Where in the user-journey will this be applied?
b. Does [redacted] intend to use government-issued ID as an option for age verification to comply with the SMMA obligation?
    i. If so, can [redacted] confirm that it will always provide a reasonable alternative means to the collection of government-issued ID for purposes of complying with the SMMA obligation, consistent with the requirement under section 63DB?
c. Will [redacted] rely on existing underage user reporting mechanisms? If so, will [redacted] make any adjustments to these mechanisms, including planning for a possibility of increased user reporting in Australia from 10 December 2025?
d. What new, if any, user reporting mechanisms does [redacted] intend to apply?

3. Review and appeals mechanisms

[redacted]

a. Will [redacted] rely on existing review and appeals mechanisms for accounts that may be erroneously determined to be held by an age-restricted user? If so, will [redacted] make any changes to these mechanisms, including planning for a possibility of increased review and appeals requests in Australia from 10 December 2025?
b. What, if any, new review and appeals mechanisms for accounts that may have been erroneously determined to be held by an age-restricted user does [redacted] intend to apply?

4. Circumvention

a. What steps will [redacted] take to prevent circumvention of the SMMA on the basis of age and/or location?
    i. What location signals will [redacted] consider beyond end-users' IP addresses to mitigate potential circumvention via VPNs?
b. [redacted] Will [redacted] use the same indicators and/or other indicators to prevent age-restricted users whose accounts have been removed or deactivated from creating new accounts?

We seek [redacted]'s response to the above questions by **21 November 2025.**

In addition to providing this information to eSafety, we request [redacted] provide eSafety with a short summary of your compliance plans and statement of commitment to comply with the SMMA obligation which can be shared with the public for transparency. We have attached a template statement which can be used as a template for this purpose. We seek [redacted]'s public statement of commitment by **14 November 2025**.

Please contact [redacted]@esafety.gov.au should you wish to discuss this letter further.

Yours faithfully,

Julie Inman Grant
eSafety Commissioner

[3] See *eSafety's Behind the Screen Transparency Report*

[redacted]

Australian Government | eSafetyCommissioner

Template commitment to compliance

Note: This template has been provided to all services that eSafety has assessed as age-restricted social media platforms as of 7 November 2025. We encourage services to complete, submit to eSafety and ultimately publish a version of the template reflecting their commitments to promote transparency, accountability and shared expectations ahead of the SMMA obligation coming into effect on 10 December 2025.

Statement of commitment to comply with SMMA obligations

[COMPANY] affirms its commitment to take reasonable steps to comply with the new Social Media Minimum Age (**SMMA**) obligations which commence on 10 December 2025.

[COMPANY] is committed to applying the principles set out in eSafety's Regulatory Guidance, including respecting and promoting the human rights that underpin the principles. Accordingly, [COMPANY] will take reasonable steps to:

- Detect and deactivate/remove accounts held by Australians under 16 with kindness, care and clear communication.
- Implement technical measures to prevent circumvention, including re-registration of those users under 16 years of age.
- Use layered age assurance methods, which include age estimation and trusted vouching, to determine an account holder's age, consistent with the guiding principles set out in eSafety's Regulatory Guidance.
- Enhance current reporting pathways for users to report underage accounts by making the reporting form easier to find and access. Reports will be reviewed by our Trust & Safety team, supported by AI signals.
- Provide clear review pathways for users to challenge decisions through accessible and fair processes that will be handled by experienced human reviewers.
- Continuously monitor and improve systems by tracking the accuracy and effectiveness of our age assurance methods

[redacted]

- Provide eSafety with regular data to demonstrate [COMPANY'S] compliance with the SMMA obligations.

Changes to accounts belonging to someone under 16

From [DAY, MONTH] 2025, suspected underage account holders will receive a notification [INSERT METHOD E.G. IN-APP OR VIA EMAIL] explaining how their account was identified as belonging to an under-16, and clear communication about Australia's SMMA law, along with the following information:

1. Account holders will have [TIME PERIOD] to download their data.
2. The account will be deactivated and remain deactivated for [TIME PERIOD] before being permanently deleted. If the account holder turns 16 within this time frame, they can request to go through an age check to have their account reinstated.
3. If the account holder has incorrectly been identified as an under-16 Australian end-user, they will have [XX] days to commence an appeal process, where they will be asked to undertake our age check process. This includes options for [INSERT INFORMATION SUCH AS UNDERGOING FACIAL AGE ESTIMATION, TRUSTED VOUCHING, OR SUBMITTING GOVERNMENT-ISSUED ID]. If the original decision is upheld, the [TIME PERIOD] deactivation period will commence, along with access to download their data for [TIME PERIOD].
    - All age checks will be done [IN-APP OR VIA XX].
4. Account holders will not be asked to provide their [INSERT INFORMATION / ID THAT WILL NOT BE COLLECTED AS PART OF AGE CHECK].
5. Account holders can request to have their account permanently deleted at any time.
6. For those looking for more information about the new law and support, visit esafety.gov.au. You can also get help and support from:
    a. Beyond Blue – 1300 22 4636
    b. Kids Helpline – 1800 55 1800
    c. Headspace – 1800 650 890
    d. Lifeline – 13 11 14

Reporting suspected underage accounts

Anyone can report suspected underage accounts through the [INSERT INFORMATION SUCH AS REPORT FEATURE OR WEB FORM]. Reports are reviewed by [INSERT INFORMATION SUCH AS TRUST & SAFETY TEAM].

Communicating these changes

We are committed to keeping users informed. These changes are being communicated through [INSERT INFORMATION SUCH AS IN-APP NOTIFICATIONS OR HELP CENTRE]. We will also be publishing updated Terms of Service of our website.

[redacted]

[redacted]

Meeting request to discuss SMMA communication timeframes [SEC=OFFICIAL]

1 message

eSafety Industry Supervision [redacted]@esafety.gov.au> Sun, Nov 16, 2025 [redacted]
To: [redacted]
Cc: [redacted], eSafety Industry Supervision [redacted]@esafety.gov.au>

OFFICIAL

Dear [redacted]

We understand [redacted] may still be considering eSafety's letter of 7 November, which requested a response regarding public-facing compliance commitments by last Friday, 14 November, and a response to eSafety's additional compliance questions by this Friday, 21 November.

While we continue to look forward to your response to eSafety's compliance questions, we note you did not provide a response relating to public-facing commitments last week.

Accordingly, **eSafety would like to meet with** [redacted] **as soon as possible** to discuss your timeframes for communicating to [redacted]'s users about the upcoming changes to comply with the SMMA obligations, in particular, if and when under 16 users will be notified about their accounts being deactivated or removed and when actions will be taken in relation to these accounts.

I can send through some proposed times shortly if you agree.

Thank you

[redacted]

Assistant Manager, Industry Supervision

Industry Compliance and Enforcement Branch

[redacted]

eSafetyCommissioner eSafety.gov.au

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.

[redacted]

TPs about compliance plans [SEC=OFFICIAL]

[redacted]@mo.communications.gov.au [redacted] Sunday, November 16, 2025 at [redacted]

To: [redacted]
Cc: [redacted]@pm.gov.au [redacted]

OFFICIAL

OFFICIAL

Hi [redacted],

In the lead up to 10 December, the Minister and PMO would appreciate talking points from [redacted] about:

1. what your age assurance waterfall will look like;
2. how you're communicating your age assurance process with your users; and
3. what your appeals process will look like for users.

Any screenshots you can provide as examples would also be helpful.

This information will help the Minister communicate with [redacted]'s users when she is doing media and also demonstrate how [redacted] is working collaboratively with the government to comply with the law.

Kind Regards,

[redacted]

[redacted] • Office of the Hon Anika Wells MP • Minister for Communications and Minister for Sport

[redacted]@mo.communications.gov.au

M [redacted]

Parliament House, Canberra ACT 2600, Australia

Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts
CONNECTING AUSTRALIANS • ENRICHING COMMUNITIES • EMPOWERING REGIONS

infrastructure.gov.au

I would like to acknowledge the traditional custodians of this land on which we meet, work and live.

I recognise and respect their continuing connection to the land, waters and communities

[redacted]

I pay my respects to Elders past and present and to all Aboriginal and Torres Strait Islanders

OFFICIAL

Attachments:

image001.png 1.7k

[redacted]

19 January 2026

CC26-0002

Congressman Jim Jordan
Chairman, Committee on the Judiciary
United States House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

CC: The Honorable Jamie B. Raskin, Ranking Member, Committee on the Judiciary

Dear Chairman Jordan

I refer to your letter dated 30 December 2025 in response to my letter of 2 December 2025. In your letter you again note a range of issues and invite me to voluntarily provide testimony at a transcribed interview before the Committee about Australia's *Online Safety Act 2021* (Cth) (the Act).

In response to the issues noted in your letter, I am providing the attached information, which describes eSafety's role and the operation of the Act.

Many of the issues you have raised are outside my role as they relate to Australian policy and legislative settings, rather than regulatory implementation, which is my statutory authority. Decisions about the underlying policy settings and scope of the Act are matters for Commonwealth Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts and the Minister for Communications.

As I outlined in my attached information, all businesses operating in Australia, including technology platforms, must comply with Australian laws, including the Act where applicable. eSafety does not prevent platforms from displaying content to users in the United States.

I hope this information will assist you and the Committee in your further exploration of these issues.

Yours sincerely,

Julie Inman Grant
eSafety Commissioner

Information about Australia's *Online Safety Act 2021 (Cth)*

The eSafety Commissioner (eSafety) welcomes the opportunity to explain to the Committee on the Judiciary of the U.S. House of Representatives the nature of our role, Australia's online safety regulatory framework, and the important free speech protections incorporated into the regulatory framework in the *Online Safety Act 2021* (Cth) (the Act).[1] Below, we have focussed on responding to the issues you have raised.

Importantly, all businesses operating in Australia regardless of where they are headquartered, must comply with Australian laws, including the Act where applicable.

In complying with Australian law, platforms are not prevented from displaying or distributing material in other jurisdictions. The Act is about protecting Australians, particularly Australian children, in line with community expectations.

We understand the United States at both federal and state level is also grappling with online safety, for example through the *Take It Down Act*[2] and local legislation passed by several US states, including Florida, Georgia, Louisiana, Mississippi, Nebraska, Ohio, Tennessee, Texas and Utah.

1. eSafety's role in protecting Australians from online harms

eSafety is Australia's independent regulator, educator and coordinator for online safety. Our purpose is to help safeguard Australians from online harms and to promote safer, more positive online experiences.

The Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts has the policy responsibility for online safety laws and policies in Australia. Decisions about the policy settings and scope of the Act is a matter for the Department and the Minister for Communications.

---

[1] https://www.legislation.gov.au/C2021A00076/latest/text.
[2] https://www.congress.gov/bill/119th-congress/senate-bill/146.

Once laws are passed by the democratically elected Australian Parliament and in effect, eSafety's role is to implement and enforce them. The eSafety Commissioner is an independent statutory role, appointed by the Minister for Communications. eSafety's remit and the eSafety Commissioner's powers and functions[3] are set out in the Act.

eSafety focusses predominantly on serious online harms such as the cyberbullying of children, adult cyber abuse, image-based abuse (sharing, or threatening to share, intimate images without the consent of the person shown) and illegal and restricted content. More details about this work are detailed below.

Since our establishment in 2015, the Australian Parliament has expanded the Act and eSafety's remit to respond to digital developments and increasing serious online harms:

- In 2015, Parliament passed the *Enhancing Online Safety Act 2015,* which established the Office of the Children's eSafety Commissioner.
- In 2017, Parliament expanded eSafety's remit to include protections for all Australians. The Children's eSafety Commissioner became the eSafety Commissioner.
- In 2019, Parliament expanded eSafety's remit to include additional responsibilities under laws criminalising the sharing of Abhorrent Violent Material, such as terrorist or extreme violent content.
- In 2021, Parliament expanded eSafety's remit through the *Online Safety Act 2021*.
- In 2024, Parliament expanded eSafety's remit to include a social media minimum age framework, which as outlined below, prevents Australian children under 16 from having an account on age restricted social media platforms.

As with all Australian Bills or legislative instruments, these legislated changes included a Statement of Compatibility, which assessed the compatibility of the measures with the rights and freedoms recognised in the 7 core international human rights treaties that Australia has ratified. Each time, the proposed powers and functions were found to be compatible with Australia's human rights and freedoms obligations.

[3] Sections 27 and 28 of the Act.

- The explanatory memorandum for the Act[4] determined that providing protections for categories of material within the Act, including the depiction of child sexual abuse or the promotion of terrorism, are consistent with the freedom of expression, as the restrictions are provided for by law, and are necessary for respect to the rights and reputation of others, or for the protection of national security, public order, health or morals. It also found the measures were reasonable and proportionate to achieving the legitimate policy objective of improving and promoting online safety for Australians.

eSafety's legislative framework has been externally and independently reviewed twice during our 10 years of operation to ensure Australia's online safety laws keep pace with the evolving online environment. Both reviews positively affirmed the vital role eSafety plays in keeping Australians safer online, while also supporting measures to strengthen our legislative framework. The most recent review was conducted in October 2024.

eSafety administers a range of schemes under the Act, including:

- The Social Media Minimum Age obligation, which commenced on 10 December 2025, and requires age restricted social media platforms to take reasonable steps to ensure Australians under 16 do not have an account on their service. This initiative was legislated on a bipartisan basis at the Commonwealth level and also has broad support across Australian states and territories. The obligation was developed in close consultation with industry, as is normal practice in Australia.
- Industry codes and standards where, by legislative design, industry codes are drafted by industry, for industry.[5] Standards may be drafted by eSafety where draft codes proposed by industry do not meet the statutory requirements for registration.
- The Basic Online Safety Expectations, where eSafety can compel transparency from certain services about how they are meeting the expectations. The requirements are designed to improve providers' safety standards and improve transparency and accountability.

---

[4] https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6680.

[5] Sections 140 and 141 of the Act.

- Complaints-based schemes, which serve as a safety net for Australians when service providers, such as social media platforms, do not adequately address user's reports or calls for help, and are designed to address:
    - Cyberbullying material targeted at Australian children.
    - Non-consensual sharing of intimate images[6] which operates similarly to the United States' *Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act 2025*, also known as the Take it Down Act – which was championed by First Lady Melania Trump. eSafety has a very high success rate in removing harmful material generally and up to 98 per cent in cases of image-based abuse.
    - Cyber-abuse material targeted at and seriously harming Australian adults.
    - Illegal and restricted online content, such as child sexual abuse material and pro-terror material.

Given the examples in the Committee's letter, we will focus on explaining the framework and operation of Australia's Online Content Scheme, as set out in the Act.[7]

2. 'Refused classification' material is considered harmful and unlawful in Australia

All platforms and publishers operating in Australia must comply with Australia's National Classification Scheme (Classification Scheme). The Classification Scheme is a cooperative arrangement between the Australian Government and state and territory governments. It governs how materials within Australia are classified. The federal Minister for Communications and the state and territory Ministers responsible for classification oversee the Scheme, rather than eSafety.

The Classification Scheme is administered by the Classification Board, rather than eSafety. Obligations under the Classification Scheme are additional to any contractual terms (terms)

[6] https://www.congress.gov/bill/119th-congress/senate-bill/146.
[7] See Part 9 of the Act.

between platforms and their end users which platforms may also invoke when independently reviewing and removing content if a user, or content they post, breaches those terms.[8]

The Act links to the Classification Scheme for a range of thresholds, including the power to issue removal notices under the Online Content Scheme. Material that is or would likely be classified as 'refused classification' under the National Classification Scheme[9] translates to 'Class 1 material' for the purposes of the Act. That definition encompasses material that:

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified,
- describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
- promotes, incites or instructs in matters of crime or violence.

To ensure our efforts to minimise harms for Australians are as effective as they can be, eSafety works with other regulators and law enforcement. Perpetrators of terrorist and violent extremist material (content) and activity (conduct), and child sexual abuse material use different jurisdictions to generate, host, display and promote their content.

Similarly, online activity[10] and the online industry[11] are also global. eSafety collaborates with law enforcement, other government agencies, and non-government partners around the world, such as the US National Center for Missing and Exploited Children[12] and INHOPE,[13] the Association of Internet Hotline Providers which supports the rapid identification and removal of child sexual abuse material from the digital world.

---

[8] See for example https://help.x.com/en/rules-and-policies/x-rules, https://transparency.meta.com/en-gb/policies/community-standards/ and https://www.tiktok.com/legal/page/us/terms-of-service/en.
[9] *Classification (Publications, Films and Computer Games) Act 1995* (Cth).
[10] Section 134 of the Act.
[11] Section 135 of the Act.
[12] https://www.missingkids.org.
[13] https://www.inhope.org/EN.

3. eSafety's approach is Australia-focussed and does not require global removal of 'refused classification' material

eSafety's removal notices do not require non-child sexual abuse material Class 1 content to be taken down from the internet globally. It is important to note that eSafety's focus is on minimising the harm to Australians from inadvertent exposure to harmful material, with a focus on children.

By adopting this approach, there is nothing eSafety does that prevents platforms from displaying whatever they want to Americans or any other citizens in other jurisdictions.

eSafety's current approach to responding to illegal and restricted content, particularly Class 1 material, builds on the Federal Court of Australia's guidance on the interpretation and application of the relevant illegal and restricted removal powers in the Act, particularly around what would constitute "removal" for the purposes of the Act.

This was most recently demonstrated through eSafety' acceptance of geo-blocking of graphic video footage of the Charlie Kirk, Iryna Zarutska, and Chandra Mouli Nagamallaiah murders as compliance with a removal notice. In each case, the Classification Board determined certain material containing violent graphic imagery as 'refused classification'. This is the highest possible rating and is given to material that is outside generally accepted community standards. Based on the Classification Board's decisions, eSafety issued removal notices for that and similar material.

Even while video footage of the Charlie Kirk, Iryna Zarutska, and Chandra Mouli Nagamallaiah murders was geo blocked in Australia, the complete video footage remained accessible on social media platforms by users outside Australia.

Platforms have effective technological capability to apply location-based content restrictions which they implement for a range of material on their services. Regulating material outside Australia is a matter for platforms and the local authorities in those locations rather than eSafety.

Removal notices related to child sexual abuse material is the only exception, with eSafety requiring removal of material rather than geo-blocking for compliance purposes. Child sexual

abuse material clearly violates most platforms' terms of service, and is also globally removed by platforms.[14]

Importantly, the Act also states that it does not apply generally to the extent (if any) that it would infringe any Australian constitutional doctrine of implied freedom of political communication.[15]

4. Preventing distribution of 'refused classification' material to Australians does not prevent distribution or display to users in other jurisdictions

Australia regulates material only in our own jurisdiction. Different jurisdictions have different rules about whether, and what kind of, material is prohibited, and have the right to regulate as they see fit for their own circumstances. Material restricted in one jurisdiction does not generally prevent that material from being displayed in another jurisdiction where that material is permitted. That same principle applies to the Online Content Scheme in the Act.

5. Transparency and review mechanisms for platforms and end-users protects rights and provides accountability

eSafety is subject to a range of accountability and transparency measures, including:

- Reporting, governance and compliance arrangements, such as corporate and annual reporting requirements, as well as requests under the *Freedom of Information Act 1982*.
- Internal review of decisions based on formalised processes.
- External reviews by the Administrative Review Tribunal, the Federal Court of Australia and the Commonwealth Ombudsman.
- Parliamentary Hearings before the Australian Parliament.

eSafety also promotes accountability and transparency in our work, including by:

- Publishing regulatory guidance for each of the complaint schemes, as well as broader compliance and enforcement materials.

---

[14] See 18 U.S. Code § 2252.
[15] Section 233 of the Act.

For example, on 16 September, eSafety released its Social Media Minimum Age Regulatory Guidance.[16] In the lead up to commencement Social Media Minimum Age obligation, eSafety consulted widely on regulatory implementation across the Australian community, including with experts and the online service providers industry. The Department's Age Assurance Technology Trial— Final Report,[17] released on 31 August 2025, also informed our regulatory approach.

- Undertaking deep consultation, engaging with a wide variety of stakeholders and pursuing an extensive array of communication and awareness raising initiatives. These are published on our website to promote transparency and accountability of eSafety's work, while also seeking to raise the profile of online safety.

- Participating in inquiry and review processes, both within Parliament and across the federal, state and territory level, and publishing our submissions.

6. External review is important for supporting eSafety's evidence-based impact evaluation of the Social Media Minimum Age obligation

As outlined above, the Social Media Minimum Age obligation commenced on 10 December 2025 and requires age restricted social media platforms to take reasonable steps to ensure Australians under 16 do not have an account on their service.

eSafety has commenced an evidence-based evaluation of the implementation and outcomes of the Social Media Minimum Age obligation. Twelve academic institutions from Australia, the United Kingdom and the United States were selected through a transparent, competitive and independent review process due to their extensive and unique experience in conducting research and evaluation into social media and mental health.

The task of the advisory group, which is made up of researchers from Australia, the United States of America and the United Kingdom is to evaluate Australia's world-first social media delay for children under 16. The advisory group, comprised of a range of world leading experts

[16] https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf.
[17] https://www.infrastructure.gov.au/department/media/publications/age-assurance-technology-trial-final-report.

will examine how the Social Media Minimum Age obligation is being implemented and evaluate its short and medium-term impacts on children, young people, and their parents or caregivers. Data from this evaluation will inform the independent review of the legislation led by the Department, which must occur within 2 years of commencement.

7. eSafety engages with other regulators and online safety experts

To ensure an evidence-based policy, eSafety works with other regulators and experts to ensure evidence-based and best practice policies are developed for Australia. This is standard practice for most areas of regulation, not just online safety. For example, regulators from other disciplines have been working cooperatively and across jurisdictions for decades, including the U.S. Federal Trade Commission (FTC). For instance, the Institute of International Communication was formed in 1969, the Global Privacy Assembly was formed in 1979 and the International Consumer Protection and Enforcement Network was established in 1992. These well-established organisations convene media and communications regulators, data protection and privacy commissioners and consumer and competition authorities, respectively.

Online safety regulation is a much newer domain and in 2022, the formation of the Global Online Safety Regulators Network (GOSRN) was announced. GOSRN has been very transparent about thematic issues and positions discussed at senior officials meetings including putting out statements about online safety regulations compatibility with a range of human rights, including freedom of expression and our commitment to achieving a greater degree of regulatory coherence for tech company compliance.

8. Common online safety approaches in Australia and the United States of America unite rather than divide us

The Australian Parliament has created laws and regulations that closely mirrors both legislation recently passed by the US Congress and efforts made by US government departments and law enforcement agencies concerning the most grievous areas of online harm impacting all of our citizens.

The *Take It Down Act*,[18] passed by Congress last year and championed by First Lady Melania Trump, closely aligns with the image-based abuse scheme in the Act, as described above, where we have a 98% success rate in remediating harm from non-consensual sharing of intimate imagery, including deepfake versions.

Additionally, we understand a number of US states have passed legislation seeking to enhance protection of children online, including California, Florida, Georgia, Louisiana, Maryland, Mississippi, Nebraska. New York, Ohio, Tennessee, Texas, Utah and Virginia.

For the decade since eSafety has been in existence, we have collaborated with the US Department of Justice to address child sexual abuse material and with the Federal Bureau of Investigation on issues of mutual concern, including sexual extortion by overseas organised criminals. In December 2024, eSafety and the Department of Homeland Security held a two-day workshop with US-based AI and technology companies and related stakeholders on jointly creating a Safety by Design Toolkit to Combat Online Child Sexual Exploitation and Abuse.

Finally, we note that the recently-registered industry codes, and transparency notices the eSafety Commissioner has issued to AI companion companies, closely align with the research the FTC is undertaking to explore harms to children around harmful outputs of AI companions. As you would know, the FTC issued orders to seven companies that provide consumer-facing AI-powered chatbots seeking information on how these firms measure, test, and monitor potentially negative impacts of this technology on children and teens, as well as limit or restrict children's or teens' use of these platforms.

[18] https://www.congress.gov/bill/119th-congress/senate-bill/146.