9:33

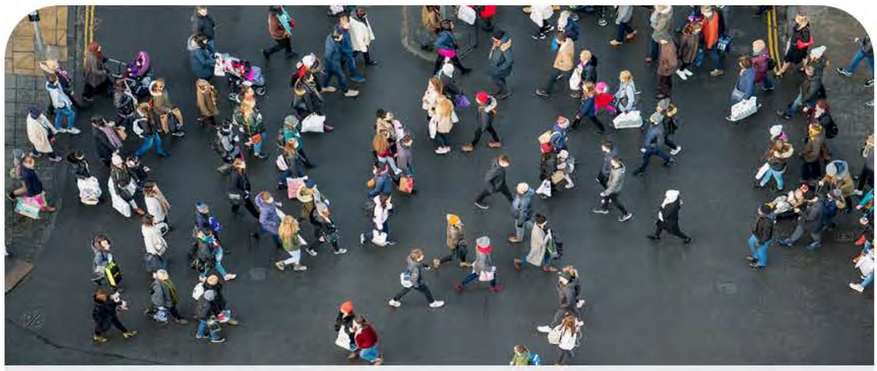
137

TD

Toby

You missed a call, but the caller didn't leave a message.

iMessage
Fri, 25 Aug at 9:58 AM



Global expectations of social media platforms and other sites to safeguard against unlawful data...

oaic.gov.au

It is worth asking s 22 is s 47F checked with us on safety implications here noting the Twitter litigation against CCDH “for scraping data”. How do you hold companies accountable for what’s happening on their platforms if they turn off their data hose or put it out of reach? There has to be a bit more balance or consideration of a range of issues...

Text Message
Tue, 29 Aug at 11:18 AM

iMessage

From: Julie Inman Grant
To: s 22
Cc: Kathryn King; Toby Dagg; s 22
Subject: RE: Correspondence for approval tomorrow [SEC=OFFICIAL]
Date: Wednesday, 31 January 2024 2:35:00 PM
Attachments: image001.png
image002.png
DRAFT Invitations to Green for briefing TD.docx

OFFICIAL

Senator Faruqi letter fine – I have added my signature. Thank you. I offered to extend this briefing to Senators Hanson-Young, Shoebridge and other members of the Green Party who have interest in these issues. I understand there are protocols but I would like to do this briefing once rather than multiple times for the same party. Should we replicate the letter and send to David Coleman and/or Peter Dutton for the Coalition? WA commission letter looking good too. Sorry, having issues inserting the signatures but these are ready to go.

From: s 22 @eSafety.gov.au>
Sent: Monday, January 29, 2024 5:23 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Cc: Kathryn King s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 22 @esafety.gov.au>
Subject: Correspondence for approval tomorrow [SEC=OFFICIAL]

OFFICIAL

Hi Julie

Please see attached and below the outstanding correspondence for your review and approval. Kathryn will also be taking you through them tomorrow in you handover.

1. Letter to Senator Faruqi – I've updated noting your feedback. Attachment A - eSafety Commissioner to Meta re Palestinian accounts.pdf, Attachment B - Letter to eSafety Commissioner re Palestinian content questions November 2023.docx.pdf
2. Invitation to Greens Leader for Standards briefing – inviting the Greens team for a briefing on the Standards.
3. Letter to WA Commissioner for Victims of Crime - in relation to their consultation on provide feedback on the Criminal Law Amendment (Intimate Images) Act 2019 (WA) and proposed responses to their consultation questions.

Reach out if you have any queries.

s 22

From: Julie Inman Grant
To: Toby Dagg; s 22
Subject: https://gizmodo.com.au/2024/02/elon-musks-x-will-give-blue-checks-to-anyone-even-terrorist-leaders/ [SEC=OFFICIAL]
Date: Friday, 16 February 2024 12:35:00 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

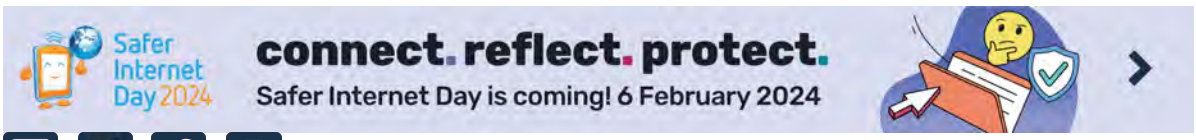
"Several leaders of Hezbollah, a designated terrorist group by the United States, are X Premium customers receiving paid services such as verification, boosted content, and longer posts, according to an investigation from the Tech Transparency Project (TTP) on Wednesday." Didn't X tell us in the online hate notice that X Premium/Blue Tick customers don't get boosted content/algorithms in response to our notice?

Elon Musk's X Will Give Blue Checks to Anyone, Even Terrorist Leaders (gizmodo.com.au)

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

From: Julie Inman Grant
To: s 22 ; DL - eSafety Commissioner and Staff
Subject: Re: Farewell, s 47F
Date: Wednesday, 28 February 2024 5:44:31 PM
Attachments: image001.png
image002.png
image004.png
image005.png
image006.png
image007.png

This all captures s 47F beautifully, s 22 She was my first contact at the Children's eSafety Commissioner when I was at Twitter. Ironically, I think I helped her set up the @esafetyoffice account that we often see "getting feedback" on the platform today.

And, so it all goes full circle!

I will also miss s 47F steady, experienced hands, her beautiful way with words and her always lovely and warm smile! I am grateful to everything she has brought to eSafety!

More than that, I want to wish her all the best in her new professional adventures and know that she will absolutely thrive!!!

All the best s 47F and we know this is farewell, but not goodbye!!!

Julie

Get Outlook for iOS

From: s 22 @esafety.gov.au>
Sent: Wednesday, February 28, 2024 4:26:04 PM
To: DL - eSafety Commissioner and Staff <s 47E(c), s 47F @esafety.gov.au>
Subject: s 47F [SEC=OFFICIAL]

OFFICIAL

Dear colleagues,

It is with mixed emotions that I share the news that s 47F will be leaving eSafety on 15 March.

s 47F is one of our longest-serving members having started at the ACMA in 2011. She played a key role in launching our office in 2015 switching from ACMA's CyberSmart to the Children's eSafety Commissioner. It was a time before we had work laptops and s 47F was solely responsible for ALL of the comms and marketing – including media, social media, eDM and corporate comms.

She has been an integral member of eSafety comms and marketing ever since contributing to 7 x Safer Internet Days , 3 x eSafety conferences, writing countless speeches, dealing with hundreds of media responses and releases, executing many communications and marketing strategies for various parts of the agency and much more.

s 47F calm demeanour, dedication and contributions have left an indelible mark at eSafety and we can all reflect on the positive impact she has had and the countless successes we have achieved together.

We wis s 47F every success as she embarks on the next chapter of her career.

We'd love you to write s 47F message to wish her well! If you would like to make a contribution to a gift, please do so. Please note your participation is entirely optional, and your warm wishes are more than enough.
https://app.grouptogether.com/s 47F farewell

Best
s 22

s 22
Manager, Marketing & Campaigns

s 22

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.

From: Julie Inman Grant
To: Kathryn King; Toby Dagg
Subject: Re: OpenAI and Elon Musk [SEC=UNOFFICIAL]
Date: Wednesday, 6 March 2024 8:12:11 PM

The OpenAI leadership talk about the dangers of open source AI models - and whenever I raise the approach in the DIS standards - people nod in agreement. Even if we are on the wrong side of Elon, we are on the right side of this debate…

Get Outlook for iOS

From: Kathryn King s 47E(c), s 47F @eSafety.gov.au>
Sent: Wednesday, March 6, 2024 7:36:38 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Subject: Re: OpenAI and Elon Musk [SEC=UNOFFICIAL]

I am compelled to use Sora to make this into a movie trailer.

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Wednesday, March 6, 2024 4:23 PM
To: Kathryn King s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Subject: OpenAI and Elon Musk [SEC=UNOFFICIAL]

#AIIntrigue

https://openai.com/blog/openai-elon-musk

Get Outlook for iOS

From: Julie Inman Grant
To: Toby Dagg; Kathryn King; s 22
Subject: CcDH vs X Corp goes to court this week [SEC=UNOFFICIAL]
Date: Wednesday, 6 March 2024 10:06:50 PM

Note purported tactics and representation of CCDH by s 47F
https://counterhate.com/blog/ccdh-prepares-for-court-hearing-after-elon-musk-sues-nonprofit-over-independent-research/

Get Outlook for iOS

From: Julie Inman Grant
To: s 22
Cc: Toby Dagg; s 22 s 47E(d) ; s 22
Subject: RE: Decision memo - consulting X Corp. on correction to BOSE report [SEC=OFFICIAL:Sensitive]
Date: Friday, 8 March 2024 10:57:00 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL: Sensitive

I agree to eSafety publishing X Corp's direction and publishing on our website. I'm happy for my signature to be added.

s 47E(d)

Thank you.

From: s 22 @eSafety.gov.au>
Sent: Friday, March 8, 2024 8:46 AM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Cc: Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; s 47E(d) @esafety.gov.au>; s 22 s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>
Subject: RE: Decision memo - consulting X Corp. on correction to BOSE report [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi Julie,

s 47E(d)

Let us know if you have any questions. Thanks

s 22

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Friday, February 9, 2024 4:31 PM
To: s 22 @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Cc: s 22 @eSafety.gov.au>; DL - eSafety BOSE s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22 s 22 @eSafety.gov.au>; s 22 s 22 @esafety.gov.au>
Subject: RE: Decision memo - consulting X Corp. on correction to BOSE report [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

s 47E(d)

From: s 22 @eSafety.gov.au>
Sent: Friday, February 9, 2024 1:09 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Cc: s 22 @eSafety.gov.au>; DL - eSafety BOSE s 47E(d) @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22 s 22 @eSafety.gov.au>; s 22 s 22 @esafety.gov.au>
Subject: RE: Decision memo - consulting X Corp. on correction to BOSE report [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi Julie,

s 47E(d)

s 47E(d)

Thanks

s 22

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Thursday, February 1, 2024 4:41 PM
To: s 22 @eSafety.gov.au>; Toby Dag s 47E(c), s 47F @esafety.gov.au>
Cc: s 22 @eSafety.gov.au>; DL - eSafety BOSE
s 47E(d) @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22
s 22 @eSafety.gov.au>; s 22
s 22 @esafety.gov.au>
Subject: RE: Decision memo - consulting X Corp. on correction to BOSE report [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Team: Here is the signed decision memo with me agreeing to both the consultation and publication, in the interest of fairness, accuracy and due diligence. Julie

---

From: s 22 @eSafety.gov.au>
Sent: Thursday, February 1, 2024 1:59 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Toby Dag s 47E(c), s 47F @esafety.gov.au>
Cc: s 22 @eSafety.gov.au>; DL - eSafety BOSE
s 47E(d) @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22
s 22 @eSafety.gov.au>; s 22
s 22 @esafety.gov.au>
Subject: Decision memo - consulting X Corp. on correction to BOSE report [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Julie,

s 47E(d)

s 47E(d)

[redacted]

Thanks to s 22 and Legal for reviewing, and to s 22 for drafting the above. This does not need an urgent response.

Thanks

s 22

s 22
Manager, Basic Online Safety Expectations
Industry Regulation and Legal Services
s 22

Australian Government | eSafetyCommissioner

esafety.gov.au

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, present and emerging.

From: Julie Inman Grant
To: Kathryn King; Toby Dagg; s 22
Subject: BOSE data mention: WSJ New Era of AI Deepfakes [SEC=UNOFFICIAL]
Date: Saturday, 9 March 2024 12:12:27 PM

Note the numbers on X cuts to trust and safety. Perhaps these WSJ journos listed below would be interested in next set of BOSE notices - or the final report, s 22 We can add them to the list.

TECHNOLOGY

New Era of AI Deepfakes Complicates 2024 Elections

Deceptive videos, audio and images are more sophisticated, easier to make as tech industry wrestles with how to keep up

Follow the WSJ in Apple News

The explosion of artificial-intelligence technology makes it easier than ever to deceive people on the internet, and is turning the 2024 U.S. presidential election into an unprecedented test on how to police deceptive content.

An early salvo was fired last month in New Hampshire. Days before the state's presidential primary, an estimated 5,000 to 25,000 calls went out telling recipients not to bother voting.

"Your vote makes a difference in November, not this Tuesday," the voice said. It sounded like President Biden, but it was created by AI, according to an analysis by security firm Pindrop. The message also discouraged independent voters from participating in the Republican primary.

On social media, however, the call's origin was up for debate. On Meta Platforms' Threads app, some users saw an attempt to suppress voter turnout. "This IS election interference," wrote one. On former President Donald Trump's site Truth Social, some users blamed Democrats for the call. "Probably not fake," one posted.

When Pindrop analyzed the audio, they found telltale signs the call was phony. The Biden voice pronounced the noisy fricative sounds that make up the letters S and F, for example, in a very unhuman way.

Two weeks later, the New Hampshire attorney general's office said it identified a Texas-based company named Life Corp. as the source of the

calls and that it issued a cease-and-desist order citing law against voter suppression. Representatives for Life Corp. didn't respond to emails seeking comment.

Thanks to recent advances in generative AI, virtually anyone can create increasingly convincing but fake images, audio and videos, as well as fictional social-media users and bots that appear human. With a busy year for elections worldwide in 2024, voters are already running into AI-powered falsehoods that risk confusing them, according to researchers and U.S. officials.

The proliferation of AI fakes also comes as social-media companies are trying to avoid having to adjudicate thorny content issues around U.S. politics. Platforms also say they want to respect free-speech considerations.

Around 70 countries estimated to cover nearly half the world's population—roughly four billion people—are set to hold national elections this year, according to the International Foundation for Electoral Systems.

While AI makers and social-media platforms often have policies against using AI in deceptive ways or misleading people about how to vote, how well those companies can enforce those rules is uncertain.

OpenAI Chief Executive Sam Altman said at a Bloomberg event in January during the World Economic Forum's annual meeting in Davos, Switzerland, that while OpenAI is preparing safeguards, he's still wary about how his company's tech might be used in elections. "We're going to have to watch this incredibly closely this year," Altman said.

OpenAI says it is taking a number of measures to prepare for elections, including prohibiting the use of its tools for political campaigning; encoding details about the provenance of images generated by its Dall-E tool; and addressing questions about how and where to vote in the U.S. with a link to CanIVote.org, operated by the National Association of Secretaries of State.

In early February, the oversight board of Facebook parent Meta Platforms called the platform's rules around doctored content incoherent, after reviewing an incident last year in which Facebook didn't remove an altered video of Biden.

The board, an outside body created by the company, found that Facebook abided by existing policy, but said the platform should act quickly to clarify its policy around manipulated content before upcoming elections. A Meta spokesman said the company was reviewing the board's guidance and would

respond within 60 days.

Meta says its plan for elections in 2024 is largely consistent with previous years. For example, it will prohibit new political ads in the final week before the U.S.'s November contest. Meta also labels photorealistic images created using its AI feature.

People who've studied elections debate how much an AI deepfake could actually sway someone's vote, especially in America where most people say they've likely already decided who they'll support for president. Yet the very possibility of AI-generated fakes could also muddy the waters in a different way by leading people to question even real images and recordings.

Claims about AI are being used to "discredit things people don't want to believe"—for example, legitimate video shot around the Oct. 7 Hamas attacks on Israel, said Renée DiResta, research manager at the Stanford Internet Observatory.

Social-media giants have been struggling for years with questions around political content. In 2020, they went to aggressive lengths to police political discourse, partly in response to reports of Russian interference in the U.S. election four years earlier.

Now, they're easing up on some counts, particularly at Elon Musk's X.

Since his 2022 acquisition of Twitter, Musk has renamed the site and rolled back many of its previous restrictions in the name of free speech. X has reinstated many previously suspended accounts and began selling verified check marks previously designed for notable figures. X also cut over 1,200 trust and safety workers, according to figures it disclosed to an Australian online safety regulator last year, part of widespread layoffs Musk said were needed to stabilize the company's financial situation.

More recently, X has said it was hiring more safety staffers, including some 100 content moderators who will work in Austin, Texas, and other positions globally.

YouTube said it stopped removing videos claiming widespread fraud occurred in the 2020 and other past U.S. elections, citing concerns about curtailing political speech. Meta took a similar stance when deciding to allow political ads to question the legitimacy of Biden's 2020 victory.

Meta also let go many employees who were working on election policy during broader layoffs starting in late 2022, though the company says its overall trust

and safety efforts have expanded.

X, Meta and YouTube all have reinstated Trump after banning him following the Jan. 6, 2021, attack on the U.S. Capitol, citing reasons including that the public should be able to hear what candidates are saying. Trump has repeatedly made the false claim that he won the 2020 election or that it was "rigged."

Katie Harbath, a former Facebook public-policy director, said she thinks platforms have gotten exhausted trying to adjudicate issues around political content. There's no clear agreement around exactly what the rules and penalties should be, she added.

"A lot of them have been more like, 'It's probably better for us to be as hands-off as possible,'" Harbath said.

The companies say they remain committed to fighting deceptive content and helping users get trustworthy information about how and where to vote. X says its efforts include bolstering its fact-checking feature Community Notes, which relies on volunteers to add context to posts.

Critics, including Musk and many conservatives, have assailed steps that social-media giants took to manage political content around 2020, particularly Twitter. They have pointed, for example, to an episode shortly before the November 2020 vote, when Twitter temporarily blocked links to New York Post articles about Hunter Biden, son of now-President Biden.

(The Post and The Wall Street Journal are both owned by News Corp.)

Twitter executives later conceded they had overstepped but said they had acted out of concern around possibly hacked materials, not due to political leanings.

Other changes this election cycle have come out of a lawsuit led by the Republican attorneys general of Missouri and Louisiana, who allege that Biden administration officials policed social-media posts in ways that amounted to unconstitutional censorship. Lower courts issued rulings imposing limits on how the federal government could communicate with social-media platforms, though the Supreme Court later put those decisions on hold. The case is now pending before the Supreme Court. Congressional Republicans also have been investigating anti-disinformation efforts.

How should social-media companies deal with AI-generated, fake content? Join the conversation below.

To comment, you'll need to be on WSJ.com

" We're having some interaction with social-media companies, but all of those interactions have changed fundamentally in the wake of the court's ruling," Federal Bureau of Investigation Director Christopher Wray said during a Senate hearing in October. He said the agency was acting "out of an abundance of caution."

Democratic officials and disinformation researchers say such communications are critical for combating nefarious online activity, including foreign influence efforts.

Federal authorities say they're on alert. So far, the U.S. hasn't detected a major foreign-backed interference operation targeting the 2024 election, according to senior intelligence officials.

Gen. Paul Nakasone, the recently retired chief of U.S. Cyber Command and the National Security Agency, vowed before stepping down that the 2024 U.S. election would be "the most secure election we've had to date" from foreign interference. "If this isn't necessarily going to work in the same methodology it did in '22 or '20," he added, "then we've got to find new ways to do it."

— *Jack Gillum contributed to this article.*

Write to Robert McMillan at robert.mcmillan@wsj.com, Alexa Corse at alexa.corse@wsj.com and Dustin Volz at dustin.volz@wsj.com

From: Julie Inman Grant
To: s 22 ; Toby Dagg; Kathryn King; s 22
Subject: NOCS Advisory Committee Presentation [SEC=OFFICIAL]
Date: Monday, 11 March 2024 3:13:00 PM
Attachments: 231213_Letter to US Senate Judiciary Committee_Big tech and child online safety FINAL.docx
image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

OFFICIAL

Noting Toby and I have this presentation to the NOCs Child Safety Advisory Committee on Thursday, as suggested by the Attorney General (it is 45 minutes) s 47C

https://www.childsafety.gov.au/resources/national-strategy-advisory-group-membership-list

Discord[1]

- Professional trust and safety staff at Discord are not automatically notified when volunteer moderators or administrators take action against CSEA. (This increases the risk of offenders continuing to abuse and re-victimise children on other parts of the service).
- Does not use tools to detect CSEA in live video/livestreams, stating it is 'prohibitively expensive'.
- Does not have an option for users to report CSEA in livestreams except for the ability for a user to report chat messages accompanying a livestream or navigating to a separate webform.
- Does not use hash matching tools to detect known CSEA videos in direct messages, and public or private servers.

X/Twitter[2]

- Only have content moderators operating by default in 12 languages. This is in comparison with over 70 languages that Google and TikTok reported that they cover.
- For the three months after X/Twitter's change in ownership, the proactive detection of CSEA fell from 90% to 75%. X/Twitter states that this has since improved.
- Does not use hash matching tools to scan for known CSEA videos on direct messages.
- Does not use tools to detect new, or 'previously unknown' CSEA material in direct messages.
- Does not use language analysis technology to detect likely grooming in tweets or direct messages, nor to detect other CSEA activity such as sexual extortion or the trading and sale of CSEA on direct messages.
- Does not have an option for users to report CSEA in-service in direct messages. The user must navigate to a separate webform.

Snap[3]

- Does not use tools to detect new, or 'previously unknown' CSEA material in Snaps, direct chat, Discover or Spotlight.
- Does not use language analysis technology to detect likely grooming in Snaps or direct chat.
- Only uses several different indicators to detect repeat offenders (recidivism) by default, reserving additional indicators for cases requiring 'deeper investigation'

Meta[4]

- If a user is banned on Facebook for CSEA, information is not always shared with Instagram, and vice versa, in order to prevent the account from operating on the other service. Meta reported that WhatsApp information on CSEA is not shared with either Facebook or Instagram.
- There are no CSEA specific reporting options on WhatsApp.

TikTok[5]

- When technology flags content or activity in direct messages as potentially involving grooming, these are not

reviewed by human moderators in order to verify and take appropriate action.

Apple[6]

- Does not use hash matching tools to detect known CSEA images or video on iMessage or iCloud.
- Does not use tools to detect CSEA in live video/livestreams on FaceTime.
- Does not use language analysis technology to detect likely grooming in iMessage.
- Does not have an option for users to report CSEA in-service in direct messages. The user must report via the abuse@apple.com email address or via Apple support.

Microsoft/Skype[7]

- Microsoft Teams, Skype and OneDrive take a median time of 2 days to respond to user reports of CSEA, and up to 19 days for cases requiring re-review. This is the longest of any services covered by eSafety's notices.
- Does not use hash matching tools to scan for known CSEA images on OneDrive content that is stored, but not shared. Content is scanned only when it is shared.
- Does not use tools to detect CSEA in live video/livestreams on Microsoft Teams or Skype.

Google[8]

- Does not block URLs to known CSEA on YouTube, Drive, Meet, Chat, Google Photos, Google Messages, Gmail or Blogger.
- Despite making its technology CSAI Match available to other services, Google does not use it to detect known CSEA videos on Gmail, Messages and Chat.
- Although it uses its own technology, Google Content Safety API, to scan for new images on its consumer version of Drive (content stored and shared content), Google Photos, YouTube and Blogger, it does not use it on Google Messages or Gmail.
- Does not use language analysis technology to detect likely grooming or other CSEA activity such as sexual extortion in Meet, Chat, Google Messages or Gmail.
- Does not have an option for users to report CSEA in-service in Gmail or Google Messages. The user must navigate to a separate webform.
- Uses a minimal number of indicators to detect repeat offenders (recidivism).

Twitch[9]

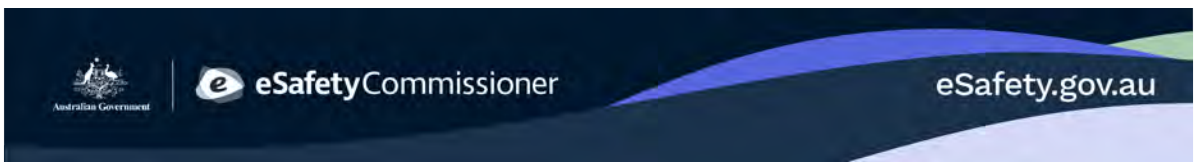
- Professional trust and safety staff at Twitch are not automatically notified when volunteer moderators or channel creator/streamers take action against CSEA. (This increases the risk of offenders continuing to abuse and re-victimise children on other parts of the service).
- Users who are not signed in to an account are not able to report in-service. Users must email Twitch support or contact the Twitch Support Twitter account.
- Only have content moderators operating by default in 24 languages. This is in comparison with over 70 languages that Google and TikTok reported that they cover.

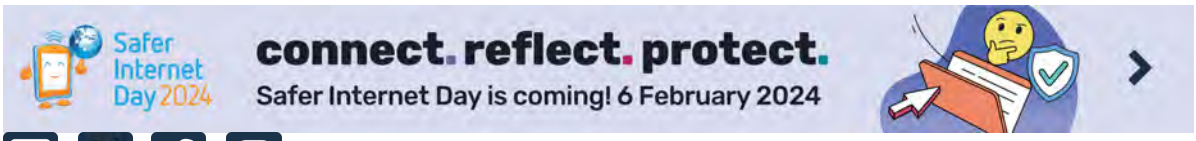
eSafety will continue using its powers to lift the lid on industry's systems and processes, and hold industry accountable, while working alongside another of our systemic regulatory powers - the industry codes and standards.

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

---

[1] The Notice to Discord covered the period 24 January 2022 to 31 January 2023

[2] The Notice to X/Twitter covered the period 24 January 2022 to 31 January 2023

[3] The Notice to Snap covered the period 24 January 2022 to 31 July 2022

[4] The Notices to Meta and WhatsApp covered the period 24 January 2022 to 31 July 2022

[5] The Notice to TikTok covered the period 24 January 2022 to 31 January 2023

[6] The Notice to Apple covered the period 24 January 2022 to 31 July 2022

[7] The Notices to Microsoft and Skype covered the period 24 January 2022 to 31 July 2022

[8] The Notice to Google covered the period 24 January 2022 to 31 January 2023

[9] The Notice to Twitch covered the period 24 January 2022 to 31 January 2023

Australian Government | eSafetyCommissioner

Wednesday, 13 December 2023

The Hon. Dick Durbin *D-IL*
Chairman Senate Judiciary Committee

Cc: Arya Hariharan , Chief Oversight Counsel for the House Judiciary Committee

Commented [JIG1]: This is the Senate Judiciary Committee. Please cc s 47F @judiciary.senate.gov is my best guess bu s 22 and I met with her last November so may have it...

The Hon. Lindsay Graham *R-SC*
Ranking Member
US Senate Committee on the Judiciary

Cc: Corey Becker, Chief Counsel for Crime and National Security for Senate Judiciary ranking member Lindsey Graham

Dear Senators Durbin & Graham ,

My name is Julie Inman Grant, and I am Australia's eSafety Commissioner. I am writing about your upcoming hearing with CEOs of Meta, X, TikTok, Snap, and Discord and to offer our eight years of regulatory insights, experiences, and findings around tech platform safety , in the hopes that it might be useful to your Congressional deliberations.

Australia's eSafety Commissioner

Established in 2015, we are the independent regulator for online safety and also serve as Australia's hotline for online child sexual abuse material , operate a legislated youth cyberbullying and image-based abuse scheme, and use broad systemic powers to increase platform transparency and accountability and shift responsibility back on the platforms through safety by design .

Mandatory Codes and Basic Online Safety Expectations (BOSE) Transparency Powers

Under our BOSE transparency compulsion powers, we have issued notices to 12 tech companies , covering 27 services, we found that none of the major technology companies were doing enough to combat illegal and seriously harmful content on their platforms . We found significant inconsistencies in the timeliness of responses to reports of child sexual abuse as well as the protections in place to prevent the livestreaming of child sexual abuse. In short, not one of the signatory companies have lived up to the commitments made through the Five Country Ministerial's Voluntary Principles to Combat Child Sexual Abuse.

Where platforms failed to respond to our transparency notices , we have taken enforcement action .

More detailed findings on Meta, X, TikTok, Snap, and Discord from our Basic Online Safety Expectations transparency reports is in Appendix 1.

It is worth noting that Australia will implement five legally enforceable codes coming into effect in December, 2023 which apply to social media services , ISPs, equipment providers, app distributors and

hosting services . These codes will require companies covered by the codes to take proactive measures to reduce the risk of child sexual abuse material, pro - terror material and other illegal material online . A sixth mandatory code covering s earch engine s commences in March 2024 and will cover both real and synthetic CSAM and pro - terror material created by generative AI . I declined to register two industry codes covering re levant electronic services and d esignat ed internet services as they did not meet appropriate community standards and my office is developing stringent draft industry standards , currently under consultation .

A bipartisan commitment

Online safety has always been a bipartisan issue in the Australian context, and we are providing these safeguards to our citizens in a way that not only preserves but promotes greater freedom of expression and recognises and strives to balance the compleme ntary imperatives of privacy and safety.

We are pleased that you are providing greater scrutiny on these important issues. We do believe that if the U.S. takes tangible and meaningful action that this will be a game changer for technology consumers everywh ere. You may also know that we have officially joined forces through the Australia – United States Joint Council on Combatting Online Child Sexual Exploitation and our continued efforts will be on - going.

We at the eSafety Commissioner stand ready to make ourselves available to share our experiences, insights and how we are negotiating responses from the sector.

Should you wish to discuss these matters in more detail, I would be happy to arrange a meeting, or to address the Committee directly.

Wishing you much success with the hearing and legislative program for 2024.

Sincerely,

Julie Inman Grant

eSafety Commissioner

Encl:

- Key findings: Basic Online Safety Expectations Industry responses to mandatory transparency notices October 2023
- Basic Online Safety Expectations: Summary of industry responses to the first mandatory transparency notice December 2022
- Summary of the Industry Codes and Standards

- Press Release on eSafety Standards Consultation

Appendix 1 – Basic Online Safety Expectations transparency reports including detailed findings on Meta, X, TikTok, Snap, Discord and other services.

The Online Safety Act 2021 gives the eSafety Commissioner (eSafety) a broad remit and functions to address online safety in a multifaceted and holistic way. This mandate includes new powers to require greater transparency and accountability from Big Tech to prevent and respond to child sexual exploitation online.

Basic Online Safety Expectations

The Basic Online Safety Expectations (The Expectations) outline the Australian Government's expectations that social media, messaging and gaming service providers and other apps and websites will take reasonable steps to keep Australians safe.

Under the Online Safety Act, eSafety can require online service providers to report on how they are meeting any or all of the Expectations. The obligation to respond to a reporting requirement is enforceable and backed by civil penalties and other mechanisms. eSafety can also publish statements about the extent to which services are meeting the Expectations.

Since the establishment of the Expectations, the Commissioner has issued two rounds of notices (or 'transparency notices') focused on child sexual exploitation and abuse (**CSEA**). These first set of transparency notices were issued to Apple, Meta (and WhatsApp), Microsoft (and Skype), Omegle, and Snap on 29 August 2022. The second set were issued on 22 February 2023 to Google, Twitter (subsequently rebranded as X), TikTok, Twitch and Discord.

Providers were asked specific questions about the tools, policies and processes they are using to address various forms of CSEA, such as the proliferation of online CSEA material, including the online grooming of children, the use of video calling services to provide live feeds of child abuse, the sexual extortion of children and what they are doing to avoid the risk of amplifying harmful content through recommender systems.

Enclosed is a copy of the two transparency reports published in response to these notices. Some of the key findings include:

Discord [1]

- Professional trust and safety staff at Discord are not automatically notified when volunteer moderators or administrators take action against CSEA. (This increases the risk of offenders continuing to abuse and re-victimise children on other parts of the service).
- Does not use tools to detect CSEA in live video/livestreams, stating it is 'prohibitively expensive'.
- Does not have an option for users to report CSEA in livestreams except for the ability for a user to report chat messages accompanying a livestream or navigating to a separate webform.
- Does not use hash matching tools to detect known CSEA videos in direct messages, and public or private servers.

X/Twitter [2]

- Only have content moderators operating by default in 12 languages. This is in comparison with over 70 languages that Google and TikTok reported that they cover.
- For the three months after X/Twitter's change in ownership, the proactive detection of CSEA fell from 90% to 75%. X/Twitter states that this has since improved.
- Does not use hash matching tools to scan for known CSEA videos on direct messages.
- Does not use tools to detect new, or 'previously unknown' CSEA material in direct messages.
- Does not use language analysis technology to detect likely grooming in tweets or direct messages, nor to detect other CSEA activity such as sexual extortion or the trading and sale of CSEA on direct messages.
- Does not have an option for users to report CSEA in-service in direct messages. The user must navigate to a separate webform.

Snap [3]

- Does not use tools to detect new, or 'previously unknown' CSEA material in Snaps, direct chat, Discover or Spotlight.
- Does not use language analysis technology to detect likely grooming in Snaps or direct chat.

---

[1] The Notice to Discord covered the period 24 January 2022 to 31 January 2023
[2] The Notice to X/Twitter covered the period 24 January 2022 to 31 January 2023
[3] The Notice to Snap covered the period 24 January 2022 to 31 July 2022

- Only uses several different indicators to detect repeat offenders (recidivism) by default, reserving additional indicators for cases requiring 'deeper investigation'

Meta [4]

- If a user is banned on Facebook for CSEA, information is not always shared with Instagram, and vice versa, in order to prevent the account from operating on the other service. Meta reported that WhatsApp information on CSEA is not shared with either Facebook or Instagram.
- There are no CSEA specific reporting options on WhatsApp.

TikTok [5]

- When technology flags content or activity in direct messages as potentially involving grooming, these are not reviewed by human moderators in order to verify and take appropriate action.

Apple [6]

- Does not use hash matching tools to detect known CSEA images or video on iMessage or iCloud.
- Does not use tools to detect CSEA in live video/livestreams on FaceTime.
- Does not use language analysis technology to detect likely grooming in iMessage.
- Does not have an option for users to report CSEA in-service in direct messages. The user must report via the abuse@apple.com email address or via Apple support.

Microsoft/Skype [7]

- Microsoft Teams, Skype and OneDrive take a median time of 2 days to respond to user reports of CSEA, and up to 19 days for cases requiring re-review. This is the longest of any services covered by eSafety's notices.
- Does not use hash matching tools to scan for known CSEA images on OneDrive content that is stored, but not shared. Content is scanned only when it is shared.
- Does not use tools to detect CSEA in live video/livestreams on Microsoft Teams or Skype.

---

[4] The Notices to Meta and WhatsApp covered the period 24 January 2022 to 31 July 2022
[5] The Notice to TikTok covered the period 24 January 2022 to 31 January 2023
[6] The Notice to Apple covered the period 24 January 2022 to 31 July 2022
[7] The Notices to Microsoft and Skype covered the period 24 January 2022 to 31 July 2022

Google [8]

- Does not block URLs to known CSEA on YouTube, Drive, Meet, Chat, Google Photos, Google Messages, Gmail or Blogger.
- Despite making its technology CSAI Match available to other services, Google does not use it to detect known CSEA videos on Gmail, Messages and Chat.
- Although it uses its own technology, Google Content Safety API, to scan for new images on its consumer version of Drive (content stored and shared content), Google Photos, YouTube and Blogger, it does not use it on Google Messages or Gmail.
- Does not use language analysis technology to detect likely grooming or other CSEA activity such as sexual extortion in Meet, Chat, Google Messages or Gmail.
- Does not have an option for users to report CSEA in-service in Gmail or Google Messages. The user must navigate to a separate webform.
- Uses a minimal number of indicators to detect repeat offenders (recidivism).

Twitch [9]

- Professional trust and safety staff at Twitch are not automatically notified when volunteer moderators or channel creator/streamers take action against CSEA. (This increases the risk of offenders continuing to abuse and re-victimise children on other parts of the service).
- Users who are not signed in to an account are not able to report in-service. Users must email Twitch support or contact the Twitch Support Twitter account.
- Only have content moderators operating by default in 24 languages. This is in comparison with over 70 languages that Google and TikTok reported that they cover.

eSafety will continue using its powers to lift the lid on industry's systems and processes, and hold industry accountable, while working alongside another of our systemic regulatory powers - the industry codes and standards.

---

[8] The Notice to Google covered the period 24 January 2022 to 31 January 2023
[9] The Notice to Twitch covered the period 24 January 2022 to 31 January 2023

Appendix 2: Enforceable Industry Codes and Standards

Industry codes and standards

The Online Safety Act also provides for industry associations to develop mandatory industry codes for eight sectors of the online industry, and for eSafety to register the codes if they meet statutory requirements. Six codes have been registered and from 16 December 2023, there are enforceable requirements on social media, ISPs, equipment providers, app stores and hosting services. A sixth code that applies to search engines will come into effect in March 2024.

Under these codes, service providers are required to take a suite of measures including in the case of social media services, the detection and removal of unlawful online material, such as videos showing the sexual abuse of children or pro-terror material.

Two draft industry codes did not provide appropriate community safeguards – one for Relevant Electronic Services (which cover a range of messaging services as well as online dating services and gaming), and one for Designated Internet Services (which includes file and photo storage services). As a result, eSafety has drafted mandatory standards for these industry sections and released these for public consultation on 20 November 2023. Once registered, the industry standards will operate alongside the new mandatory industry codes giving eSafety the ability to enforce these requirements, including through court proceedings.

A second set of codes and standards will be developed to ensure industry minimise the risk of children's exposure to restricted content, such as online pornography.

As a global community, it is imperative that we set and enforce expectations of the technology industry to prevent and respond to child sexual exploitation and abuse. We therefore welcome the bipartisan actions of the Senate Judicial Committee in calling on greater transparency and accountability for Big Tech.

From: Julie Inman Grant
To: s 47F
Cc: s 47F Toby Dagg; s 22
Subject: Australian eSafety Commissioner issues 6 transparency notices around how major companies are preventing and minimising TVEC on their platforms [SEC=OFFICIAL]
Date: Monday, 18 March 2024 10:40:00 PM
Attachments: Media release TVEC Notices.docx
image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

Dear s 47F

We read over the weekend with great interest the DSA notices you sent out around generative AI. Congratulations!

We also hosted Commissioner Johansson and Ambassador Visentin in our Sydney offices and the Ambassador asked us to keep a placeholder for Roberto Viola's digital partnership visit, which we will gladly do.

I am writing to advise that I have given transparency notices under Australia's Online Safety Act to Meta, WhatsApp, Google, Reddit, X Corp, and Telegram requiring these companies to report on how they are preventing and minimising terrorism and violent extremism on their services. The press release will be under embargo for the next couple of hours.

The notices require the companies to explain how they are meeting the Australian Government's Basic Online Safety Expectations, and aim to provide transparency on the systems, tools, processes, and resources that may be used by platforms to tackle terrorist and violent extremism on their services.

We are asking questions about features we know are exploited by bad actors like livestreaming, file storage, algorithms and recommender systems. For relevant services, we are also asking about their generative AI features, which we know terrorists and violent extremists are looking at how they can exploit.

For many years, governments and civil society have called on the online industry to take greater steps to counter online radicalisation and the weaponization of the internet by terrorists and violent extremists. Terrorist attacks in Christchurch, Buffalo, Halle and elsewhere demonstrate the tragic consequences when violent extremists are able to exploit online services to radicalise, incite, and glorify acts of mass violence. Five years on from the Christchurch attack, eSafety continues to receive reports about recordings of abhorrent footage from this and other attacks being shared on mainstream platforms.

The tech companies that provide these services have a responsibility to ensure that their products cannot be used to perpetrate such harm. However, to date there has been a lack of transparency about the tangible measures the online industry is taking to address TVE and a lack of accountability for any gaps.

Industry, governments and civil society spent years developing the Voluntary Transparency Reporting Framework through the OECD to provide a consensus baseline of transparency. Two years on, only two companies, Discord and Mega, have reported, and some of the companies who have received notices do not even publish their own transparency reports.

It is clear that relying on companies to voluntarily report on the steps they are taking is not working. Where industry participants are not providing transparency, we are looking to fill the gaps, compel answers, and hold industry to account. Our questions deliberately build on those agreed through the OECD process.

Reddit and Telegram are also required to answer questions about the measures they have in place to detect and remove child sexual exploitation and abuse (CSEA). Neither have been required by eSafety to report on this harm previously.

As we have done with previous notices on CSEA and online hate, eSafety will publish a transparency report summarising the information and insights we obtain through this process. You can find our previous reports here, which we have seen some companies – although not all – respond to by making key improvements. We will continue to use these powers, alongside our powers to enforce obligations in six industry mandatory Codes now in force, as well as two forthcoming Standards, to ensure industry live up to their responsibility and put in place appropriate safeguards.

Please contact s 22 Executive Manager of Industry Regulation and Legal Services (s 22 @eSafety.gov.au) should you have any questions.

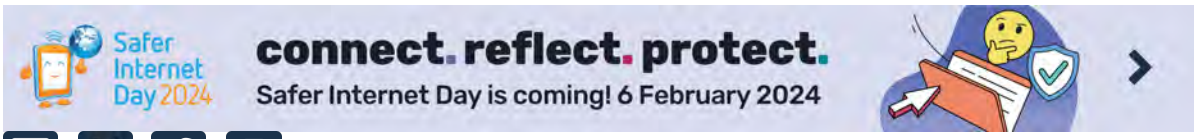
Yours sincerely,

Julie

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

Media release EMBARGOED UNTIL 12.01am AEST 19 MARCH

Tech companies grilled on how they are tackling terror and violent extremism

Australia's eSafety Commissioner has issued legal notices to Google, Meta, Twitter/X, WhatsApp, Telegram and Reddit requiring each company to report on steps they are taking to protect Australians from terrorist and violent extremist material and activity.

The spread of this material and its role in online radicalisation remains a concern both in Australia and internationally, with 2019 terrorist attacks in Christchurch NZ and Halle Germany, and more recently Buffalo NY, underscoring how social media and other online services can be exploited by violent extremists, leading to radicalisation and threats to public safety.

The online safety regulator issued the notices under transparency powers granted under the Online Safety Act, which will require the six companies to answer a series of detailed questions about how they are tackling the issue.

eSafety Commissioner Julie Inman Grant said eSafety continues to receive reports about perpetrator-produced material from terror attacks, including the 2019 terrorist attack in Christchurch, that are reshared on mainstream platforms.

"We remain concerned about how extremists weaponise technology like live-streaming, algorithms and recommender systems and other features to promote or share this hugely harmful material," Ms Inman Grant said.

"We are also concerned by reports that terrorists and violent extremists are moving to capitalise on the emergence of generative AI and are experimenting with ways this new technology can be misused to cause harm.

"Earlier this month the UN-backed Tech against Terrorism reported that it had identified users of an Islamic State forum comparing the attributes of Google's Gemini, ChatGPT, and Microsoft's Copilot.

"The tech companies that provide these services have a responsibility to ensure that these features and their services cannot be exploited to perpetrate such harm and that's why we are sending these notices to get a look under the hood at what they are and are not doing."

According to a recent OECD report, Telegram is the number one ranked mainstream platform when it comes to the prevalence of terrorist and violent extremist material, with Google's YouTube ranked second and Twitter/X coming in third. The Meta-owned Facebook and Instagram round out the top five placing fourth and fifth respectively.

WhatsApp is ranked 8th while reports have confirmed the Buffalo shooter's 'manifesto' cited Reddit as the service that played a role in his radicalisation towards violent white supremacist extremism.

"It's no coincidence we have chosen these companies to send notices to as there is evidence that their services are exploited by terrorists and violent extremists. We want to know why this is and what they are doing to tackle the issue," Ms Inman Grant said.

“Transparency and accountability are essential for ensuring the online industry is meeting the community’s expectations by protecting their users from these harms. Also, understanding proactive steps being taken by platforms to effectively combat TVEC is in the public and national interest.

“That’s why transparency is a key pillar of the Global Internet Forum to Counter Terrorism and the Christchurch Call, global initiatives that many of these companies are signed up to. And yet we do not know the answer to many of these basic questions.

“And, disappointingly, none of these companies have chosen to provide this information through the existing voluntary framework – developed in conjunction with industry – provided by the OECD. This shows why regulation, and mandatory notices, are needed to truly understand the true scope of challenges, and opportunities.”

As part of these notices, eSafety will also be asking Telegram and Reddit about measures they have in place to detect and remove child sexual exploitation and abuse.

The six companies will have 49 days to provide responses to the eSafety Commissioner.

For more information or to arrange an interview, please phone 0439 519 684 or email media@esafety.gov.au

From: Julie Inman Grant
To: s 47F @ec.europa.eu; s 47F
Cc: Toby Dagg; s 22
Subject: Australian eSafety Commissioner issues 6 transparency notices around how major companies are preventing and minimising TVEC on their platforms [SEC=OFFICIAL]
Date: Monday, 18 March 2024 10:40:00 PM
Attachments: Media release TVEC Notices.docx
image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

Dear DG-Home Colleagues:

We had the distinct pleasure of hosting Commissioner Johansson, Ambassador Visentin and team today in our Sydney offices. Per usual, it was a very productive and enlightening discussion and our efforts around combatting both CSAM and TVEC could not be more aligned. This press release will be under embargo for the next couple of hours.

To that end, I would like to advise that I have given transparency notices under Australia's Online Safety Act to Meta, WhatsApp, Google, Reddit, X Corp, and Telegram requiring these companies to report on how they are preventing and minimising terrorism and violent extremism on their services.

The notices require the companies to explain how they are meeting the Australian Government's Basic Online Safety Expectations, and aim to provide transparency on the systems, tools, processes, and resources that may be used by platforms to tackle terrorist and violent extremism on their services.

We are asking questions about features we know are exploited by bad actors like livestreaming, file storage, algorithms and recommender systems. For relevant services, we are also asking about their generative AI features, which we know terrorists and violent extremists are looking at how they can exploit.

For many years, governments and civil society have called on the online industry to take greater steps to counter online radicalisation and the weaponization of the internet by terrorists and violent extremists. Terrorist attacks in Christchurch, Buffalo, Halle and elsewhere demonstrate the tragic consequences when violent extremists are able to exploit online services to radicalise, incite, and glorify acts of mass violence. Five years on from the Christchurch attack, eSafety continues to receive reports about recordings of abhorrent footage from this and other attacks being shared on mainstream platforms.

The tech companies that provide these services have a responsibility to ensure that their products cannot be used to perpetrate such harm. However, to date there has been a lack of transparency about the tangible measures the online industry is taking to address TVE and a lack of accountability for any gaps.

Industry, governments and civil society spent years developing the Voluntary Transparency Reporting Framework through the OECD to provide a consensus baseline of transparency. Two years on, only two companies, Discord and Mega, have reported, and some of the companies who have received notices do not even publish their own transparency reports.

It is clear that relying on companies to voluntarily report on the steps they are taking is not working. Where industry participants are not providing transparency, we are looking to fill the gaps, compel answers, and hold industry to account. Our questions deliberately build on those agreed through the OECD process.

Reddit and Telegram are also required to answer questions about the measures they have in place to detect and remove child sexual exploitation and abuse (CSEA). Neither have been required by eSafety to report on this harm previously.

As we have done with previous notices on CSEA and online hate, eSafety will publish a transparency report summarising the information and insights we obtain through this process. You can find our previous reports here, which we have seen some companies – although not all – respond to by making key improvements. We will continue to use these powers, alongside our powers to enforce obligations in six industry mandatory Codes now in force, as well as two forthcoming Standards, to ensure industry live up to their responsibility and put in place appropriate safeguards.

Please contact s 22 Executive Manager of Industry Regulation and Legal Services (s 22 @eSafety.gov.au) should you have any questions.

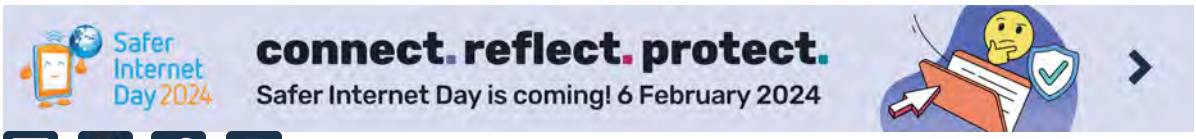
Yours sincerely,

Julie

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

From: Julie Inman Grant
To: s 47F
Cc: Toby Dagg; s 22
Subject: Australian eSafety Commissioner issues 6 transparency notices around how major companies are preventing and minimising TVEC on their platforms [SEC=OFFICIAL]
Date: Monday, 18 March 2024 10:42:00 PM
Attachments: Media release TVEC Notices.docx
image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

Dear Deputy Director s 47F

I would like to advise that I have given transparency notices under Australia's Online Safety Act to Meta, WhatsApp, Google, Reddit, X Corp, and Telegram requiring these companies to report on how they are preventing and minimising terrorism and violent extremism on their services. The press release will be under embargo for the next two hours.

The notices require the companies to explain how they are meeting the Australian Government's Basic Online Safety Expectations, and aim to provide transparency on the systems, tools, processes, and resources that may be used by platforms to tackle terrorist and violent extremism on their services.

We are asking questions about features we know are exploited by bad actors like livestreaming, file storage, algorithms and recommender systems. For relevant services, we are also asking about their generative AI features, which we know terrorists and violent extremists are looking at how they can exploit.

For many years, governments and civil society have called on the online industry to take greater steps to counter online radicalisation and the weaponization of the internet by terrorists and violent extremists. Terrorist attacks in Christchurch, Buffalo, Halle and elsewhere demonstrate the tragic consequences when violent extremists are able to exploit online services to radicalise, incite, and glorify acts of mass violence. Five years on from the Christchurch attack, eSafety continues to receive reports about recordings of abhorrent footage from this and other attacks being shared on mainstream platforms.

The tech companies that provide these services have a responsibility to ensure that their products cannot be used to perpetrate such harm. However, to date there has been a lack of transparency about the tangible measures the online industry is taking to address TVE and a lack of accountability for any gaps.

Industry, governments and civil society spent years developing the Voluntary Transparency Reporting Framework through the OECD to provide a consensus baseline of transparency. Two years on, only two companies, Discord and Mega, have reported, and some of the companies who have received notices do not even publish their own transparency reports.

It is clear that relying on companies to voluntarily report on the steps they are taking is not working. Where industry participants are not providing transparency, we are looking to fill the gaps, compel answers, and hold industry to account. Our questions deliberately build on those agreed through the OECD process.

Reddit and Telegram are also required to answer questions about the measures they have in place to detect and remove child sexual exploitation and abuse (CSEA). Neither have been required by eSafety to report on this harm previously.

As we have done with previous notices on CSEA and online hate, eSafety will publish a transparency report summarising the information and insights we obtain through this process. You can find our previous reports here, which we have seen some companies – although not all – respond to by making key improvements. We will continue to use these powers, alongside our powers to enforce obligations in six industry mandatory Codes now in force, as well as two forthcoming Standards, to ensure industry live up to their responsibility and put in place appropriate safeguards.

Please contact s 22 Executive Manager of Industry Regulation and Legal Services (s 22 @eSafety.gov.au) should you have any questions.

Yours sincerely,

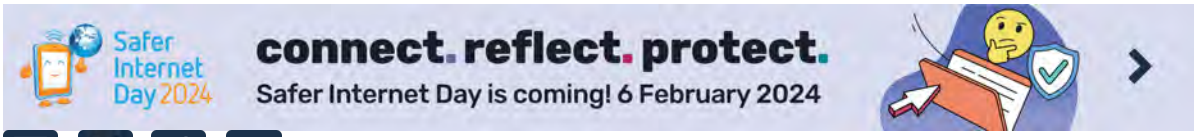
Julie

Julie Inman Grant

Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

From: Julie Inman Grant
To: s 47F
Cc: s 47F Toby Dagg; s 22
Subject: Australian eSafety Commissioner issues 6 transparency notices around how major companies are preventing and minimising TVEC on their platforms [SEC=OFFICIAL]
Date: Monday, 18 March 2024 11:01:00 PM
Attachments: Media release TVEC Notices.docx
image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

s 47F and Team:

Thank you so much for being so generous with your time and insights in January this year. It feels as if we have fit another year into the following months since that time! We are keen to talk further and wanted to advise that I have given transparency notices under Australia's Online Safety Act to Meta, WhatsApp, Google, Reddit, X Corp, and Telegram requiring these companies to report on how they are preventing and minimising terrorism and violent extremism on their services.

This embargoed press release will be going live in a little over an hour.

The notices require the companies to explain how they are meeting the Australian Government's Basic Online Safety Expectations, and aim to provide transparency on the systems, tools, processes, and resources that may be used by platforms to tackle terrorist and violent extremism on their services.

We are asking questions about features we know are exploited by bad actors like livestreaming, file storage, algorithms and recommender systems. For relevant services, we are also asking about their generative AI features, which we know terrorists and violent extremists are looking at how they can exploit.

For many years, governments and civil society have called on the online industry to take greater steps to counter online radicalisation and the weaponization of the internet by terrorists and violent extremists. Terrorist attacks in Christchurch, Buffalo, Halle and elsewhere demonstrate the tragic consequences when violent extremists are able to exploit online services to radicalise, incite, and glorify acts of mass violence. Five years on from the Christchurch attack, eSafety continues to receive reports about recordings of abhorrent footage from this and other attacks being shared on mainstream platforms.

The tech companies that provide these services have a responsibility to ensure that their products cannot be used to perpetrate such harm. However, to date there has been a lack of transparency about the tangible measures the online industry is taking to address TVE and a lack of accountability for any gaps.

Industry, governments and civil society spent years developing the Voluntary Transparency Reporting Framework through the OECD to provide a consensus baseline of transparency. Two years on, only two companies, Discord and Mega, have reported, and some of the companies who have received notices do not even publish their own transparency reports.

It is clear that relying on companies to voluntarily report on the steps they are taking is not working. Where industry participants are not providing transparency, we are looking to fill the gaps, compel answers, and hold industry to account. Our questions deliberately build on those agreed through the OECD process.

Reddit and Telegram are also required to answer questions about the measures they have in place to detect and remove child sexual exploitation and abuse (CSEA). Neither have been required by eSafety to report on this harm previously.

As we have done with previous notices on CSEA and online hate, eSafety will publish a transparency report summarising the information and insights we obtain through this process. You can find our previous reports here, which we have seen some companies – although not all – respond to by making key improvements. We will continue to use these powers, alongside our powers to enforce obligations in six industry mandatory Codes now in force, as well as two forthcoming Standards, to ensure industry live up to their responsibility and put in place appropriate safeguards.

Please contact s 22 Executive Manager of Industry Regulation and Legal Services (s 22 eSafety.gov.au) should you have any questions.

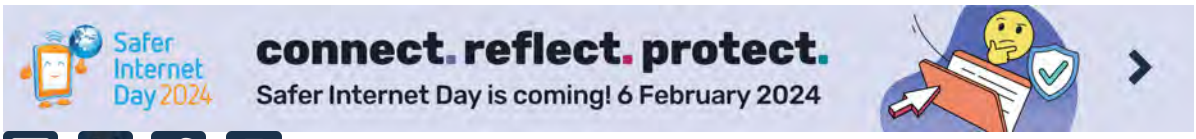
Yours sincerely,

Julie

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

From: Julie Inman Grant
To: s 47F Tech Against Terrorism s 47F
Cc: Toby Dagg; s 22
Subject: Australian eSafety Commissioner issues 6 transparency notices around how major companies are preventing and minimising TVEC on their platforms [SEC=OFFICIAL]
Date: Monday, 18 March 2024 11:01:26 PM
Attachments: Media release TVEC Notices.docx
image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

Dear s 47F

I would like to advise that I have given transparency notices under Australia's Online Safety Act to Meta, WhatsApp, Google, Reddit, X Corp, and Telegram requiring these companies to report on how they are preventing and minimising terrorism and violent extremism on their services.

This embargoed press release will be going live in a little over an hour.

The notices require the companies to explain how they are meeting the Australian Government's Basic Online Safety Expectations, and aim to provide transparency on the systems, tools, processes, and resources that may be used by platforms to tackle terrorist and violent extremism on their services.

We are asking questions about features we know are exploited by bad actors like livestreaming, file storage, algorithms and recommender systems. For relevant services, we are also asking about their generative AI features, which we know terrorists and violent extremists are looking at how they can exploit. You will notice that we evoke Tech Against Terrorism's latest intelligence reports to provide evidence – and I want to reinforce that we find these incredibly valuable. Thank you for the incredible disruption work you and your colleagues are doing.

For many years, governments and civil society have called on the online industry to take greater steps to counter online radicalisation and the weaponization of the internet by terrorists and violent extremists. Terrorist attacks in Christchurch, Buffalo, Halle and elsewhere demonstrate the tragic consequences when violent extremists are able to exploit online services to radicalise, incite, and glorify acts of mass violence. Five years on from the Christchurch attack, eSafety continues to receive reports about recordings of abhorrent footage from this and other attacks being shared on mainstream platforms.

The tech companies that provide these services have a responsibility to ensure that their products cannot be used to perpetrate such harm. However, to date there has been a lack of transparency about the tangible measures the online industry is taking to address TVE and a lack of accountability for any gaps.

It seems like eons ago we first met at Boston University in 2019 to launch the OECD's VTRF. As you well know, industry, governments and civil society spent years developing the Voluntary Transparency Reporting Framework to provide a consensus baseline of transparency. You would also be very aware that only two companies, Discord and Mega, have reported, and some of the companies who have received notices do not even publish their own transparency reports.

It is clear that relying on companies to voluntarily report on the steps they are taking is not working. Where industry participants are not providing transparency, we are looking to fill the gaps, compel answers, and hold industry to account. Our questions deliberately build on those agreed through the OECD process.

Reddit and Telegram are also required to answer questions about the measures they have in place to detect and remove child sexual exploitation and abuse (CSEA). Neither have been required by eSafety to report on this harm previously.

As we have done with previous notices on CSEA and online hate, eSafety will publish a transparency report summarising the information and insights we obtain through this process. You can find our previous reports here, which we have seen some companies – although not all – respond to by making key improvements. We will continue to use these powers, alongside our powers to enforce obligations in six industry mandatory Codes now in force, as well as two forthcoming Standards, to ensure industry live up to their responsibility and put in place appropriate safeguards.

Please contact s 22 Executive Manager of Industry Regulation and Legal Services (s 22 @eSafety.gov.au) should you have any questions.

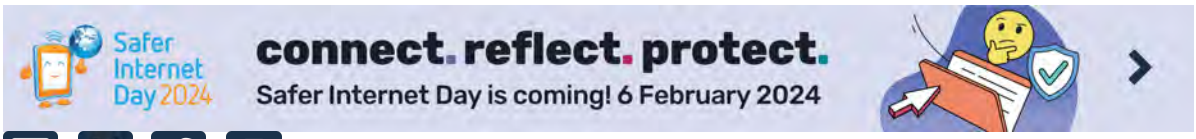
Yours sincerely,

Julie

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

From: Julie Inman Grant
To: s 47F @gifct.org
Cc: Toby Dagg; s 22
Subject: Australian eSafety Commissioner issues 6 transparency notices around how major companies are preventing and minimising TVEC on their platforms [SEC=OFFICIAL]
Date: Tuesday, 19 March 2024 8:13:00 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png
Media release TVEC Notices.docx

OFFICIAL

Dear s 47F

I would like to advise that I have given transparency notices under Australia's Online Safety Act to Meta, WhatsApp, Google, Reddit, X Corp, and Telegram requiring these companies to report on how they are preventing and minimising terrorism and violent extremism on their services. We appreciate the work that the GIFCT is doing in this space.

The notices require the companies to explain how they are meeting the Australian Government's Basic Online Safety Expectations, and aim to provide transparency on the systems, tools, processes, and resources that may be used by platforms to tackle terrorist and violent extremism on their services.

We are asking questions about features we know are exploited by bad actors like livestreaming, file storage, algorithms and recommender systems. For relevant services, we are also asking about their generative AI features, which we know terrorists and violent extremists are looking at how they can exploit.

For many years, governments and civil society have called on the online industry to take greater steps to counter online radicalisation and the weaponization of the internet by terrorists and violent extremists. Terrorist attacks in Christchurch, Buffalo, Halle and elsewhere demonstrate the tragic consequences when violent extremists are able to exploit online services to radicalise, incite, and glorify acts of mass violence. Five years on from the Christchurch attack, eSafety continues to receive reports about recordings of abhorrent footage from this and other attacks being shared on mainstream platforms.

The tech companies that provide these services have a responsibility to ensure that their products cannot be used to perpetrate such harm. However, to date there has been a lack of transparency about the tangible measures the online industry is taking to address TVE and a lack of accountability for any gaps.

Industry, governments and civil society spent years developing the Voluntary Transparency Reporting Framework through the OECD to provide a consensus baseline of transparency. Two years on, only two companies, Discord and Mega, have reported, and some of the companies who have received notices do not even publish their own transparency reports.

It is clear that relying on companies to voluntarily report on the steps they are taking is not working. Where industry participants are not providing transparency, we are looking to fill the gaps, compel answers, and hold industry to account. Our questions deliberately build on those agreed through the OECD process.

Reddit and Telegram are also required to answer questions about the measures they have in place to detect and remove child sexual exploitation and abuse (CSEA). Neither have been required by eSafety to report on this harm previously.

As we have done with previous notices on CSEA and online hate, eSafety will publish a transparency report summarising the information and insights we obtain through this process. You can find our previous reports here, which we have seen some companies – although not all – respond to by making key improvements. We will continue to use these powers, alongside our powers to enforce obligations in six industry mandatory Codes now in force, as well as two forthcoming Standards, to ensure industry live up to their responsibility and put in place appropriate safeguards.

Please contact s 22 Executive Manager of Industry Regulation and Legal Services (s 22 @eSafety.gov.au) should you have any questions.

Yours sincerely,

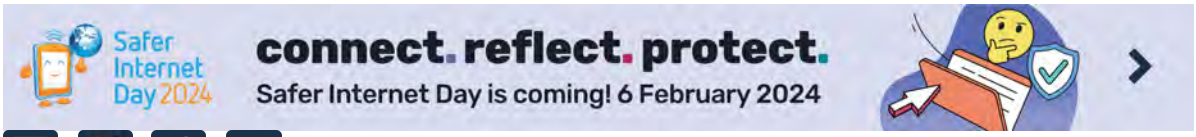
Julie

Julie Inman Grant

Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

From: Julie Inman Grant
To: Toby Dagg; s 22 ; Kathryn King; Media OeSC
Subject: Elon Musk replies to post by far-right Austrian linked to Christchurch terror I
Date: Wednesday, 20 March 2024 7:49:56 AM

Another useful and relevant piece from Josh Taylor. J

https://www.theguardian.com/technology/2024/mar/19/elon-musk-replies-x-twitter-martin-sellner-far-right-identitarian-movement-christchurch-terrorist-attack

Get Outlook for iOS

From: Julie Inman Grant
To: Toby Dagg; Kathryn King
Subject: Re: Quick readout: X Corp. mediation [SEC=OFFICIAL:Sensitive]
Date: Wednesday, 27 March 2024 12:44:48 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png

s 45, s 47E(d), s 47F

[redacted]

From: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Sent: Tuesday, March 26, 2024 1:21:06 AM
To: Kathryn King s 47E(c), s 47F @eSafety.gov.au>; Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Subject: Quick readout: X Corp. mediation [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

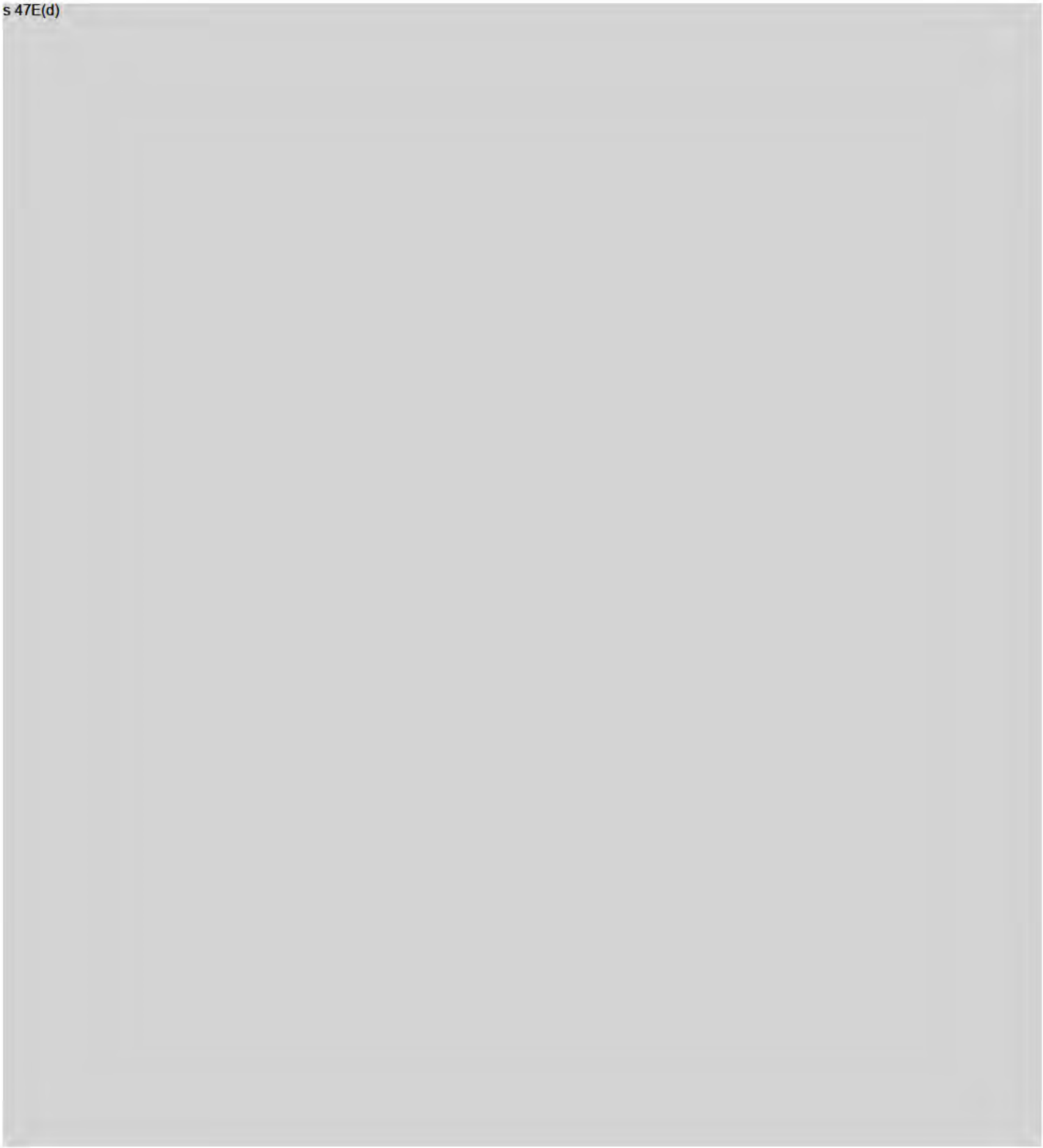
Hi both

I promised you a readout of the X Corp. mediation today, and will provide a brief summary below that we can discuss once you're back on deck, Julie.

s 47E(d)

[redacted]

s 47E(d)



Happy to talk through in more detail next week.

TD.

Toby Dagg
General Manager
Regulatory Operations Group

s 47E(c), s 47F

esafety.gov.au

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, present and emerging.

From: Julie Inman Grant
To: s 22 Toby Dagg; Kathryn King
Subject: Re: X Corp loses lawsuit against CCDH - Hate Watch Dog [SEC=UNOFFICIAL]
Date: Sunday, 31 March 2024 2:29:17 PM

A few intriguing developments in US litigation, including conservative AG engagement:

https://amp.theguardian.com/us-news/2024/mar/30/media-matters-lawsuit-missouri-elon-musk

https://slate.com/news-and-politics/2024/03/elon-musk-media-matters-supreme-court.html

Interesting to look at Kaplan's dismissal...

https://www.kaplanhecker.com/newsroom/khf-secures-dismissal-center-countering-digital-hate-ccdh-x-corp-v-center-countering

Get Outlook for iOS

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Monday, March 25, 2024 10:53 am
To: s 22 @eSafety.gov.au>; s 22
s 22 @eSafety.gov.au>; s 22
s 22 @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Subject: X Corp loses lawsuit against CCDH - Hate Watch Dog [SEC=UNOFFICIAL]

https://www.reuters.com/technology/musks-x-corp-loses-lawsuit-against-hate-speech-watchdog-2024-03-25/

Get Outlook for iOS

From: Toby Dagg
To: s 22 Julie Inman Grant; Kathryn King; s 22
Cc: s 22
Subject: Re: Decision required: OSA review - Governance Group meeting follow up [SEC=OFFICIAL]
Date: Wednesday, 3 April 2024 10:21:20 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png
image009.png

OFFICIAL

Hi s 22

My own apologies for the delay in getting back to you.

Thanks for the email.

Re key dates, noted. Have we received the issues paper yet? I gather not.

On the deep dives topics, noted. We have a pre-meeting scheduled for Friday to bottom out a position (of some sort) on codes, but I would also like to use that time to ensure we're aligned on the key questions on the BOSE, especially what we want in term of reform.

In relation to the updated list of material to provide s 47F I have no problems with the items and tend to agree that we might hold on those volumetric abuse items until the backgrounder is finalised. Honestly, we might want to note that the notion of a volumetric attack seems somewhat quaint in March 2024 when compared with our first usage of the term five or so years ago. That is because Twitter/X has never been more prone to being weaponised and there is a far greater degree of coordination now than ever before. So, I say 'quaint' because online attacks seem increasingly to have a volumetric component as standard issue.

Looking forward to discussing on Friday.

TD.

From: s 22 @esafety.gov.au>
Sent: 02 April 2024 15:45
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 @eSafety.gov.au>
Cc: s 22 @eSafety.gov.au>; s 22 s 22 @eSafety.gov.au>; s 22 @esafety.gov.au>; s 22

s 22 @eSafety.gov.au>
Subject: Decision required: OSA review - Governance Group meeting follow up [SEC=OFFICIAL]

OFFICIAL

Hi All

Firstly, apologies for the lengthy email, but there are some actions that require decisions from the Governance Group. I am seeking responses to **items 3 and 4 by COB tomorrow** to allow progress and scheduling. To break it down I have listed items under the following headings:

1. Key dates – for **noting.**
2. Advice from Department on deep dives – for **noting.**
3. Deep dives requested by the Reviewer to inform the discussion paper – for **noting and awareness.**
4. Suggested deep dives to inform the broader review - for **agreement.**
5. Documents to share with the Reviewer - for **agreement.**

1. **Key dates**

Keys date to be aware of

- Expecting to receive a draft Issues paper this week with response by end of week.
- Department aiming to send the Issues paper to the MO by 25 April.
- s 47F

2. **Deep dives**

s 22 sought clarification from the Department on if the deep dives are for the issues paper or broader Review, in short both.
I've gotten confirmation that the 8 April is fine for the BOSE and they understand it needs to be separate, so we will do BOSE first, then Penalties/Enforcement and then Codes.
In terms of whether these meetings are for the Issues Paper or for the broader review, the response is that they cover both. The Reviewer wants to take an early run at the most critical issues with a view to recommendations but also wants to ensure she has the context correct so the Issues Paper is well pitched. We will receive a draft of the Issues Paper probably early next week with a same week turnaround.

3. **Deep dives requested to inform discussion paper**

Deep dive	**Timing**	**Branch responsible for content**
Introduction to key issues and regulatory schemes	27 February	RPS - completed
Online hate	22 March	RPS - completed
BOSE	8 April (scheduled)	IRLS
Codes	w/c 8 April (to be scheduled)	IRLS, with any pre-reading provided to s 47F by 5 April s 22 – please advise if you would like a pre-meeting to discuss an internal position.

Penalties	w/c 15 April (to be scheduled)	RPS and IRLS, with pre-reading provided to s 47F by 12 April A pre-meeting to discuss an internal position is scheduled for 11 April.

4. **Suggested further deep dives**

If agree, to be confirmed with Dept/Reviewer and expected after the discussion paper released.

Deep dive	**Timing**	**Area responsible for content**
Information Gathering and sharing • Information sharing: sharing, gathering/requiring disclosure, secrecy; and account preservation, BSI, evidence	TBC	Investigations / IRLS. With digital tech/data and legal to be consulted. Proposed background material • Reshare slides from first session and tables already made
Emerging technologies – metaverse/immersive tech/content, contact, conduct • Content/contact/conduct • IBA examples • Anti-recidivism powers (e.g. remedial direction, account-related) • Metaverse and immersive environments	TBC	RPS / Investigations Proposed background material • Tech trends papers – E2EE, metaverse, doxing etc
Volumetric attacks	TBC	RPS / Investigations Proposed background material • Volumetric attacks paper

5. **List of potential documents or links to be shared with reviewer,** with thanks to s 22 for pulling this list together:

Please note if you agree, do not wish for the document to be shared, or would like to discuss

- Volumetric Abuse Backgrounder 2024 – close to finalisation, recommend send all related material with this document once complete
- Letter to s 47F (attached) – recommend hold off until volumetric brief finalised and probably not send as could be taken out of context
- Draft letter to platform (attached) – recommend hold off until volumetric brief finalised and probably not send as could be taken out of context
- 2021 Memorandum on Volumetric Abuse – recommend hold off until volumetric brief

finalised

- C3P youtube
- IWF podcast
- Neural hashing: most recent correspondence with Snap and Apple on Sexual Extortion – recommend not send as could be taken out of context or hold until BOSE Deep Dive
- CSINT Conversations: Stopping online abuse of children - Could Apple have the answer? (youtube.com) - s 22 has noted that this is 'a very clear explainer of what CSAM is and tech solutions'
- CSAM Detection - Technical Summary (apple.com)
- AGD hate speech documents – Department has provided these and is organising a meeting; s 22 has requested that we be involved / have visibility.
- NSW Premier's Dashboard on Hate further information
- Hate Speech Toplines.pptx - Topline findings on online hate from adult survey – a separate meeting or other communication may be more appropriate
- 25. Back Pocket Brief - Online hate - FINAL.docx (sharepoint.com) – we chose not to send this as the briefing already sent is more comprehensive
- Federal Register of Legislation - Online Safety (Basic Online Safety Expectations) Determination 2022 - Recommend we send this and the two below over with the presentation before the BOSE meeting
- Key-Findings-Basic-Online-Safety-Expectations-Summary-of-response-to-non-periodic-notice-issued-to-X-Corp.Twitter-in-June-2023.pdf (esafety.gov.au)
- Full-Report-Basic-Online-Safety-Expectations-Summary-of-response-from-X-CorpTwitter-to-eSafetys-transparency-notice-on-online hate.pdf
- Brief_Irish Online Safety Code.docx (sharepoint.com)
- Country Brief - Ireland - (January 2024).docx (sharepoint.com)
- Fact sheet: Draft Online Safety (Relevant Electronic Services – Class 1A and Class 1B Material) Industry Standard 2024
- Draft Online Safety (Relevant Electronic Services - Class 1A and Class 1B Material) Industry Standard 2024_0.pdf
- Draft Online Safety (Designated Internet Services-Class 1A and Class 1B Material) Industry Standard 2024.pdf
- Material written about the Standard thus far - if any
- End-to-end encryption trends and challenges — position statement | eSafety Commissioner
- Protecting Children in the Age of End-to-End Encryption (american.edu)
- Hany Farid videos:
  - https://www.iwf.org.uk/news-media/blogs/encryption-vs-privacy-in-conversation-with-professor-hany-farid/
  - https://www.youtube.com/watch?v=FzyHsq9CiK0
  - https://annualreport2021.iwf.org.uk/about/hfarid
  - https://podcasts.apple.com/au/podcast/1-encryption-vs-privacy-in-conversation-with-professor/id1637147155?i=1000571601684
- Connect the Reviewer with an expert like Hany Farid and organise a meeting?
- Connect the Reviewer to the INHOPE meeting in April?
- Connect the Reviewer to the NCMEC meeting in April?

Thanks

s 22
Executive Manager
Strategy, Engagement and Research
eSafety Commissioner

s 22 s 22

esafety.gov.au

Australian Government | eSafetyCommissioner

From: Julie Inman Grant
To: Kathryn King; Toby Dagg; s 22
Subject: Re: Pretty extraordinary- X judge in Brazil [SEC=UNOFFICIAL]
Date: Monday, 8 April 2024 9:44:08 PM

---

https://apple.news/AVBlrObT_TGCHH_Qf-dCMeA

Get Outlook for iOS

From: Julie Inman Grant
Sent: Monday, April 8, 2024 7:50:20 PM
To: Kathryn King s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>
Subject: Pretty extraordinary- X judge in Brazil [SEC=UNOFFICIAL]

https://x.com/elonmusk/status/1776989005848207503?s=46&t=LKaPiNL33rLi-iL-F-AZVA

Get Outlook for iOS

From: Julie Inman Grant
To: s 22 Toby Dagg; Kathryn King; s 22
Cc: s 22
Subject: RE: follow up to two queries [SEC=OFFICIAL]
Date: Tuesday, 9 April 2024 10:00:00 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

OFFICIAL

On the Ombusdmen messaging, thanks.

On the recommender system issue, this wasn't just about X – this was about the second tranche of notices and whether or not there were any significant or useful findings around harmful algorithms/recommender systems.

From: s 22 @eSafety.gov.au>
Sent: Tuesday, April 9, 2024 9:58 AM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 s 22 @esafety.gov.au>
Cc: s 22 @eSafety.gov.au>
Subject: follow up to two queries [SEC=OFFICIAL]

OFFICIAL

Hi Julie,

I meant to come back to you last week on two points that you raised.

Apologies for the delay but here is the follow-up

1. **X Corp. any new information we learnt on their recommender systems/algorithms from the Notice**
   I confirmed with s 22 that there was nothing new we learnt about their recommender system from either their response to the online hate or CSEA notice. We published the design objectives and signals used, but they didn't reveal anything that we wouldn't have expected
2. **Ombudsman**
   As discussed, we should be balanced in how we treat the decision of the Commonwealth Ombudsman in February this year re the s 47F complaint given it is not an adversarial process and a positive outcome isn't a "win" per se . The wording I passed onto s 22 last week was: "The Commonwealth Ombudsman received a complaint regarding an ACA decision made by eSafety in 2023. The Commonwealth

Ombudsman having considered all the relevant circumstances, decided that no further investigation was warranted and closed the matter."

Let me know if you have any questions and apologies for the delay

s 22

s 22

Executive Manager – Industry Regulation and Legal Services

Australian Government | eSafetyCommissioner

s 22

esafety.gov.au

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, present and emerging.

From: Julie Inman Grant
To: Toby Dagg
Subject: RE: For GM approval: eSafety submission to AHRC"s national project mapping threats to TGD human rights in Australia. [SEC=OFFICIAL]
Date: Tuesday, 9 April 2024 11:34:00 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

s 47C, s 47E(d)

[redacted]

From: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Sent: Tuesday, Ap 0:53 AM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Subject: FW: For GM approval: eSafety submission to AHRC's national project mapping threats to TGD human rights in Australia. [SEC=OFFICIAL]

OFFICIAL

Julie, just fyi and further to our discussion. I will keep you updated as the further draft progresses.

From: s 22 @esafety.gov.au>
Sent: Tuesday, April 9, 2024 9:30 AM
To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Subject: RE: Fo val: eSafety submission to AHRC's national project mapping threats to TGD human rights in Australia. [SEC=OFFICIAL]

OFFICIAL

Thanks Toby

And apologies – with everything going on at the moment I probably did not look at this as critically as I should have.

Leave it with me.

s 22

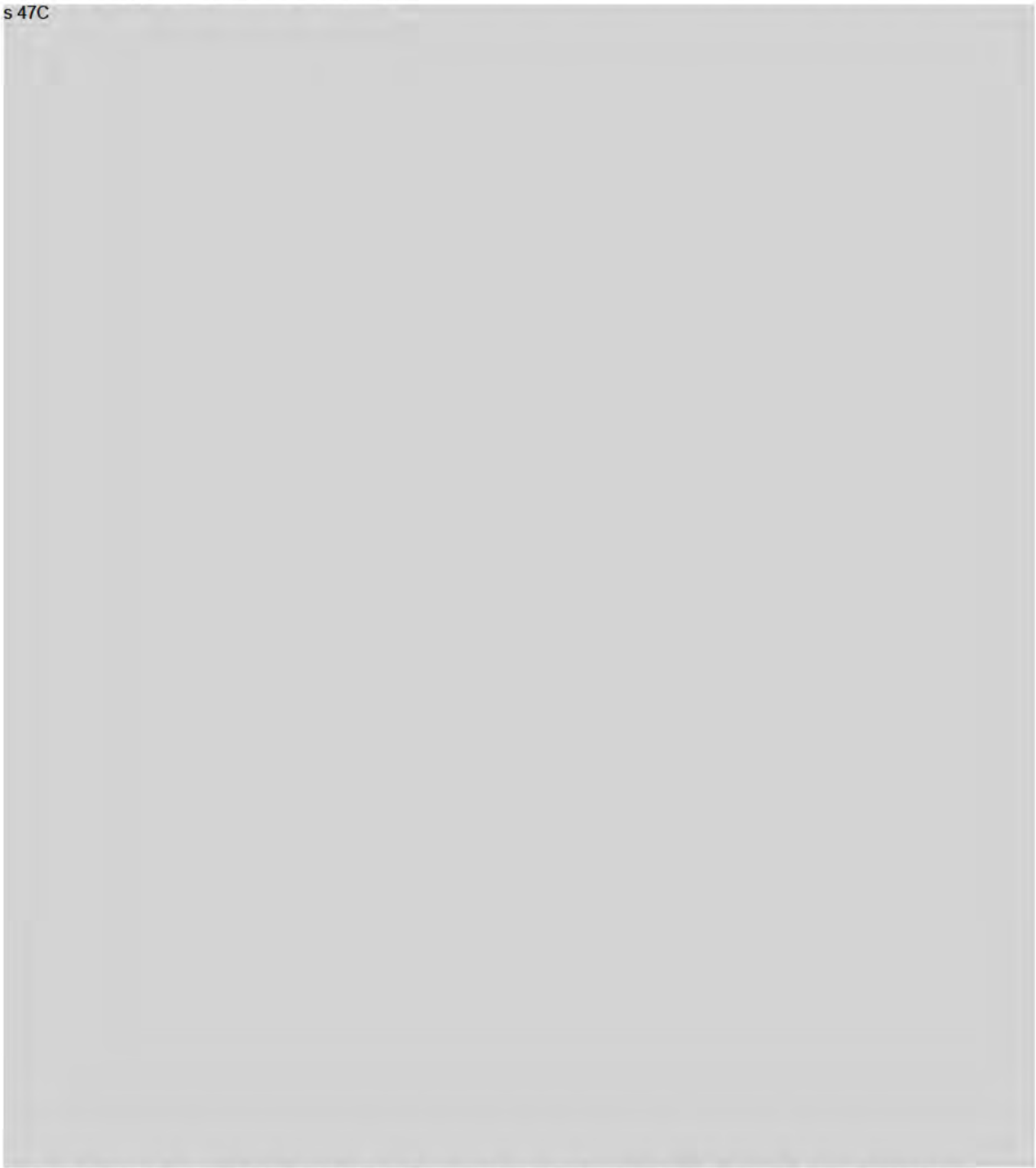
From: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Sent: Tuesday, April 9, 2024 9:15 AM
To: s 22 @esafety.gov.au>
Subject: FW: For GM approval: eSafety submission to AHRC's national project mapping threats to TGD human rights in Australia. [SEC=OFFICIAL]
Importance: High

OFFICIAL

Hi s 22

I've now read the submission. I'm afraid to say that it needs a lot of work before Julie will be happy to sign off and I can't approve this until there has been substantial improvement.

s 47C



There is other feedback, which I will provide through comments and edits. Happy to discuss, of course, but we will need to turn around a much stronger version of this before Julie reviews.

Toby.

From: s 22 @esafety.gov.au>
Sent: Friday, April 5, 2024 4:20 PM
To: s 22 @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Cc: s 22 @esafety.gov.au>; s 22 @esafety.gov.au>
Subject: RE: For GM approval: eSafety submission to AHRC's national project mapping threats to TGD human rights in Australia. [SEC=OFFICIAL]

Just to add to this Toby. I know s 22 has said we involved Strat Comms but it was reviewed by s 22 (specifically as requested by Julie)

s 22

From: s 22 @eSafety.gov.au>
Sent: Friday, April 5, 2024 3:42 PM
To: Toby Dagg s 47E(c), s 47E @esafety.gov.au>
Cc: s 22 @esafety.gov.au>; s 22 @esafety.gov.au>; s 22 s 22 @esafety.gov.au>
Subject: For GM approval: eSafety submission to AHRC's national project mapping threats to TGD human rights in Australia. [SEC=OFFICIAL]

OFFICIAL

Hi Toby, hope your week has gone well.

eSafety have been invited to provide a submission to the Australian Human Rights Commission's national project mapping threats to trans and gender diverse (TGD) human rights in Australia.

Having spoken to the AHRC, they see this project as a key first step to understand the scale of offline/online harms that affect TGD communities and could, in the future, help inform the work that eSafety undertakes in the space to support marginalised and at-risk communities.

eSafety response to AHRC national project mapping threats to TGD human rights.docx

In summary, our response encompasses:

- Context to eSafety and our role.
- Our mission to foster safer online environments.
- Our research and reporting insights that help us build a picture of the online experiences of TGD communities.
- Our relevant work in this space that align with the three Ps – including our EPI programs focused on LGBTIQ+ audiences and Gendered violence, our work with BOSE and Codes and our proactive approach to promote Safety By Design amongst the tech industry.

This response has been pulled together with contributions from relevant eSafety teams and branch areas including EPI, Strategy & Policy, Strat Comms, Investigations, Codes, BOSE, SBD and Research. It has also been approved at the EPI EM level.

We are seeking your review/approval on eSafety's submission **by Thursday 11th April** to meet AHRC's deadline.

Please do let me know if you would like to chat about any of the above in further detail, too.

Have a lovely weekend,

s 22

s 22
A/Manager, eSafety Communities
s 22
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.

From: Julie Inman Grant
To: Toby Dagg; s 22
Subject: Re: Elon Musk Has a Porn Problem - Bloomberg Businessweek [SEC=UNOFFICIAL]
Date: Wednesday, 10 April 2024 9:11:44 PM

If you think you've been seeing more X-rated content on X lately, you're not alone. Elon Musk's social media platform has long been permissive about suggestive material, but as Musk cut his content moderation teams, there seems to be more of the stuff floating around—and in more prominent places. This week, John Herrman of *New York* magazine, who recently published a story about a strange, particularly viral type of post, joins the *Elon, Inc.* panel to talk about X and porn. But first, Tesla sales numbers. They are not good. Not good at all. Here are some of the topics discussed:

In recent days, Tesla analysts had cut their projected Tesla sales figures. But as Bloomberg senior reporter Dana Hull tells us, not by nearly enough. Tesla delivered just 386,810 vehicles in the first three months of the year, causing the already-ailing Tesla stock to drop more than 6% in the hours following the news.

There are a number of reasons for the disappointing numbers, but many point the finger at Musk's outrageous comments on X (and beyond). One of the more provocative statements to this effect came from longtime Tesla bull investor Ross Gerber. The big winner here, of course, might be the Tesla shortsellers.

Over on X, even casual users have noted very prominent pornographic material—often unwanted. It's true this was a chronic issue on the platform when it was called Twitter, back before Elon Musk owned it. But these days it has only gotten worse as porn spambots proliferate. The one that has become a meme recently is a variation of the phrase "pussy in bio," which often leads to fairly simple scams. The interested clickers follow a series of links to ostensibly talk to a local single. It turns out you don't need complicated technology to hoodwink the lonely—you just need a platform that doesn't seem able to stamp out such a phenomenon at scale.

Besides "PIB" scams, there's plenty of porn on X without the fraud, especially from OnlyFans creators who are using the service to market themselves. Twitter, even pre-Musk, had been unusual among social networks for having liberal content policies that allowed for porn as long as it was correctly labeled and not published in certain high-profile areas of the app. The company even considered starting its own version of Onlyfans.

But as Herrman reports, X is also full of posts promoting Onlyfans agencies–essentially accounts for OnlyFans creators that are staffed by call center workers impersonating actual people. They can wind up working a bit like the flirt sites.

The ubiquity of porn and porn-adjacent spam on X might represent a growth opportunity for the troubled company, but it could further undercut Musk's efforts to win back advertisers who left amid the Tesla chief executive's endorsement of an anti-semitic conspiracy theory. Not to mention users who find the come-ons uncomfortable.

The gutting of content moderation teams clearly has ramifications for the proliferation of porn content. As we discussed in a previous episode, Twitter's response to the viral deepfake porn of Taylor Swift was, for days, just to block searches for Taylor Swift.

Does this mean X will turn into a permanent home for porn, and porn spam? Maybe, but there are also signs that X wants to do more than just complain about sexual content—it might try to profit from it. Bloomberg and others reported last week that X is testing ways to develop user groups for "adult" posts. That's something that the company has looked into before, but it proved too risky, as there are many kinds of exploitative and criminal sexual content that tend to surface.

About the show: Each week, listen in as host David Papadopoulos (and sometimes Max Chafkin) convenes a panel of Bloomberg journalists who are tracking Elon Musk's companies and the surprising ways they intersect, breaking down his latest moves and what they could mean for us all.

Get Outlook for iOS

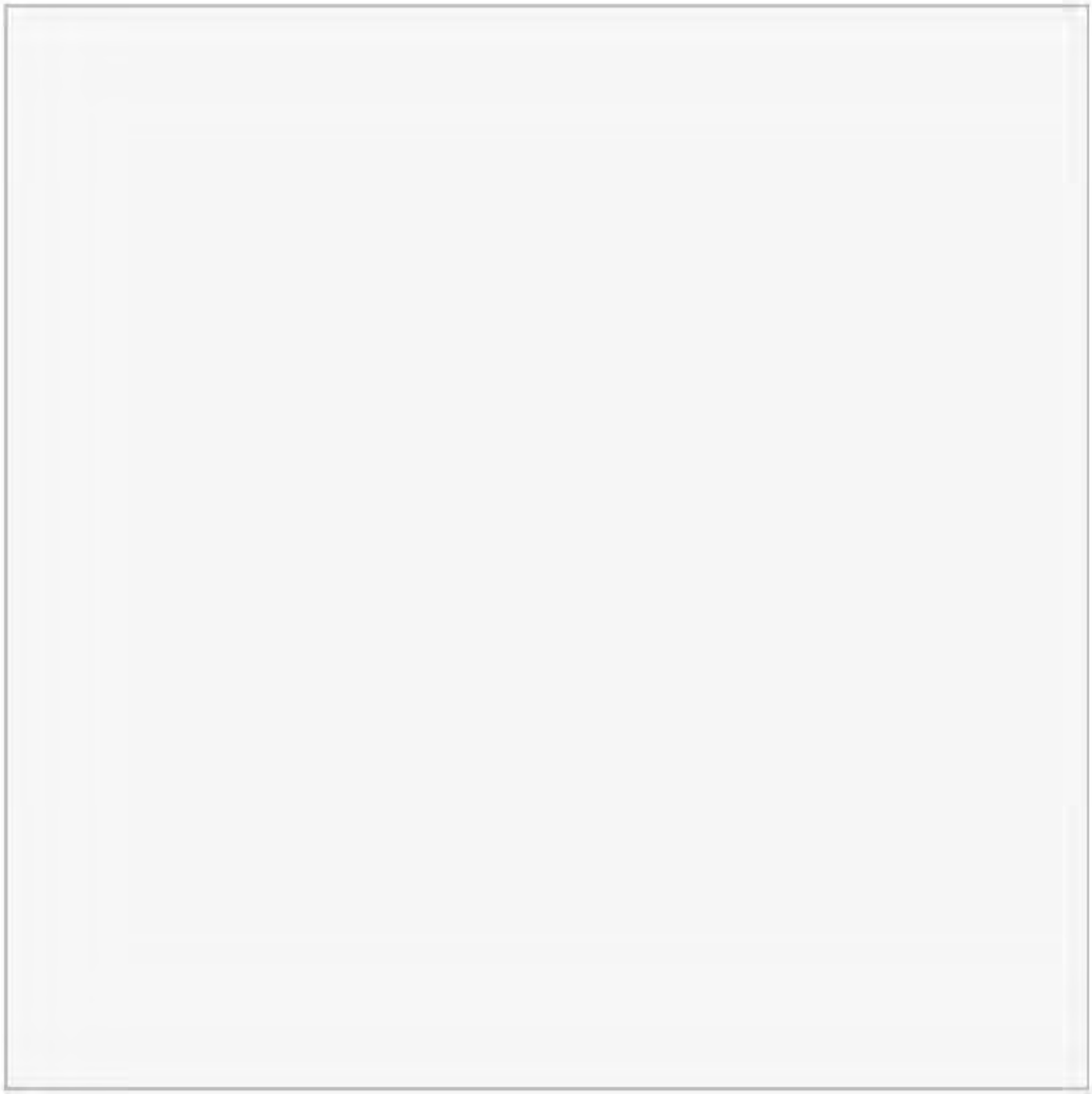
From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Wednesday, April 10, 2024 8:21:52 PM
To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 eSafety.gov.au>; s 22 s 22 @esafety.gov.au>
Subject: Elon Musk Has a Porn Problem - Bloomberg Businessweek [SEC=UNOFFICIAL]

Charming!

https://apple.news/AhbDfe31mRTaNMCpVV9Z5UQ

Elon Musk Has a Porn Problem - Bloomberg Businessweek

Get Outlook for iOS



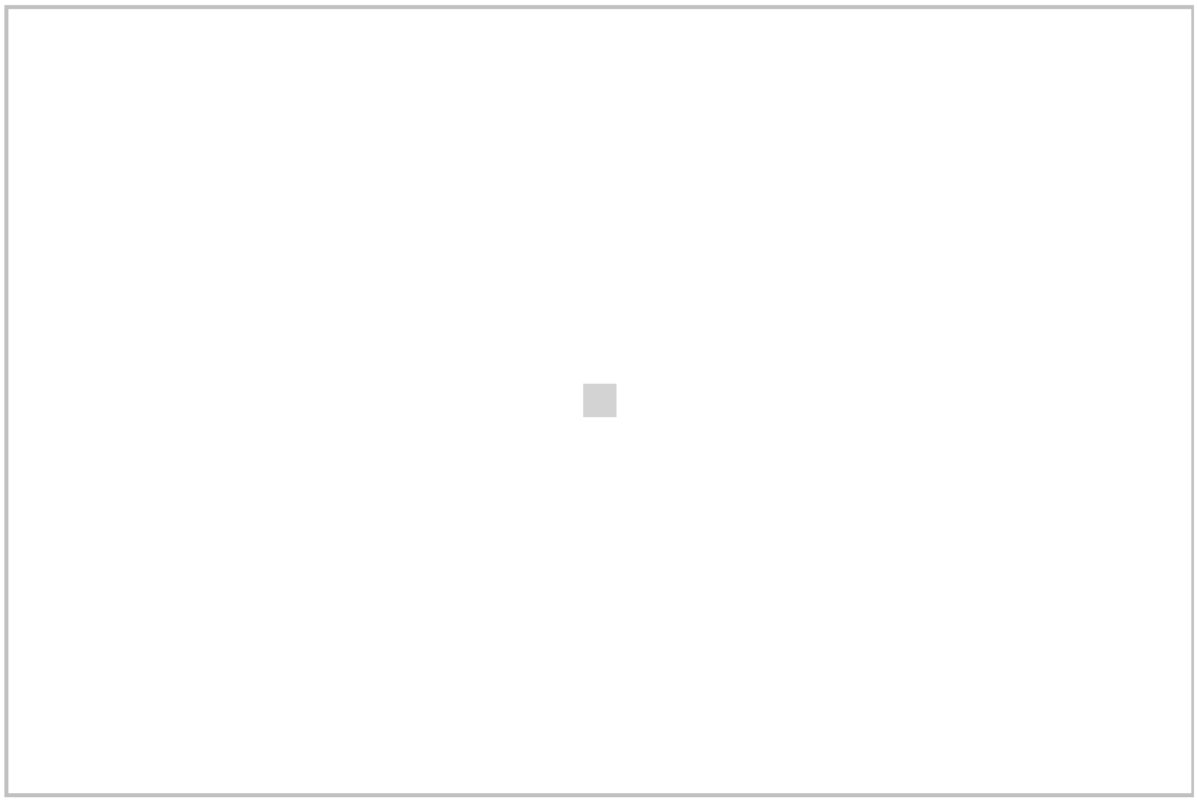
View in browser

The Technology 202

By Will Oremus

Happy Wednesday! Hope your eyes are recovering. Send news tips to: will.oremus@washpost.com.

Elon Musk picks his speech battle



Musk's X is defying orders from Brazilian Supreme Court judge Alexandre de Moraes, shown here, who has accused him of the "criminal instrumentalization of X." (Sergio Lima/AFP/Getty Images)

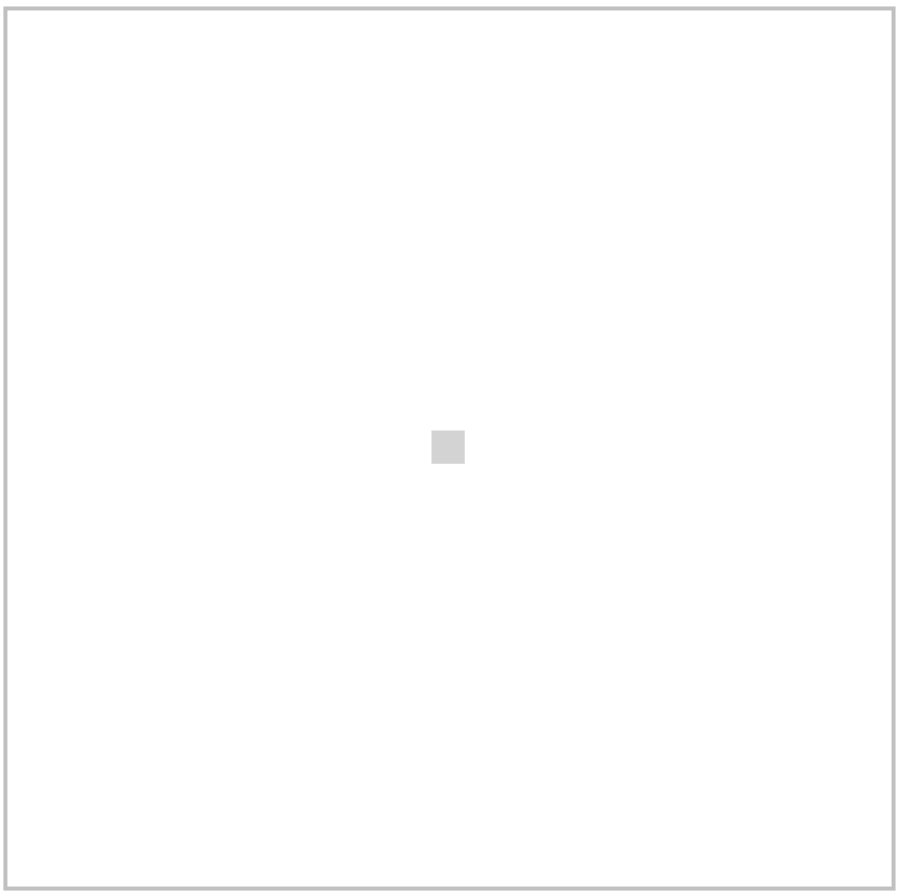
Though **Elon Musk** often insists his goal with X is to promote free speech, his actions have rarely been those of the "free-speech absolutist" he once claimed to be. Yes, he has rolled back the social platform's policies on hate speech, cut back on content moderation and reinstated banned extremists under the free-speech banner. But he has also made up rules to ban accounts he doesn't like, suspended journalists and sued nonprofit advocacy groups in what one judge ruled was a bid to silence critics.

In the United States, the First Amendment and Section 230 of the Communications Decency Act give X a free hand to moderate or tolerate speech as it sees fit. And while many on the left have decried Musk's policies, they've been widely cheered on the right. But it's worth remembering that most X users are not American. And other countries have their own speech laws, some of them much

more restrictive.

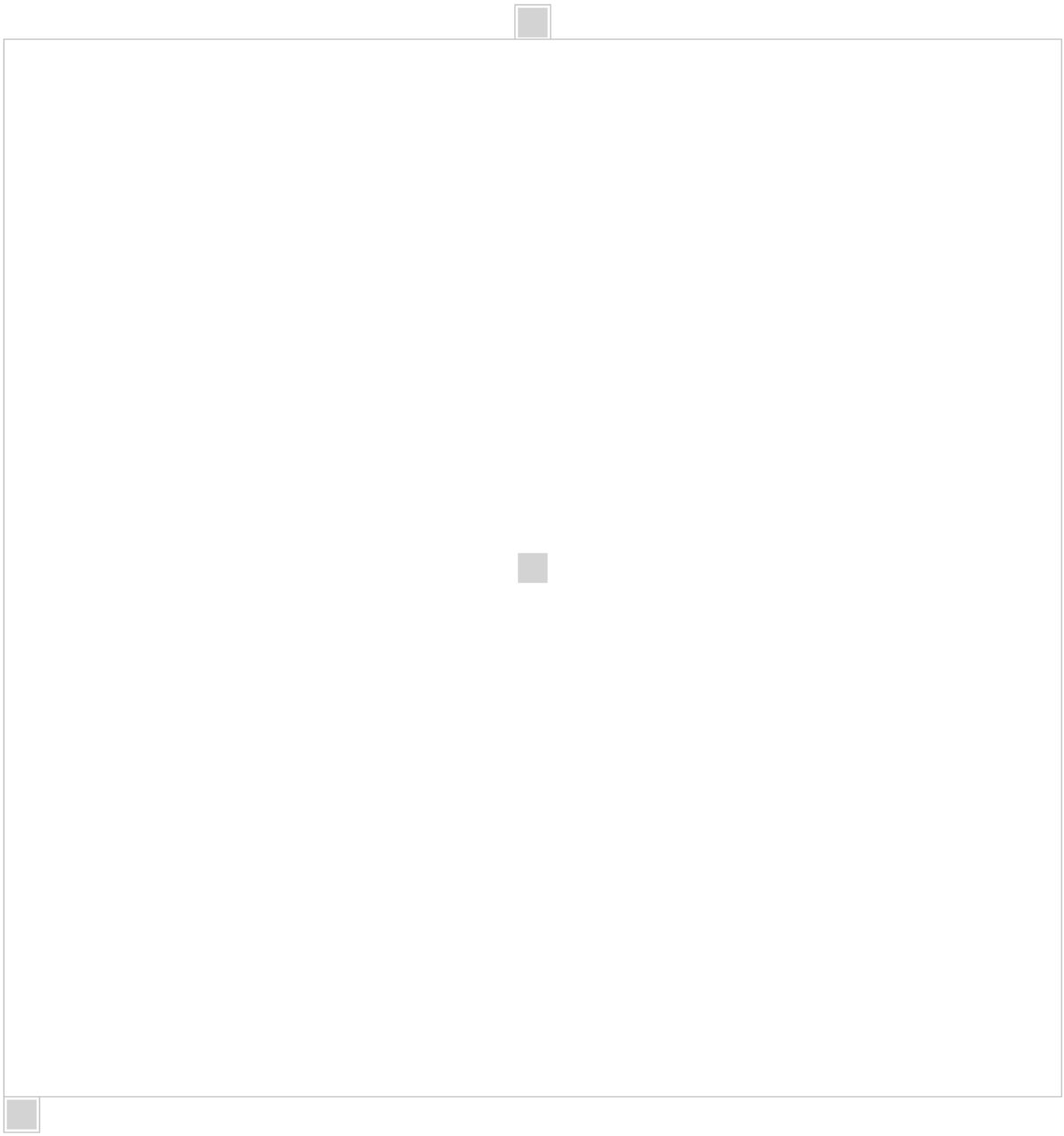
Since acquiring Twitter, which once prided itself on protecting dissidents abroad, Musk has proved unusually compliant when it comes to government censorship and surveillance requests.

In April 2022, Musk tweeted what seemed to be his clearest definition yet of what “free speech” means to him in the context of social media, saying it’s simply “that which matches the law.”



While Musk hasn’t always held true to that principle domestically, he has generally adhered to it overseas. In India, for example, X agreed to block links to a BBC documentary that cast a critical lens on Indian Prime Minister **Narendra Modi**, and it has since capitulated to systematic censorship there. In Turkey, the company restricted tweets at the behest of President **Recep Tayyip Erdogan** on the eve

of a critical election. Musk defended both decisions on the grounds that X had no choice but to comply.



In fact, as of a year ago, Rest of World reported that the company had not refused a single censorship request since Musk took over.

In recent days, however, he has dug in for a high-stakes battle in Brazil that shows he is willing to take a stand against foreign governments — if the speech of right-wing activists is at stake.

The standoff is over orders from Brazilian Supreme Court Justice **Alexandre de Moraes** to block a number of accounts for “spreading

anti-democratic ideas that undermine the Brazilian democratic state." As my colleagues **Niha Masih** and **María Luisa Paúl** reported, those include far-right figures allied with former president **Jair Bolsonaro**, whose supporters stormed Brazilian government buildings on Jan. 8, 2023, following Bolsonaro's electoral defeat.

On Saturday, Musk posted on X that the platform was defying those orders and "lifting all restrictions" on the accounts in question. "This judge has applied massive fines, threatened to arrest our employees and cut off access to X in Brazil," Musk wrote, referring to Moraes. "As a result, we will probably lose all revenue in Brazil and have to shut down our office there. But principles matter more than profit."

As foreign markets go, Brazil is no small potatoes. It is one of X's largest markets outside the United States, and it plays a similar role there, with politicians and activists using it as a megaphone and water cooler to debate public issues. So Musk really is risking X's business. But where did those principles come from all of a sudden?

Musk's showdown with Brazil's Moraes comes after a "Twitter Files" installment that detailed how Moraes and other Brazilian officials pressured social media companies to remove content.

As I wrote when Musk's handpicked journalists began publishing the Twitter Files in late 2022, they have helped Musk justify his takeover of Twitter by casting him as a crusader exposing the "censorship" of the company's previous leadership. Focusing almost exclusively on content moderation against conservatives, they have also helped endear him to Republicans, providing them fodder with which to sue the Biden administration and pressure disinformation researchers.

For Musk and his backers on the right, Brazil presents a parallel scenario in which a liberal government is trying to hold its populist-right predecessor to account for attempting to subvert a democratic election.

Still, Musk's own credo would seem to imply that he should be complying with Brazil's laws.

In Musk's 2022 defining of free speech, he added that "If people want less free speech, they will ask government to pass laws to that effect." Brazil's laws do in fact allow for government restrictions on certain kinds of speech. The country became a democracy only in 1985, after decades of authoritarian rule, and its leaders regard that democracy as fragile — especially in the wake of the 2023 insurrection, which was fueled partly via social media. Accordingly, for better or worse, the country is now cracking down on speech it deems a threat to that democracy.

One can argue those laws go too far or give the government too much power to silence its opposition, said **Thiago de Aragão**, a senior associate with the Center for Strategic and International Studies who advises companies on risks in Latin America. But he said it's hard to see Musk's stand as principled, given how he has gone about it.

"It would be more understandable if he had exhausted all legal means and lost," de Aragão said. "Instead he's beginning from the end" by publicly defying the orders and even calling Moraes "a dictator" who has Brazil's president "on a leash."

That suggests Musk's real motive is to provoke a confrontation that serves his own ends, de Aragão said.

"Personally, I believe he actually wants very much for Moraes to ban [X] at least temporarily, because that would crown and legitimate his narrative" that he's "a champion of free speech."

Agency scanner

Funding shortfall forces FCC to slash monthly broadband benefits in May

By Tony Romm • Read more »

New FCC rule requires internet service providers to display fees

By Eva Dou • Read more »

Hill happenings

Children's online safety legislation gains champions in House

By Bloomberg Government • Read more »

Inside the industry

Content creators ask Meta to reverse politics limits on

Instagram, Threads

By Taylor Lorenz • **Read more »**

Meta’s Nick Clegg plays down AI’s threat to global democracy

By The Guardian • **Read more »**

GM’s Cruise robotaxis are back in Phoenix — but people are driving them

By TechCrunch • **Read more »**

AI race heats up as OpenAI, Google and Mistral release new models

By The Guardian • **Read more »**

AI disinfo detection startup Alethea raises $20 million

By Axios • **Read more »**

Competition watch

WordPress owner buys Beeper, app that enabled iMessage on Android

By Bloomberg • **Read more »**

YouTube launches new Shopping features

By TechCrunch • **Read more »**

Trending

YouTube is the most consequential technology in America

By Shira Ovide • **Read more »**

Daybook

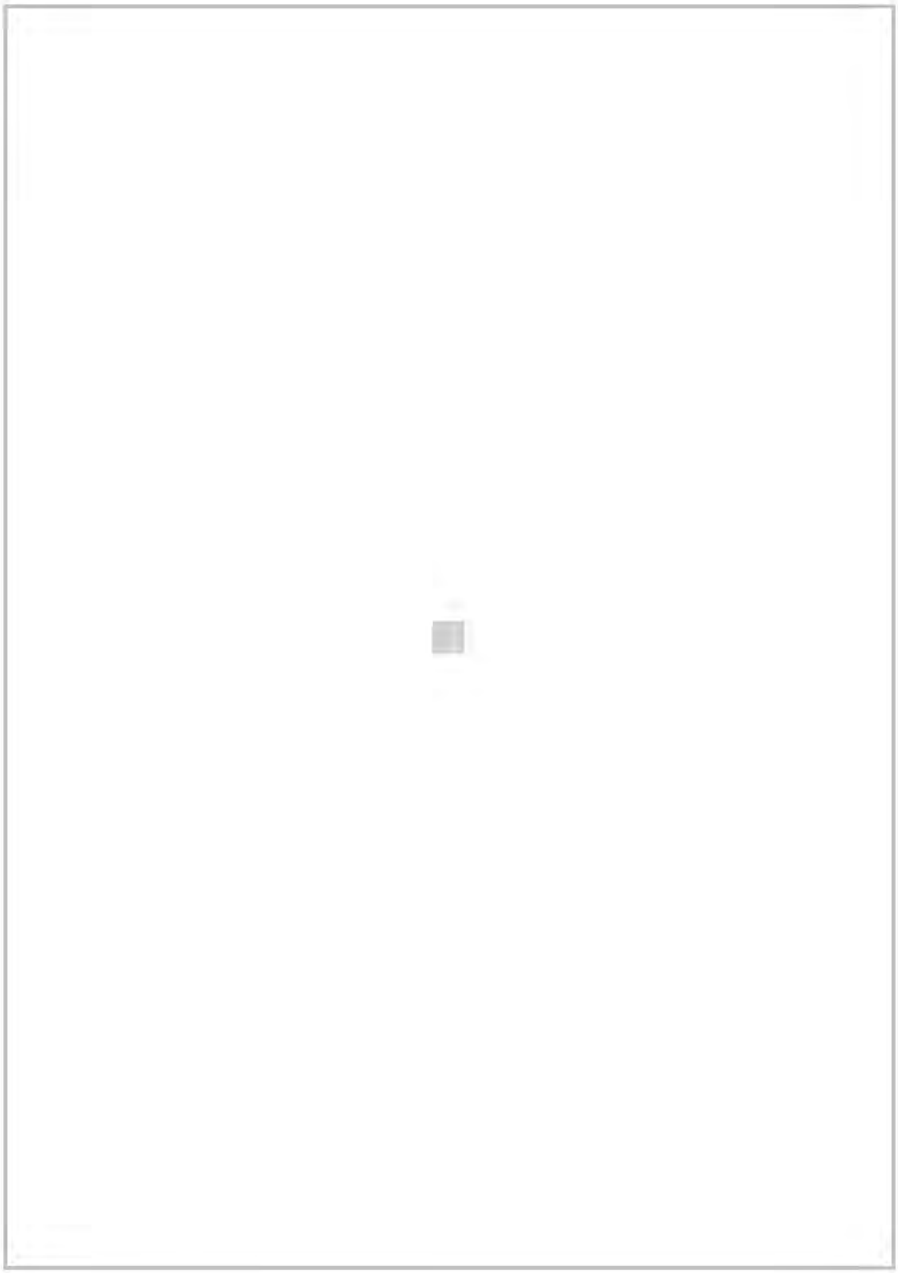
- Georgetown University Law School holds an event, “Global Perspectives on AI Governance,” today at 3 p.m.

- Washington Post Live hosts an event, “This is Climate Summit: Tipping Points,” Thursday at 9 a.m, including conversations with **John Podesta**, Maryland Gov. **Wes Moore** and environmental entrepreneurs on climate change and the role of technology in combatting it. Register here to watch.

- The Knight-Georgetown Institute hosts an event, “Burning Questions: Online Deception and Generative AI,” Thursday at 11 a.m.

- The House Energy and Commerce Committee holds a hearing, “Where Are We Now: Section 230 of the Communications Decency Act of 1996,” on Thursday at 1 p.m.

Before you log off



That's all for today — thank you so much for joining us! Make sure to tell others to subscribe to The Technology 202 here. Get in touch with Cristiano (via email or social media) and Will (via email or social media) for tips, feedback or greetings!

More intelligence for leaders.

Our 202 newsletters are your go-to source for all things Washington. Check out the rest of the suite.

An essential morning briefing for leaders in the nation's capital. Delivered weekdays.

Sign up

From: Toby Dagg
To: Julie Inman Grant; Kathryn King; s 22
Cc: s 22
Subject: Call from Meta: Update [SEC=OFFICIAL]
Date: Wednesday, 17 April 2024 12:38:47 PM
Attachments: Outlook-Email-Foot.png
Outlook-Email-Foot.png
Outlook-Email-Foot.png
Outlook-k1wh5gdi.png
Outlook-hlrerof1.png
Outlook-s2milsnw.png
Outlook-k4yhidsr.png
Outlook-t32knl0k.png

OFFICIAL

Hi all

I just had a call from s 47F s 47E(d) s 47F, s 47E(d), s 47G

s

Toby.

Toby Dagg
General Manager
Regulatory Operations Group

s 47F, s 47E(c)
s 47F, s 47E(c)
esafety.gov.au

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, present and

emerging.

From: Toby Dagg
To: Julie Inman Grant; Kathryn King; s 22
Subject: Fwd: Time to talk this afternoon? [SEC=OFFICIAL]
Date: Wednesday, 17 April 2024 6:21:36 PM
Attachments: Outlook-Email-Foot.png
Outlook-51qyfpca.png
Outlook-1w3dg3oe.png
Outlook-wmi1qav1.png
Outlook-Email-Foot.png
Outlook-znch3vzu.png
Outlook-xoivdvjw.png
Outlook-j4wpn1jl.png
Outlook-0qcsrq22.png
Outlook-ahkzduxx.png
Outlook-xuxbd0e1.png
Outlook-5aycv2xf.png
Outlook-Email-Foot.png

All, see message from X Corp. confirming they have geoblocked the material. They are not seeking an extension and regard their actions as achieving compliance.

Get Outlook for iOS

From: s 47F
Sent: Wednesday, April 17, 2024 5:49:05 PM
To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Subject: Re: Time to talk this afternoon? [SEC=OFFICIAL]

Dear Toby,

Thank you very much for your emails and for your time on the call today, it is much appreciated.

Our internal teams have actioned all the reported post URLs in the notice and each of these posts have been withheld in Australia. These actions were taken within 24 hours of our receipt of the notice.

To respectfully clarify, we are not seeking an extension of time to comply with the notice.

For more information about X's Country Withheld Content policy, please refer to our dedicated information page: https://help.twitter.com/en/rules-and-policies/post-withheld-by-country.

Our teams remain available to respond to and address any technical issues which your teams may be experiencing with our reporting forms.
Please let us know if you are continuing to face any technical issues, as we understand the teams have been able to report.

We continue to take these matters seriously and remain available to answer any questions or to connect directly as well.

Thank you again for your time today.

With kind regards,
s 47F

On Wed, Apr 17, 2024 at 2:48 PM Toby Dagg s 47E(c), s 47F @esafety.gov.au> wrote:

> **OFFICIAL**
>
> Hi s 47F
>
> Thanks for your time just now to discuss the state of play in relation to X Corp's response to the eSafety Commissioner's class 1 removal notice, issued yesterday at 2.35pm.

You noted in the call that X Corp. is seeking an extension of time to comply with the notice. Could you please provide this request to me in writing, along with the grounds for why an extension is needed, **by 5.00pm today AEST**.

In addition, you noted that X Corp.'s approach may include geo-blocking the material that is the subject of the class 1 removal notice, but that may not engage the laws of other jurisdictions.

Are you able to confirm whether the approach of geo-blocking is being employed by X Corp. in this instance in response to the class 1 removal notice?

Kind regards,

Toby.

Toby Dagg
General Manager
Regulatory Operations Group
s 47E(c), s 47F
esafety.gov.au

From: s 47F
Sent: 17 April 2024 14:45
To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Subject: Re: Time to talk this afternoon? [SEC=OFFICIAL]

yes joining now if ok?

On Wed, Apr 17, 2024 at 1:35 PM Toby Dagg s 47E(c), s 47F @esafety.gov.au> wrote:

OFFICIAL

Hi s 47F I'm available now.

Does Teams work?

https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZTQzOWQxN2EtNWVlMS00OWE0LWI4MjEtZDgwYjc5OTRiODE5%40thread.v2/0?context=%7b%22Tid%22%3a%22ba2b0386-d947-42bf-bf2d-870f776833ef%22%2c%22Oid%22%3a%22e1f4b5fe-ef8e-44fd-af3a-b6c4348fae14%22%7d

Otherwise, s 47E(c), s 47F

From: s 47F

Sent: 17 April 2024 14:33
To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Subject: Re: Time to talk this afternoon? [SEC=OFFICIAL]

Hi Toby,

Thank you. May I call? What time works for you?

Kind regards,
s 47F

s 47F
Global Government Affairs, APAC
Follow me s 47F

On Wed, 17 Apr 2024 at 11:57, Toby Dagg s 47E(c), s 47F @esafety.gov.au> wrote:

OFFICIAL

Hi s 47F

As you know, the eSafety Commissioner issued X Corp. a removal notice yesterday afternoon about 2.35pm in connection with a livestreamed video showing the terror-related stabbing attack against Bishop Emmanuel.

We received an automated response acknowledging service, but we have not heard anything further. The 24 hour compliance period for the notice expires soon and I was wanting to check your availability for a call to discuss X Corp's position.

I also wanted to take this opportunity to clarify that, under section 109 of the Online Safety Act 2021, compliance with the removal notice requires that the material is neither accessible to, nor delivered to, **any** end-users in Australia using the service.

One other thing I wanted to discuss was the experience of our investigations teams with using the law enforcement portal today. This is a channel we have employed frequently – including as recently as the weekend in response to the Bondi Junction attack -- to make notifications and flag material of concern on X.

Today, we have found our ability to use the channel obstructed by the need to solve multiple puzzles. These need to be successfully completed before any submission can be made. One eSafety investigator was led through the process a total of ten times before being able to submit the form. We are now experiencing instability with the form. Can you advise why this is the case? Given that the portal is for law enforcement and government requests the requirement for ease of use is very high.

Thanks, and hoping we can urgently talk.

Toby.

Toby Dagg

General Manager

Regulatory Operations Group

s 47E(c), s 47F

esafety.gov.au

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, present and emerging.

From: Julie Inman Grant
To: Toby Dagg; Kathryn King
Subject: Re: Follow up [SEC=OFFICIAL]
Date: Wednesday, 17 April 2024 6:27:48 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

Yes, that explains the 3500 X notifications. But billboard Chris said he was joining with free speech Australia on the AAT challenge. No mention of X Corp. do we know if they have joined this or if it's going to be a separate AAT challenge?

s 47E(d)

Get Outlook for iOS

From: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Sent: Wednesday, April 17, 2024 6:23:50 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>
Subject: Fwd: Follow up [SEC=OFFICIAL]

X Corp has challenged the Billboard Chris notice in the AAT.

Get Outlook for iOS

From: s 47E(c), s 47F
Sent: Wednesday, April 17, 2024 5:47 pm
To: s 22 @eSafety.gov.au>
Cc: s 22 @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 47F
Subject: Re: Follow up [SEC=OFFICIAL]

> You don't often get email from lstott@x.com. Learn why this is important

Dear s 22

Further to your email below, and by way of update, please be advised that our legal challenge was filed with the AAT today. A formal letter from Thomson Geer, our solicitors, will follow.

Kind regards

s 47F

On Fri, Apr 5, 2024 at 7:58 PM s 47F wrote:

> Hi s 22
>
> Thank you to you and the team for your time with us yesterday. Noted on this and we'll

be back in touch with you with an update soon.

Kind regards,
s 47F

On Fri, Apr 5, 2024 at 4:51 PM s 22 @esafety.gov.au> wrote:

OFFICIAL

Hi s 47F

Thank you for the call yesterday. As discussed, I would be grateful if you could let me know when eSafety will be formally notified by X Corp of the proposed legal proceedings proposed in the tweet from X Corp's GlobalGovermentAffairs account on 30 March 2024. As you would appreciate, there is some interest in the issue and it would be helpful if we knew X Corp.'s formal position.

Kind regards,

s 22

s 22

Executive Manager – Industry Regulation and Legal Services

Australian Government | eSafetyCommissioner

s 22

esafety.gov.au

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, present and emerging.

From: Toby Dagg
To: Julie Inman Grant; Kathryn King; Rafizadeh, Shervin; s 22
Cc: s 47F
Subject: Update on state of play -- Wakeley attack -- Thursday 18 April 2024 [SEC=OFFICIAL]
Date: Thursday, 18 April 2024 5:35:00 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png

OFFICIAL

Good evening

I wanted to provide you all with an update on eSafety's actions in relation to the Wakeley attack material at close of play, Thursday.

s 47E(d)

s 47E(d)

Happy to discuss,

Toby.

Toby Dagg
General Manager
Regulatory Operations Group

s 47E(c), s 47F

esafety.gov.au

From: Julie Inman Grant
To: DL - eSafety Commissioner and Staff
Subject: eSafety Actions in the Wake of Horrific Violence [SEC=OFFICIAL]
Date: Thursday, 18 April 2024 5:37:00 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png

OFFICIAL

Hi everyone,

Following the distressing events of the past week I wanted to acknowledge the impact that both Bondi and the second violent attack in Fairfield may have on each of us and outline the steps that eSafety has taken to help address the spread of related distressing content online.

Firstly, I want to assure you all that where you are affected by these incidents, you have our support. In addition to accessing to our Employee Assistance Program we encourage you to be in touch with your team Manager to talk through any concerns if you need. Please know that our doors are always open.

In terms of eSafety's response, our actions were once again swift. We have continued to work with scaled up operations and connecting across government to respond to the spike in harmful and distressing content circulating online. This includes 'class 1' material depicting gratuitous or offensive violence with a high degree of impact or detail. We are working closely with platforms, especially social media platforms, to quickly remove this material and remind them of our expectation that their terms of service be expeditiously enforced to protect Australians.

Unfortunately, while the majority of mainstream social media platforms have engaged with us, I was not satisfied enough was being done to protect Australians from this most extreme and gratuitous violent material circulating online.

That is why I exercised my powers under the Online Safety Act to formally compel them to remove the content. On Tuesday, I issued class 1 removal notices to X and Meta. To date, we are satisfied with the steps Meta has taken to comply. We are currently assessing the extent to which X Corp. has complied and whether further regulatory action may be required.

Following the Wakeley attack the Prime Minister spoke with media expressing his condolences, concerns and highlighting eSafety's powers to act. Minister Rowland also spoke with media and was, as always, highly supportive of our work and she has written to X Corp, reiterating the Australian Government's expectation that it cooperate with both formal and informal requests from eSafety.

There was significant media interest to which we responded by scheduling a doorstop press conference outside the Sydney office, followed by an additional media statement providing further updates later in the day.

We also reached out with:

- a letter to NSW educators, Trusted eSafety Providers (TEPs), mental health and other key stakeholders
- a letter to parliamentarians and state premiers
- social media posts on Facebook, Instagram, LinkedIn and Twitter/X covering what to do if you see distressing content, followed by additional posts highlighting the actions that eSafety is taking to address the increase in this material, and what the community can do to support this
- a special edition electronic newsletter (EDM) to all 62,000 eSafety subscribers to offer our support and advice for parents and carers to help children – many of whom are on school holidays in NSW and the ACT – make sense of these attacks.

These have resulted in really positive engagements, high EDM open rates and significant referrals to our web resources.
As the situation evolves, we will continue to engage with major platforms, as necessary, regarding their approach to responding to content of the attacks being reshared and reposted. We will employ the full suite of powers under the Online Safety Act when they are required to protect Australians from extreme violent content. This includes issuing class 1 notices to platforms providing access to this material.

The events of this week remind us that we need to work together to use our voices, to promote basic respect and a strong sense of community, both online and off. This is work I know we all strive to achieve.

My sincere thanks to all those involved in the rapid response to another horrifying event, including Strat Comms, EPI, Investigations and staff throughout eSafety. Once again you demonstrated how we can ramp up to respond to a crisis, offering much-needed support to Australians. I am so grateful for your invaluable work.

We will keep you all apprised of any major developments!

All the best,

Julie

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

From: Julie Inman Grant
To: Toby Dagg; s 22 Kathryn King
Subject: FW: Case# 0366115108: Twitter Receipt of Content Removal Request - Office of the eSafety Commissioner [ref:!00DA00K0A8.!500Vp05CksP:ref] [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]
Date: Friday, 19 April 2024 10:30:00 AM

OFFICIAL: Sensitive
Legal Privilege

Can you please send me the notice we sent to X Corp s 42 I haven't seen any of this and it will help fill in the blanks for me.

Just as an aside, I have never seen a response from a technology company to a government entity that is so rude – they have no freaking people in Australia to respond to the request. I think this gives an indication of how they are likely to take a more aggressive and perhaps vitriolic approach.

From: Twitter Support <support@twitter.com>
Sent: Friday, April 19, 2024 5:45 AM
To: Requests <Requests@eSafety.gov.au>
Subject: Case# 0366115108: Twitter Receipt of Content Removal Request - Office of the eSafety Commissioner [ref:!00DA00K0A8.!500Vp05CksP:ref]

19 April 2024

requests@esafety.gov.au

s 22
Principal Lawyer
eSafety Commissioner

Dear s 22

Re: Your letter dated 18 April 2024
Your Reference: CYR-0511323, CYR-0511326, CYR-0511327 and CYR-0511328

While we appreciate the sensitivity of this request, we respectfully note that requesting a response to be drafted outside regular Australian business hours is both unreasonable and inappropriate. Given the time in Australia that the notice was served, we have not had the opportunity to properly brief our outside counsel and seek legal advice. It is only fair and a fundamental right that we be given a proper opportunity to seek appropriate legal advice on such an important issue.

However, in light of the sensitive and urgent nature of subject matter, we will endeavour to provide a response by 3.00 pm today, 19 April, 2024.

Please confirm as a matter of urgency that eSafety is content with the above course of action.

We appreciate your patience and cooperation.

Sincerely,

X

ref:!00DA00K0A8.!500Vp05CksP:ref

From: Julie Inman Grant
To: Toby Dagg
Cc: s 22 ; Kathryn King; s 22
Subject: RE: Urgent: Request for advice re non-compliance with removal notice [AGSDMS-DMS.FID5151389] [SEC=OFFICIAL]
Date: Friday, 19 April 2024 11:26:00 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image006.png
image007.png
image008.png

OFFICIAL

I'm sure you are all over this but X Corp's policies, and whether or not they are enforcing their own policies, may be called into question. They do distinguish in their policies between "content removal" and "country withheld material." Under the X rule around "Perpetrators of Violent Attacks" of February, 2023, the policy says:

We will remove any accounts maintained by individual perpetrators of terrorist, violent extremist, or mass violent attacks, as well as any accounts glorifying the perpetrator(s), or dedicated to sharing manifestos and/or third party links where related content is hosted. We may also remove Posts disseminating manifestos or other content produced by perpetrators.

I understand through my reading of the brief that we did only ask for the URLs to be removed, not any of the accounts perpetuating the content (it would be interesting to know if when you speak to the X Corp team if any accounts have been removed, in line with their own policy).

It's interesting to note that their policy on Country Withheld Content doesn't indicate if this will apply to just harmful material or illegal material too but I think a fair reading would be that illegal content would be treated in accordance with the "Perpetrators of Violent Attacks" policy.

As discussed on the call, withhold the content is a choice or as X Corp puts it in its blog of April, 2023, it is a philosophy. It is not about technical feasibility. "Freedom of Speech, Not Reach: An update on our enforcement philosophy"

Again, what is interesting to me is that the policy says:

"While these labels will initially only apply to a set of Tweets that potentially violate our Hateful Conduct policy, we plan to expand their application to other applicable policy areas in the coming months."

There is no indication that this action has been expanded to cover illegal or violent content.

Julie

From: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Sent: Friday, April 19, 2024 10:48 AM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Cc: s 22 @eSafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>
Subject: Fw: Urgent: Request for advice re non-compliance with removal notice [AGSDMS-DMS.FID5151389] [SEC=OFFICIAL]

From: Toby Dagg
To: s 47F
Cc: Julie Inman Grant; Kathryn King; s 47F ; Rafizadeh, Shervin
Subject: As requested: email summarising actions this week and assessment of platform response [SEC=OFFICIAL]
Date: Friday, 19 April 2024 2:27:27 PM
Attachments: Outlook-Email-Foot.png
Outlook-Email-Foot.png
Outlook-Email-Foot.png
Outlook-453u1mam.png
Outlook-lyiafwpr.png
Outlook-agb2xwyv.png
Outlook-ogudqh5k.png
Outlook-davv0vu5.png
Importance: High

OFFICIAL

Hi s 47F

I have extracted the below from advice shared throughout the week with the MO and Dept:

Bondi Junction stabbings:

s 47E(d)

s 47E(d)

Wakeley stabbing:

s 47E(d)

Other actions during the week:

- a letter to NSW educators, Trusted eSafety Providers (TEPs), mental health and other key stakeholders
- a letter to parliamentarians and state premiers
- social media posts on Facebook, Instagram, LinkedIn and Twitter/X covering what to do if you see distressing content, followed by additional posts highlighting the actions that eSafety is taking to address the increase in this material, and what the community can do to support this
- a special edition electronic newsletter (EDM) to all 62,000 eSafety subscribers to offer

our support and advice for parents and carers to help children – many of whom are on school holidays in NSW and the ACT – make sense of these attacks.

The most recent information I can share is that Julie and I met at 11.30am with NSW Premier and Cabinet today s 47F) where we briefed on actions taken and limits of powers, noting no power to take action against entire accounts and no specific power to deal with hate speech. Julie also noted that she had written to Premier Minns and other premiers, and offered meeting to discuss role and powers.

I can't make any representations at all about the overall sufficiency of the platforms' response, but only what we are able to observe from our limited capacity to monitor. We cannot view activity across the entirety of platforms – this is not possible. Our concern is X, given nature of content being shared, non-compliance, and other factors, and in addition to other sites of concern such as gore sites this is where we are concentrating collective energy to support achieving compliance. Weare happy to take reports of material on Meta services and others such as TikTok and Snap and expect they will be actioned. I need to be clear that eradication/sterilisation of all material is not possible or realistic, but suppression/limitation is. More than 5 years after Christchurch, the attacker material is still in circulation online.

Toby

Toby Dagg
General Manager
Regulatory Operations Group

s 47E(c), s 47F

esafety.gov.au

From: Julie Inman Grant
To: Toby Dagg s 47F
Cc: Kathryn King; s 47F ; Rafizadeh, Shervin; s 22
Subject: RE: As requested: email summarising actions this week and assessment of platform response [SEC=OFFICIAL]
Date: Friday, 19 April 2024 3:24:00 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png

OFFICIAL

All, looping in s 22 from StratComms to tie this all together.

We have been working as fast as we can to get out further notifications to a few key gore sites and send out link deletion notices to the search engines to limit Australian access to these sites. s 47E(d)

s 47E(d)

Let us know if you have any questions or concerns.

Julie

From: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Sent: Friday, April 19, 2024 2:39 PM
To: s 47F @mo.communications.gov.au>
Cc: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 47F @MO.Communications.gov.au>; Rafizadeh, Shervin <Shervin.Rafizadeh@MO.communications.gov.au>
Subject: Re: As requested: email summarising actions this week and assessment of platform response [SEC=OFFICIAL]

OFFICIAL

Yes, likewise s 47F Thanks.

From: s 47F @mo.communications.gov.au>

Sent: 19 April 2024 14:37
To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Cc: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 47F @MO.Communications.gov.au>; Rafizadeh, Shervin <Shervin.Rafizadeh@MO.communications.gov.au>
Subject: RE: As requested: email summarising actions this week and assessment of platform response [SEC=OFFICIAL]

OFFICIAL

Grateful for your response, Toby.

Hoping you can enjoy some weekend.

Looking forward to meeting the team soon.

s 47F

OFFICIAL

From: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Sent: Friday, 19 A 27 PM
To: s 47F @mo.communications.gov.au>
Cc: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 47F @MO.Communications.gov.au>; Rafizadeh, Shervin <Shervin.Rafizadeh@MO.communications.gov.au>
Subject: As requested: email summarising actions this week and assessment of platform response [SEC=OFFICIAL]
Importance: High

OFFICIAL

Hi s 47F

I have extracted the below from advice shared throughout the week with the MO and Dept:

Bondi Junction stabbings:

- s 47E(d)
-
-
-

s 47E(d)

Wakeley stabbing:

s 47E(d)

- s 47E(d)


Other actions during the week:

- a letter to NSW educators, Trusted eSafety Providers (TEPs), mental health and other key stakeholders
- a letter to parliamentarians and state premiers
- social media posts on Facebook, Instagram, LinkedIn and Twitter/X covering what to do if you see distressing content, followed by additional posts highlighting the actions that eSafety is taking to address the increase in this material, and what the community can do to support this
- a special edition electronic newsletter (EDM) to all 62,000 eSafety subscribers to offer our support and advice for parents and carers to help children – many of whom are on school holidays in NSW and the ACT – make sense of these attacks.

The most recent information I can share is that Julie and I met at 11.30am with NSW Premier and Cabinet today s 47F) where we briefed on actions taken and limits of powers, noting no power to take action against entire accounts and no specific power to deal with hate speech. Julie also noted that she had written to Premier Minns and other premiers, and offered meeting to discuss role and powers.

I can't make any representations at all about the overall sufficiency of the platforms' response, but only what we are able to observe from our limited capacity to monitor. We cannot view activity across the entirety of platforms – this is not possible. Our concern is X, given nature of content being shared, non-compliance, and other factors, and in addition to other sites of concern such as gore sites this is where we are concentrating collective energy to support achieving compliance. Weare happy to take reports of material on Meta services and others such as TikTok and Snap and expect they will be actioned. I need to be clear that eradication/sterilisation of all material is not possible or realistic, but suppression/limitation is. More than 5 years after Christchurch, the attacker material is still in circulation online.

Toby

Toby Dagg

General Manager

Regulatory Operations Group

s 47E(c), s 47F

esafety.gov.au

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, present and emerging.

From: Julie Inman Grant
To: Kathryn King; Toby Dagg; s 22
Subject: Fwd: Update: Meta"s response to the Sydney attacks
Date: Monday, 22 April 2024 10:22:28 PM

s 47E(d)

Julie

Get Outlook for iOS

From: s 47F
Sent: Monday, April 22, 2024 8:20 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 22 s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 s 22 @esafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Cc: s 47F

Subject: Update: Meta's response to the Sydney attacks

Hi Julie,

Enclosed please see our letter with details about our response to the recent Sydney attacks.

Kind regards,

s 47F

--
Regional Director of Policy | Australia, Japan, Korea, New Zealand & Pacific Islands
M: s 47F | E: s 47F

image002.png

Meta

22 April 2024

Ms Julie Inman Grant
eSafety Commissioner
PO Box Q500, Queen Victoria Building NSW 1230

By email: s 47E(c), s 47F @eSafety.gov.au

Dear Julie

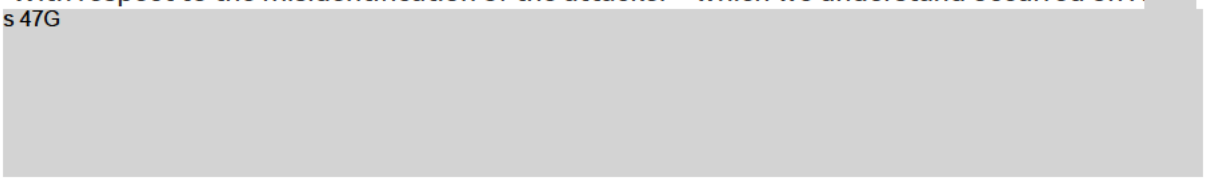
s 47G Before turning to the details, on behalf of everyone at Meta, I wanted to share my deepest sympathies with the victims and their friends and families who were impacted by these attacks. s 47G

s 47G

s 47G

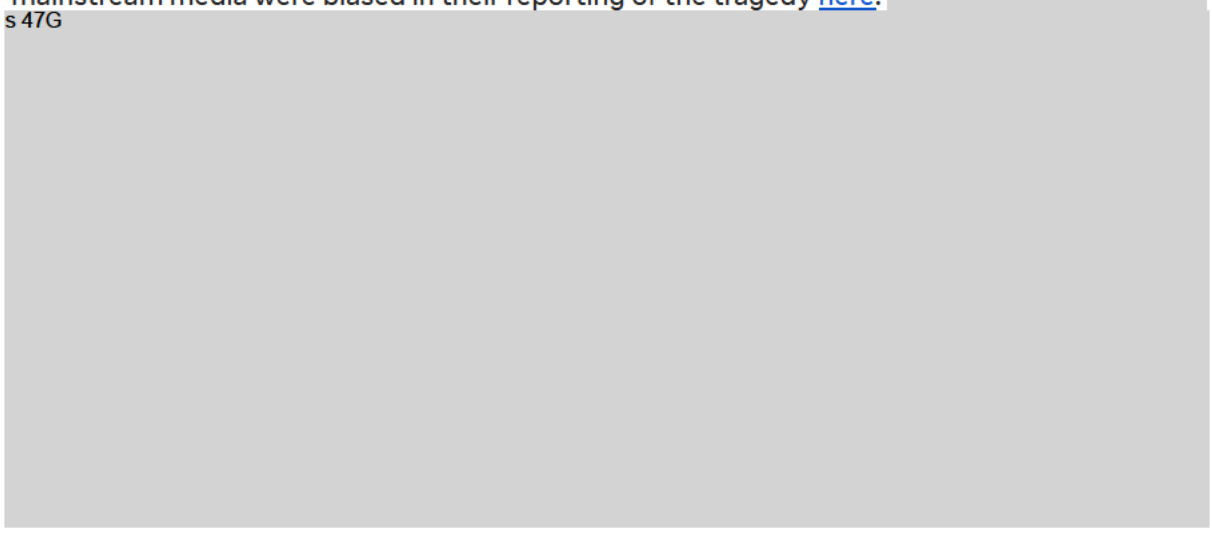
With respect to the misidentification of the attacker – which we understand occurred on X

s 47G



s 47G – the fact check from AFP was published here and the fact check from AAP is here. In addition, AAP fact checked claims that the Bondi attacks were a false flag event here and claims that mainstream media were biased in their reporting of the tragedy here. s 47G

s 47G



s 47G

Our thoughts continue to be with the victims and communities impacted by these tragedies s 47G as they respond and support people through the coming months.

s 47G

If you have any questions or would like any further information here, please do not hesitate to let us know.

Yours sincerely

s 47F

Regional Director of Policy
Australia, Japan, Korea, New Zealand & Pacific Islands

From: Julie Inman Grant
To: Toby Dagg; Kathryn King; s 22
s 22
Cc: s 22
Subject: FW: Stanford report / announcement today on NCMEC [SEC=OFFICIAL]
Date: Tuesday, 23 April 2024 2:59:00 PM

OFFICIAL

Will try to connect with WPGA but not sure that I can – we have a few things happening! We shall see if any of this cuts through the X reportage but it could have implications and reverberations for the Standards questions so just flagging with you all.

Here is the WA Post piece:

Tech

AI is about to make the online child sex abuse problem much worse

A flood of AI-generated child pornography threatens to overwhelm the nation's creaky reporting system for child exploitation, Stanford report warns.
April 22, 2024 at 11:00 p.m. Sydney Time

The nation's system for tracking down and prosecuting people who sexually exploit children online is overwhelmed and buckling, a new report finds — and artificial intelligence is about to make the problem much worse.

The Stanford Internet Observatory report takes a detailed look at the CyberTipline, a federally authorized clearinghouse for reports of online child sexual abuse material, known as CSAM. The tip line fields tens of millions of CSAM reports each year from such platforms as Facebook, Snapchat and TikTok, and forwards them to law enforcement agencies, sometimes leading to prosecutions that can bust up pedophile and sex trafficking rings.

But just 5 to 8 percent of those reports ever lead to arrests, the report said, due to a shortage of funding and resources, legal constraints, and a cascade of shortcomings in the process for reporting, prioritizing and investigating them. If those limitations aren't addressed soon, the authors warn, the system could become unworkable as the latest AI image generators unleash a deluge of sexual imagery of virtual children that is increasingly "indistinguishable from real photos of children."

"These cracks are going to become chasms in a world in which AI is generating brand-new CSAM," said Alex Stamos, a Stanford University cybersecurity expert who co-wrote the report. While computer-generated child pornography presents its own problems, he said that the bigger risk is that "AI CSAM is going to bury the actual sexual abuse content," diverting resources from actual children in need of rescue.

The report adds to a growing outcry over the proliferation of CSAM, which can ruin children's lives, and the likelihood that generative AI tools will exacerbate the problem. It comes as Congress is considering a suite of bills aimed at protecting kids online, after senators grilled tech

CEOs in a January hearing.

Among those is the Kids Online Safety Act, which would impose sweeping new requirements on tech companies to mitigate a range of potential harms to young users. Some child-safety advocates also are pushing for changes to the Section 230 liability shield for online platforms. Though their findings might seem to add urgency to that legislative push, the authors of the Stanford report focused their recommendations on bolstering the current reporting system rather than cracking down on online platforms.

“There’s lots of investment that could go into just improving the current system before you do anything that is privacy-invasive,” such as passing laws that push online platforms to scan for CSAM or requiring “back doors” for law enforcement in encrypted messaging apps, Stamos said. The former director of the Stanford Internet Observatory, Stamos also once served as security chief at Facebook and Yahoo.

The report makes the case that the 26-year-old CyberTipline, which the nonprofit National Center for Missing and Exploited Children is authorized by law to operate, is “enormously valuable” yet “not living up to its potential.”

Among the key problems outlined in the report:

- “Low-quality” reporting of CSAM by some tech companies.
- A lack of resources, both financial and technological, at NCMEC.
- Legal constraints on both NCMEC and law enforcement.
- Law enforcement’s struggles to prioritize an ever-growing mountain of reports.

Now, all of those problems are set to be compounded by an onslaught of AI-generated child sexual content. Last year, the nonprofit child-safety group Thorn reported that it is seeing a proliferation of such images online amid a “predatory arms race” on pedophile forums.

While the tech industry has developed databases for detecting known examples of CSAM, pedophiles can now use AI to generate novel ones almost instantly. That may be partly because leading AI image generators have been trained on real CSAM, as the Stanford Internet Observatory reported in December.

When online platforms become aware of CSAM, they’re required under federal law to report it to the CyberTipline for NCMEC to examine and forward to the relevant authorities. But the law doesn’t require online platforms to look for CSAM in the first place. And constitutional protections against warrantless searches restrict the ability of either the government or NCMEC to pressure tech companies into doing so.

NCMEC, meanwhile, relies largely on an overworked team of human reviewers, the report finds, partly due to limited funding and partly because restrictions on handling CSAM make it hard to use AI tools for help.

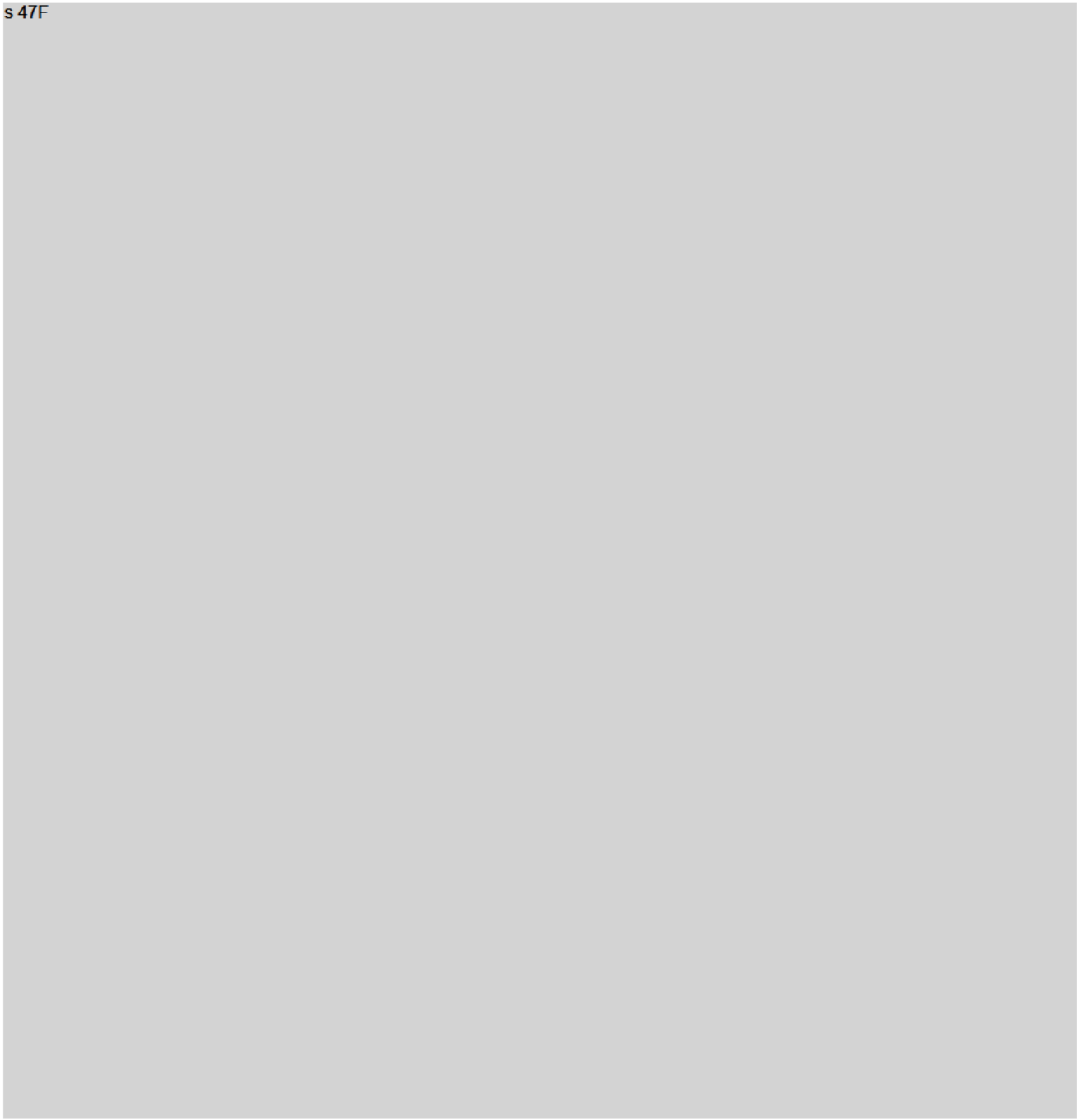
To address these issues, the report calls on Congress to increase the center's budget, clarify how tech companies can handle and report CSAM without exposing themselves to liability, and clarify the laws around AI-generated CSAM. It also calls on tech companies to invest more in detecting and carefully reporting CSAM, makes recommendations for NCMEC to improve its technology and asks law enforcement to train its officers on how to investigate CSAM reports.

In theory, tech companies could help manage the influx of AI CSAM by working to identify and differentiate it in their reports, said Riana Pfefferkorn, a Stanford Internet Observatory research scholar who co-wrote the report. But under the current system, there's "no incentive for the platform to look."

Though the Stanford report does not endorse the Kids Online Safety Act, its recommendations include several of the provisions in the Report Act, which is more narrowly focused on CSAM reporting. The Senate passed the Report Act in December, and it awaits action in the House. In a statement Monday, the Center for Missing and Exploited Children said it appreciates Stanford's "thorough consideration of the inherent challenges faced, not just by NCMEC, but by every stakeholder who plays a key role in the CyberTipline ecosystem." The organization said it looks forward to exploring the report's recommendations.

s 47F

s 47F


s 47F

From: Julie Inman Grant
To: DL - eSafety Commissioner and Staff
Subject: eSafety Commissioner Update on X Court Legal Proceedings and Regulatory Actions [SEC=OFFICIAL]
Date: Tuesday, 23 April 2024 5:48:00 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png

OFFICIAL

Dear eSafety Colleagues:

As you will have seen across the large ground swell of media over the past days, eSafety has continued to pursue action in response to X's refusal to comply with its notice to remove extreme violent video content depicting the attempted murder of an individual related to the Wakeley stabbing.

Since my last update we have moved at pace, yesterday filing against X Corp in the Federal court, and being granted, an interim injunction which compels X Corp to hide the class 1 material that was the subject of eSafety's original removal notice on 16 April. The interim injunction, which allows time for a second hearing to take place at the discretion of the court, is in place until Wednesday 24 April at 5pm AEST. Ultimately, there will also be a subsequent hearing to finalise the matter.

Journalist Clare Armstrong wrote a compelling piece on the matter which clarifies a number of key issues and I encourage everyone to take a look if you can: *Blatant falsehoods behind X's defence of Sydney terror attack posts*.

Nothing significant we achieve at eSafety is done in isolation – it is always a concerted team effort. The accomplishments thus far have been the result of the diligent and relentless work of so many across eSafety, and I could not be more proud! In particular, I would like to acknowledge s 22 , as well as our incredible GMs, Toby and Kathryn, who have provided tireless support throughout the weekend and late into last night. s 22 , our new head of Investigations is diving right in on day 2 and is already demonstrating his value!

This is truly a monumental milestone for eSafety, as we test our powers to the fullest extent. These actions demonstrate eSafety's regulatory maturity both within Australia, and on the world stage. There may be continued ups and downs, but we will continue to weather this storm, together. And, I truly believe we will be on the both the right side of history – and human decency.

Media and Government response

It's unsurprising that this issue has led to some of the highest levels of media interest that eSafety has ever experienced. There has been broad coverage both domestically and internationally which has been bolstered with overwhelming bi-partisan support and public statements including from:

- Prime Minister, Anthony Albanese
- Communications Minister, Michelle Rowland
- Opposition Leader, Peter Dutton
- Shadow Communications Minister, David Coleman
- Health Minister, Mark Butler
- Minister for the Environment and Water, Tanya Plibersek
- Government Services Minister, Bill Shorten
- NSW Premier, Chris Minns.

Some examples of their support over the last few days acknowledges the incredible work of eSafety that you all should be so proud of:

'… what the eSafety Commissioner is doing is her job to protect the interests of Australians. And the idea that someone would go to court for the right to put up violent content on a platform … shows how out of touch Mr. Musk is. Social media needs to have social responsibility with it. Mr. Musk is not showing any.' **Prime Minister, Anthony Albanese on ABC News Breakfast, 23 April**

'I think there's a bipartisan position in relation to this. ... we've seen some of the comments from Elon Musk overnight, they see the mselves above the law. And the Australian law here should apply equally in the real world as it does online.' **Opposition Leader,**

Peter Dutton, Insiders, 21 April

'… it's the precise powers of the Online Safety Act that the eSafety Commissioner is using to require these platforms to take this material down, and they have to comply with the law of Australia. It's not optional. It doesn't matter who you are. If you want to operate in Australia, you've got to play by the rules of Australia. And we back the eSafety Commissioner 100%.' **Shadow Communications Minister, David Coleman, ABC Afternoon Briefing, 22 April**

'We believe it is incredibly disappointing that Elon Musk, instead of complying with a lawful direction, has decided to make fun of it. Decency can't be dead. And I think any Australian looking at that would go, oh, come on. It's a pretty simple and straightforward request. It's a lawful request and it's one that conforms with what most Australians would think was the right and a decent thing to do.' **Assistant Treasurer and Minister for Financial Services, Stephen Jones, Radio National, 22 April**

Negative online commentary

We are well and truly being backed in!

On the flip side, you may also have seen some negative online commentary about the actions and a range of public ire against me directly. This has included Elon Musk calling me the 'Australian censorship commissar' which has led to some pretty ugly personal online sledges. I wanted to let you know that I am taking some of our own advice on building my online resilience and am managing well. This online invective is designed to belittle and intimidate but will not deter us from using our graduated and discretionary enforcement powers to see this process through. There is so much at-stake here for so many Australians.

For those of you who have reached out to me personally, thank you!! I have been very touched by your compassion and concern and this has absolutely bolstered me. I'm being incredibly well supported by my team, including Toby, Kathryn, s 22 and s 22 and all the managers and staff throughout eSafety. It is the people at eSafety that inspire me to come to work every day, even on the days that seem quite harrowing!

While it may be disheartening to see that there has also been some threatening behaviour and social media trolling of our accounts, this unfortunately comes with the territory of pushing boundaries. Fighting online abuse is absolutely what we stand for and we need to remain steadfast yet thoughtful in our resolve to continue moving forward. Our frontline staff are addressing this effectively through our enquiries channels and social media management and my thanks go to those of you who skilfully address the sometimes challenging content.

We encourage everyone to be aware of their social media accounts and public profile, and to follow our own advice to **report** and **block** menacing online behaviour. You may consider making public social media profiles private, not accept new followers that you don't know and not include your place of work as part of your social media profile or on social networking platforms not related to work, like Meta and X. The ACMA's Social Media: Acceptable Use Policy may also provide some useful information.

If you are experiencing personal abuse because of this issue please report it and don't hesitate to let your manager know if you feel unsafe or threatened. Reach out and disclose to someone you trust, including your immediate manager. Above all, look after yourselves and remember that you can access our Employee Assistance Program at any time if you require support.

Physical Safety and security

Given the high level of interest in this issue and the volume and tone of some online commentary, I want you to know that we have also liaised with the AFP around physical and personal safety. We are not aware of any heightened risk at this time but continue to be in regular contact with the ACMA and building security to ensure we are taking the necessary steps to protect eSafety staff at all times.

With this background of increased public scrutiny and debate, we recommend you be continuously vigilant and mindful of your own safety. As always, we recommend removing your government pass when you leave the building or are on public transport, being vigilant about tailgating (using your swipe card to enter/exit all points of the building and not letting others follow you in or out). If you see anything unusual or have any further concerns, please don't hesitate to notify Kathryn King and s 22

We will keep you updated as events evolve and thank you all, as always, for your ongoing support – and for the incredibly important work you do, every day!

All my best,

Julie

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

From: Julie Inman Grant
To: Toby Dagg; Kathryn King; s 22
Subject: AFR: Musk Lawyers to Fight Orders on Two Fronts [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]
Date: Wednesday, 24 April 2024 9:51:24 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
ISD Research Briefing - Moscow Terror Attack Footage and Islamic State Bodycam Video Spreads on X (25.03.24).pdf

---

OFFICIAL: Sensitive
Legal Privilege

On bureaucratic bungle and over-reach. Is it problematic that TG are backgrounding journos on their legal strategy before the court hears their arguments? The AFR piece is here:

2063447606_20250424_afr.pdf

I believe it is in the affidavit, but I do believe that it is very germane that eSafety would have the expectation that X Corp would respond to a class 1 removal request with full removal as they did with the 3 URLs of Christchurch content we reported to them a few months back and which s 22 confirmed.

Also, I attach the research analysis from ISD on the Moscow Terror Attack Footage on X. This talks about how X (and formerly Twitter) generally requires user to add the interstitial to sensitive media. But here they note that 19 OF THE 50 IDENTIFIED BYSTANDER VIDEOS SHARED ON X HAD SENSITIVE CONTENT WARNINGS PLACED ON THEM BY THE PLATFORM, REPRESENTING 38% OF THE TOTAL VIDEOS COLLECTED. The platform deleted 4 of the videos [this assumes full removal]. See this passage:

Key Findings

Graphic Bystander Footage

In the first few hours after the news of the attacks, **ISD collected 50 bystander videos spread by 48 unique accounts on X that included shots of the attackers shooting victims from afar, as well as the bodies of victims throughout the concert hall**.

These types of videos are potentially permitted under X's Sensitive Media policy if they are marked as sensitive by users when posted.

The bystander videos of the attacks on X had 16.4 million views on March 22, and were primarily spread by paid subscription users on the platform — 80% of the users that shared these prominent graphic bystander videos were X Premium users with a 'verified' blue checkmark by the platform.

19 of the 50 identified bystander videos shared on X had sensitive content warnings placed on them by the platform, representing 38% of the total videos collected. The platform deleted 4 of the videos.

48 hours after the initial bystander videos were shared on X, **views of the videos jumped by 25.8 million on March 24, culminating in a total of 42.2 million views of the bystander videos featuring dead bodies on camera, as well as the attackers firing on groups of victims in the concert hall.**

The largest share of bystander video identified on X featuring the bodies of victims and attackers firing on victims were in English (14.4 million views), followed by Spanish (1.6 million views), and French (28,000 views).

Not sure if we would be able to submit as evidence but thought it was worth flagging. Technical experts? Of course, other governments, like the European Commission, rely on ISD research and intelligence for their regulatory actions. Julie

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @esafety.gov.au

signature_4012186592

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

INITIAL BRIEFING:

MOSCOW TERROR ATTACK FOOTAGE AND ISLAMIC STATE BODYCAM VIDEO SPREADS ON X

March 25, 2024

In the immediate aftermath of an Islamic State terrorist attack in Moscow which left at least 133 people dead, ISD analysts mapped the proliferation of over 70 pieces of branded terrorist content from the group's Amaq News Agency on X, generating over 20 million views in the 48 hours after the attack. Graphic bystander footage was also readily available - much of it shared by Premium X accounts - generating over 40 million views in the aftermath of the attack, with less than 40% showing sensitive content warnings.

Summary

The Islamic State claimed a complex terrorist attack at Crocus City Hall in Russia on Friday, March 22, which left at least 133 people dead inside of a concert hall in Krasnogorsk near Moscow. Footage from the attack was shared widely across X (formerly Twitter), as well as other platforms, and detailed how the men involved in the attack methodically shot at victims inside of the concert hall. Several reports indicated that the assailants detonated a bomb prior to infiltrating the concert hall and firing on victims. Bystander video filmed at the scene was initially widely shared on X, victims could be seen throughout the videos.

The Islamic State's Amaq News Agency claimed the attack on Friday, March 22. On Saturday, March 23, Amaq provided an update to the claim, providing photographs of the attackers and a much longer, detailed read-out of the attack on the venue. This was followed by a claim by the Islamic State central media apparatus. Following the claim by the Islamic State central media apparatus, Amaq released a bodycam video of the attack from the vantage point of the attackers. The claims by Amaq and the Islamic State did not state the *wilayah*, or province (such as the group's 'Khorasan' province). US intelligence officials confirmed that the attack was conducted by the Islamic State.

The attack came two weeks after the US Embassy in Moscow released a warning on March 7, as did the United Kingdom, about a potential extremist attack targeting concerts. Over the past few months, the Islamic State Khorasan Province (ISKP) had been threatening Russia as well as involved in disrupted plots across Europe. On the same day the US Embassy in Moscow released its warning to US citizens, the Kremlin claimed to have disrupted a ISKP plot that was intended to target a synagogue. There have been 8 disrupted Islamic State plots in Russia since 2021. In September of 2022, ISKP targeted the Russian Embassy in Kabul, Afghanistan, resulting in the deaths of two staff members.

This briefing details the initial insights from both the Amaq video and the bystander footage spread on X, and the lapses in moderation which allowed its spread in English, Arabic, Spanish

and French. The briefing is focused on X due to the high number of videos shared in wake of the attacks, high view counts (according to platform metrics) and their rapid proliferation. Millions of X users were exposed to both the bystander graphic footage (often without sensitive content warnings or interstitials) and the Amaq branded video due to how the platform operates, e.g. paid 'X Premium' users have their posts shown in more timelines.

ISD is still collecting data in the aftermath of the attacks and notes false information as well as rampant Islamophobia has accompanied many of the videos shared on X in the wake of the attack. The data collected for this briefing was collected manually.

Key Findings

Graphic Bystander Footage

In the first few hours after the news of the attacks, **ISD collected 50 bystander videos spread by 48 unique accounts on X that included shots of the attackers shooting victims from afar, as well as the bodies of victims throughout the concert hall**. These types of videos are potentially permitted under X's Sensitive Media policy if they are marked as sensitive by users when posted.

The bystander videos of the attacks on X had 16.4 million views on March 22, and were primarily spread by paid subscription users on the platform — 80% of the users that shared these prominent graphic bystander videos were X Premium users with a 'verified' blue checkmark by the platform.

19 of the 50 identified bystander videos shared on X had sensitive content warnings placed on them by the platform, representing 38% of the total videos collected. The platform deleted 4 of the videos.

48 hours after the initial bystander videos were shared on X, **views of the videos jumped by 25.8 million on March 24, culminating in a total of 42.2 million views of the bystander videos featuring dead bodies on camera, as well as the attackers firing on groups of victims in the concert hall.**

The largest share of bystander video identified on X featuring the bodies of victims and attackers firing on victims were in English (14.4 million views), followed by Spanish (1.6 million views), and French (28,000 views).

Illegal Terrorist Content

Following the release of the Islamic State Amaq News Agency body camera footage captured by one of the attackers on March 23, **ISD found 73 full or edited Amaq branded videos spread by 70 unique accounts on X, which generated 22.3 million views**. Such content is illegal under the EU's Terrorism Content Online (TCO) regulation, as Amaq is an official media agency of the Islamic State, a terrorist group proscribed by the EU. The TCO explicitly points out that

terrorist content is most harmful in the first hours after its appearance, and obliges online platforms to stop the dissemination of such content as early as possible.

The most viewed full and unedited Amaq video (no blurring of the Amaq branding and includes the throat slitting of a victim on the ground) in the dataset **garnered 3.7 million views and was shared by an X Premium account in Arabic. The account purports to be a news account focused on the United States. Such examples appear to show the challenge X faces in moderating content in languages such as Arabic.**

The Amaq videos posted on X were viewed 44 million times by March 24, doubling their initial view counts in 24 hours. ISD also found only half of the Amaq videos found were deleted by March 24.

43 of the 70 unique users that posted the full or edited Amaq video on X were paid subscribers with blue checkmarks, supposedly verified as meeting the platform's eligibility requirements. This userbase includes influencers, X-based news agencies delivering content in Spanish, Arabic, and English, and Kremlin-aligned accounts. This means these 43 users could profit from the sharing of terrorist content in the wake of the attack. The X Premium system provides incentives for users to garner the most views on their content for payment by the platform via the Ads Revenue Sharing feature.

From: Julie Inman Grant
To: s 47F s 22
Cc: Toby Dagg; Kathryn King; s 22 ; Rafizadeh, Shervin; s 47F
Subject: Re: X Corp non-compliance with eSafety notices [SEC=OFFICIAL]
Date: Thursday, 25 April 2024 6:20:54 PM
Attachments: image001.png
image007.png
image009.png
image011.png
image013.png
image015.png

Hello s 47F All:

I hope you have all had a lovely and reflective ANZAC Day! A little circuit breaker after the week we have all had is welcomed.

s 47F here is our statement following the hearing last evening. https://www.esafety.gov.au/newsroom/media-releases/statement-on-federal-court-order

We will remain very circumspect in our media commentary while we prepare for the next hearing on May 10th.

Global media is definitely starting to pick this up and the Prime Minister plays a pivotal role in all of these stories. See the NYT piece here: https://www.nytimes.com/2024/04/24/technology/elon-musk-videos-x-australia-court.html?smid=nytcore-ios-share&referringSource=articleShare&sgrp=c-cb

On behalf of all of us at eSafety, we really wanted to thank you and the Prime Minister for backing us in. We are continuing to work very hard to ensure we get the best online safety outcomes for Australians!

We will certainly keep you apprised of any significant developments.

All the best, Julie

Get Outlook for iOS

From: s 47F @pm.gov.au>
Sent: Thursday, April 25, 2024 5:49:14 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 22 @esafety.gov.au>
Cc: Toby Dagg s 47E(c), s 47F @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 s 22 @ au>; s 22 @eSafety.gov.au>; Rafizadeh, Shervin <Shervin.Rafizadeh@MO.communications.gov.au>; s 47F @MO.communications.gov.au>; s 47F @MO.Communications.gov.au>; s 47F @mo.communications.gov.au>
Subject: RE: X Corp non-compliance with eSafety notices [SEC=OFFICIAL]

Hi Julie,

Thank you for this update and for the additional information.

I'd be most grateful to be kept updated with the latest from eSafety including any public statements.

Many thanks,

s 47F

s 47F | **Senior Adviser**
Office of the Prime Minister, Anthony Albanese MP
Parliament House, Canberra ACT 2600
M s 47F | E s 47F @pm.gov.au

I acknowledge the Traditional Owners of the lands and waters where I work. I pay my respect to their culture, and their elders past, present and emerging.

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Sunday, 21 April 2024 9:26 PM
To: s 22 @esafety.gov.au>; s 47F @pm.gov.au>
Cc: Toby Dagg s 47E(c), s 47F @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; Rafizadeh, Shervin

<Shervin.Rafizadeh@MO.communications.gov.au>; s 47F @MO.communications.gov.au>; s 47F s 47F @MO.Communications.gov.au>; s 47F @mo.communications.gov.au>
Subject: RE: X Corp non-compliance with eSafety notices [SEC=OFFICIAL]

OFFICIAL

Hello s 47F – I'd like to convey my thanks too – and its great to be working with you again. The question of geoblocking vs removal will be the heart of the court case and I would be very concerned about pre-empting this discussion before the court hears our arguments tomorrow. I'd also note that this action ("Country withheld Content" or geo-blocking) where violent material is concerned is not consistent with X Corp's own policies.

Here is a statement from CEO Linda Yacarrino to EU Commissioner Thierry Breton is response to a removal notice around violent material from the Israeli-Hamas conflict last October:

" For the avoidance of doubt, we strictly adhere to our policies concerning illegal content and we continue to remove illegal content including terrorist content from our platform."

We at eSafety firmly believe that they should have responded to Australia's formal removal request the same way. Happy to answer any further questions.

Julie

From: s 22 @esafety.gov.au>
Sent: Sunday, April 21, 2024 9:19 PM
To: s 47F @pm.gov.au
Cc: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 47E(c), s 47F s 47E(c), s 47F @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; Rafizadeh, Shervin <Shervin.Rafizadeh@MO.communications.gov.au>; s 47F s 47F @MO.communications.gov.au>; s 47F @MO.Communications.gov.au>; s 47F s 47F @mo.communications.gov.au>
Subject: X Corp non-compliance with eSafety notices [SEC=OFFICIAL]

OFFICIAL

Hi s 47F

s 47E(d)

Attached are our most recent talking points (developed today), which may also assist. I hope this is helpful. Please don't hesitate to contact me should you have any questions or concerns.

I note with gratitude the statements of unity that the Prime Minister and other Ministers have added to the public conversation over the last couple of days. These have been enormously helpful in presenting a cohesive response.

Best regards,

s 22

s 22

Executive Manager
Strategic Communications
eSafety Commissioner

s 22
EA: s 22 @esafety.gov.au | s 22

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.

From: Julie Inman Grant
To: s 22
Cc: Toby Dagg
Subject: Our friend AI Gary is leaving X Corp [SEC=UNOFFICIAL]
Date: Monday, 29 April 2024 8:05:54 PM

---

https://x.com/garymarcus/status/1784258933961732169?s=12&t=LKaPiNL33rLi-iL-F-AZVA

PS Toby, they managed to put up an interstitial!!!
Get Outlook for iOS

From: Julie Inman Grant
To: s 22 Toby Dagg; s 22 Kathryn King
Cc: s 22
Subject: RE: Notices of two applications for review received by the AAT [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]
Date: Thursday, 2 May 2024 9:14:40 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

OFFICIAL: Sensitive
Legal Privilege

Well, let's strap ourselves in here! We will have a very heavy legal and regulatory plate over the coming months and given transitions, Kathryn, Toby and I will talk about what we need to do to appropriately staff up and cover a few major gaps in response to what I think we can fairly call an "all hands on deck moment."

s 47E(d)

Australia's online safety regulator has drawn a line in the sand for X. Will she prevail? | Australia news | The Guardian

"The regulator has also used its more graduated powers to have URLs removed from search results, but it has never used its power to have an app removed from app stores.

Most of the time, the platforms comply or eSafety does not pursue the matter further.

At least, that was the case until Musk took over X at the end of 2022.

The chair of Digital Rights Watch, Lizzie O'Shea, says eSafety was largely dependent upon cooperation with tech platforms, but that has shifted.

"The recent dispute with X poses a challenge as the company has not only resisted cooperation but is now challenging the basis for these laws, demonstrating that they appear to have little concern for maintaining a social licence to operate, at least insofar as regulators are concerned," she says.

"The eSafety commissioner has a difficult and important job, but her powers are also limited and have to be balanced against other concerns, whether they be practical or human rights ones."

eSafety and X are now involved in at least three legal cases in Australia over notices issued to the company. The stabbing attack notice is slated as the first to be heard later this month."

From: s 22 @eSafety.gov.au>
Sent: Wednesday, May 1, 2024 2:48 PM
To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>; Julie Inman Grant
s 47E(c), s 47F @eSafety.gov.au>; s 22 @eSafety.gov.au>
Cc: s 22 @eSafety.gov.au>; s 22
s 22 @eSafety.gov.au>; s 22 @esafety.gov.au>; s 22
s 22 @esafety.gov.au>; s 22
s 22 @esafety.gov.au>; s 22 @eSafety.gov.au>;
s 22 @esafety.gov.au>; s 22
s 22 @eSafety.gov.au>; s 22 @esafety.gov.au>
Subject: Notices of two applications for review received by the AAT [SEC=OFFICIAL]

OFFICIAL

Hi Julie and Toby

The AAT has sent through this afternoon two notices of application for review lodged by X Corp against eSafety decisions.

- eSafety's section 88 removal notice to X Corp in relation to the adult cyber abuse directed at s 47F
- eSafety's notice under section 56(2) to X Corp seeking information on X Corp's treatment of TVE in connection with the BOSE.

s 47E(d) We have 28 days to lodge the documents required by the AAT.
s 22 will manage the first case and s 22 the second (with help from their team).

s 47E(d)

s 47E(d)

At this stage, only limited information is available publicly via the AAT's eCase search – see https://online.aat.gov.au/eCaseSearch/Home/Results?ApplicationType=REV&SurnameOrgName=X%20Corp. s 47E(d)

Thanks

s 22

s 22
Executive Manager – Industry Regulation and Legal Services

Australian Government | eSafetyCommissioner

s 22
esafety.gov.au

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, present and emerging.

From: Toby Dagg
To: Julie Inman Grant
Subject: Re: CyAN blog post in defense of eSafety Commissioner [SEC=OFFICIAL]
Date: Friday, 3 May 2024 8:55:54 AM
Attachments: image001.png

OFFICIAL

Wow, what a clear, straightforward and effective repudiation of the misinformation. Very generous of CyAN, and a welcome reminder of the leadership you've demonstrated, Julie.

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: 03 May 2024 08:50
To: s 47F Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Cc: s 47F
Subject: RE: CyAN blog post in defense of eSafety Commissioner [SEC=OFFICIAL]

OFFICIAL

s 47F : Thank you so much for putting this compelling blog. Not only does it hit all the right points and the right notes, this is precisely the kind of expert support we need right now. It is amazing how few people understand how the Internet and content moderation work – there is no French Internet, there is no Australian Internet, there is a global internet, with most of these harmful posts be hosted on servers in California. But you understand all that! I just wanted to thank you all – your support means the world!

Many thanks, Julie

From: s 47F
Sent: Friday, May 3, 2024 12:24 AM
To: Julie Inman Grant; Toby Dagg
Cc: s 47F
Subject: CyAN blog post in defense of eSafety Commissioner

Certaines personnes qui ont reçu ce courrier ne reçoivent pas souvent du courrier de la part de s 47F . Découvrez pourquoi cela est important

Dear Julie and Toby,

The Cybersecurity Advisors Network (CyAN) has published a blog post today in support of your work against hate online.

- Our blog post is here: https://cybersecurityadvisors.network/2024/05/02/in-defense-of-esafety-upholding-democratic-processes-in-the-digital-age/
- LinkedIn post is here:

https://www.linkedin.com/feed/update/urn:li:activity:7191797837859303427

CyAN is a community of cybersecurity and trust & safety professionals that I co-founded in 2015, with 80 members in Europe, Australia and also in the USA.

This blog post has been led by our board member s 47F in our Australian chapter, our member s 47F, and reviewed by our board.

We hope this small contribution will be of some value to you, let us know if we could do more,

Best regards,

s 47F
President
Cybersecurity Advisors Network (CyAN)
s 47F

From: Julie Inman Grant
To: s 22 s 22
Cc: Toby Dagg; Kathryn King
Subject: Geoblocking insight [SEC=SENSITIVE]
Date: Friday, 3 May 2024 1:44:24 PM

Hi from the Canberra airport! Great seeing you Sunday/Monday — so glad we got a chance to connect. Meetings over the last few days have all been positive, I think. Lots more to do on the code and other matters, but I think we're moving in the right direction.

Happy to connect on the X stuff once I'm back in the US (in a private capacity, not as a representative of Match, obviously). But here are a few initial notes re: the items you flagged:

* Geo-blocking, i.e. Country Withheld Content (CWC), has always been about illegal content *only*, not other forms of problematic material. In the "old days," CWC was applied by a different part of T&S - the Legal Policy org (under s 47F, during your time at the company), rather than the other parts of T&S or User Services. It was designed specifically for cases where Twitter received demands to remove content that a jurisdiction believed to be illegal under local law, and where Twitter found that the content did not violate the company's TOS.
* re: geoblocking and the determination of location — Twitter uses a combination of IP and GPS/device signal to try to "guess" a user's location. Those techniques are standard across the industry (i.e. Meta do the same things), and as you know are circumventable via VPNs. There's not much anyone can really do to improve the effectiveness of a country-specific block.
* As a technical matter, Twitter's enforcement abilities here, from least severe to most, are: (1) add a warning interstitial atop the content that it may be graphic but keep the content available; (2) country-withhold the content only in Australia such that users accessing Twitter from within AU (based on geolocation as specified above) see a message saying it has been restricted by legal demand; (3) globally country-withhold the content such that any viewer in any country sees a message saying it has been restricted by legal demand (more on this below); (4) remove the content globally under TOS such that any viewer in any country sees a message saying the content violated the Twitter Rules.
* re: (3) above - global CWC is *not* something Twitter does commonly, but it is something the company has the technical ability to do. They've deployed it re: content and accounts in Brazil based on continual escalation of court cases. There is precedent here, and the technical ability to do so, but it's quite rare. The argument is that global country-withholding is overreaching, because regulators in country X should not have the right to limit what people in country Y see.
* The absurdity of this case, in my estimation, is that the content you are requesting removal of *does in fact violate Twitter's global TOS*. That's obviously not my call anymore - but under the rules we had in place pre-Nov 2022 (and which I understand to still be in place today), I can say with near certainty that the content in question would have been globally removed (NOT CWC'd) under Twitter's TOS.

Get Outlook for iOS

From: Toby Dagg
To: s 22 Julie Inman Grant; s 22
Cc: s 22 ; Kathryn King; s 22
Subject: Re: Contact with X [SEC=OFFICIAL]
Date: Friday, 3 May 2024 7:58:42 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

Hi s 22

Yes, that is correct – the class 1 designation was reached because the material depicts real crime and violence with a high degree of impact, with that impact arguably heightened further by the fact that the attack on Bishop Emmanuel was designated by NSW Police as terror-related.

But this brief (thanks, s 22 – great work) does go to show how prepared X is to take removal action, and that it does so. Useful, I would hope, to at least demonstrate that the company has committed to *removal* as a response to policy violations.

TD.

From: s 22 @eSafety.gov.au>
Sent: 03 May 2024 19:49
To: Julie Inman s 47E(c), s 47F @eSafety.gov.au>; s 22
s 22 @esafety.gov.au>
Cc: s 22 @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>;
s 22 @esafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>;
s 22 @eSafety.gov.au>; s 22 @esafety.gov.au>;
s 22 @eSafety.gov.au>
Subject: RE: Contact with X [SEC=OFFICIAL]

OFFICIAL

Thank you Julie and s 22

s 42

Thanks

s 22

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Friday, May 3, 2024 5:41 PM
To: s 22 esafety.gov.au>
Cc: s 22 @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 @esafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 s 22 @esafety.gov.au>
Subject: RE: Contact with X [SEC=OFFICIAL]

OFFICIAL

This is really, really excellent! Exactly what I had in mind. Such great – and quick – work, s 22 I may add a few things as I go. I can see you can click through to the Annextures but I wonder if it makes sense to also have a version that is one document (with page breaks) so that it can be easily skimmed without clicking through.

I also mentioned today the 2023 GIFCT Report on Borderline Content. Here is the key intro:

"Borderline content can be conceived of in two ways; (1) either as content usually protected by free speech parameters in a democratic environment, but inappropriate in public forums ie. "borderline illegal", or "lawful but awful", or (2) as content that brushes up against a platform's policies for violating content ie. "borderline violative" but is not clearly violating a policy.

It is broadly agreed that although borderline content is not technically illegal, it still has the potential to cause harm. Subsequently, there is pressure for tech companies to better understand and take appropriate action on this type of content, whether that is by removing it, taking other moderation actions, or ensuring it does not receive undue algorithmic optimisation reaching mass audiences. While democratic governments have deemed that certain segments of speech should be legally protected, tech companies have recognized the harms that can arise from speech that is legal but problematic and harmful in the context of a particular public debate. Tech platforms therefore largely address any 'borderline illegal' terrorist and violent extremist content (TVEC) through their specific terrorist and violent extremist or dangerous organisation policies."

I haven't gone deeper on the GIFCT and Tech Against Terrorism sites but getting a primer on how content moderation generally works around this content so that we can really establish the

"industry standard" response is always helpful.

Thanks for this excellent work! Julie

From: s 22 @esafety.gov.au>
Sent: Friday, May 3, 2024 5:24 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Cc: s 22 @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 @esafety.gov.au>
Subject: RE: Contact with X [SEC=OFFICIAL]

OFFICIAL

Hi Julie

With thanks to s 22 sharing the draft brief on international approaches and commentary. We will continue to search for third party commentary next week. But please let us know if this aligns with what you were after.

Thanks
s 22

s 22
Executive Manager
Strategy, Engagement and Research
eSafety Commissioner

s 22
esafety.gov.au

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Friday, May 3, 2024 1:53 PM
To: s 22 @esafety.gov.au>
Cc: s 22 @esafety.gov.au>
Subject: Fwd: Contact with X [SEC=OFFICIAL]

We are getting feedback from AGS on what they need for the hearing - on Monday - but getting guidance.

Get Outlook for iOS

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Friday, May 3, 2024 8:20 AM

To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>
Subject: Fwd: Contact with X [SEC=OFFICIAL]

s 47E(d)

s 47E(d)

Get Outlook for iOS

From: s 47F @dfat.gov.au>
Sent: Thursday, May 2, 2024 11:05 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Subject: Contact with X [SEC=OFFICIAL]

OFFICIAL

Hi Julie, Toby,

s 47E(d)

s 47F

s 47F
Ambassador
Cyber Affairs and Critical Technology
Department of Foreign Affairs and Trade
P: s 47F | M: s 47F | E: s 47F @dfat.gov.au

EA: s 47F | Ph: s 47F M: s 47F
E: s 47F @dfat.gov.au

From: Julie Inman Grant
To: s 22 Toby Dagg; s 22
Cc: s 22 ; Kathryn King; s 22
Subject: RE: Contact with X [SEC=OFFICIAL]
Date: Monday, 6 May 2024 6:05:17 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

OFFICIAL

This is excellent – particularly the TAT, Christchurch Call and X Corp's own statements about why they remove this content. The DSA transparency report data is compelling as well – again indicating "global content removal" is standard operating procedure. s 47E(d)

Nicely done s 22 and s 22 – thanks so much! Julie

From: s 22 @esafety.gov.au>
Sent: Monday, May 6, 2024 3:54 PM
To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Cc: s 22 @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 @esafety.gov.au>; s 22 s 22 @eSafety.gov.au>; s 22 s 22 @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>
Subject: RE: Contact with X [SEC=OFFICIAL]

OFFICIAL

Hi all,

Again, with thanks to s 22 , updated brief here brief, incorporating both Julie and s 22 feedback, and BOSE team have reviewed the new content under 'common TVEC moderation approaches.'

Thanks
s 22

s 22
Executive Manager
Strategy, Engagement and Research
eSafety Commissioner

s 22
esafety.gov.au

From: Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Sent: Friday, May 3, 2024 7:59 PM
To: s 22 @eSafety.gov.au>; Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 22 @esafety.gov.au>
Cc: s 22 @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 @esafety.gov.au>; s 22 s 22 @eSafety.gov.au>; s 22 s 22 @esafety.gov.au>; s 22 @eSafety.gov.au>
Subject: Re: Contact with X [SEC=OFFICIAL]

OFFICIAL

Hi s 22

Yes, that is correct – the class 1 designation was reached because the material depicts real crime and violence with a high degree of impact, with that impact arguably heightened further by the fact that the attack on Bishop Emmanuel was designated by NSW Police as terror-related.

But this brief (thanks, s 22 – great work) does go to show how prepared X is to take removal action, and that it does so. Useful, I would hope, to at least demonstrate that the company has committed to *removal* as a response to policy violations.

TD.

From: s 22 @eSafety.gov.au>
Sent: 03 May 2024 19:49
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 22 s 22 @esafety.gov.au>
Cc: s 22 @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 @esafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @esafety.gov.au>; s 22 @eSafety.gov.au>
Subject: RE: Contact with X [SEC=OFFICIAL]

OFFICIAL

Thank you Julie and s 22

s 42

s 42

Thanks

s 22

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Friday, May 3, 2024 5:41 PM
To: s 22 @esafety.gov.au>
Cc: s 22 @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 @esafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 s 22 @esafety.gov.au>
Subject: RE: Contact with X [SEC=OFFICIAL]

OFFICIAL

This is really, really excellent! Exactly what I had in mind. Such great – and quick – work, s 22 I may add a few things as I go. I can see you can click through to the Annextures but I wonder if it makes sense to also have a version that is one document (with page breaks) so that it can be easily skimmed without clicking through.

I also mentioned today the 2023 GIFCT Report on Borderline Content. Here is the key intro:

"Borderline content can be conceived of in two ways; (1) either as content usually protected by free speech parameters in a democratic environment, but inappropriate in public forums ie. "borderline illegal", or "lawful but awful", or (2) as content that brushes up against a platform's policies for violating content ie. "borderline violative" but is not clearly violating a policy.

It is broadly agreed that although borderline content is not technically illegal, it still has the potential to cause harm. Subsequently, there is pressure for tech companies to better understand and take appropriate action on this type of content, whether that is by removing it, taking other moderation actions, or ensuring it does not receive undue algorithmic optimisation reaching mass audiences. While democratic governments have deemed that certain segments of speech should be legally protected, tech companies have recognized the harms that can arise from speech that is legal but problematic and harmful

in the context of a particular public debate. Tech platforms therefore largely address any 'borderline illegal' terrorist and violent extremist content (TVEC) through their specific terrorist and violent extremist or dangerous organisation policies."

I haven't gone deeper on the GIFCT and Tech Against Terrorism sites but getting a primer on how content moderation generally works around this content so that we can really establish the "industry standard" response is always helpful.

Thanks for this excellent work! Julie

From: s 22 @esafety.gov.au>
Sent: Friday, May 3, 2024 5:24 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Cc: s 22 @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>; s 22 @esafety.gov.au>
Subject: RE: Contact with X [SEC=OFFICIAL]

OFFICIAL

Hi Julie

With thanks to s 22 sharing the draft brief on international approaches and commentary. We will continue to search for third party commentary next week. But please let us know if this aligns with what you were after.

Thanks
s 22

s 22
Executive Manager
Strategy, Engagement and Research
eSafety Commissioner

s 22
esafety.gov.au

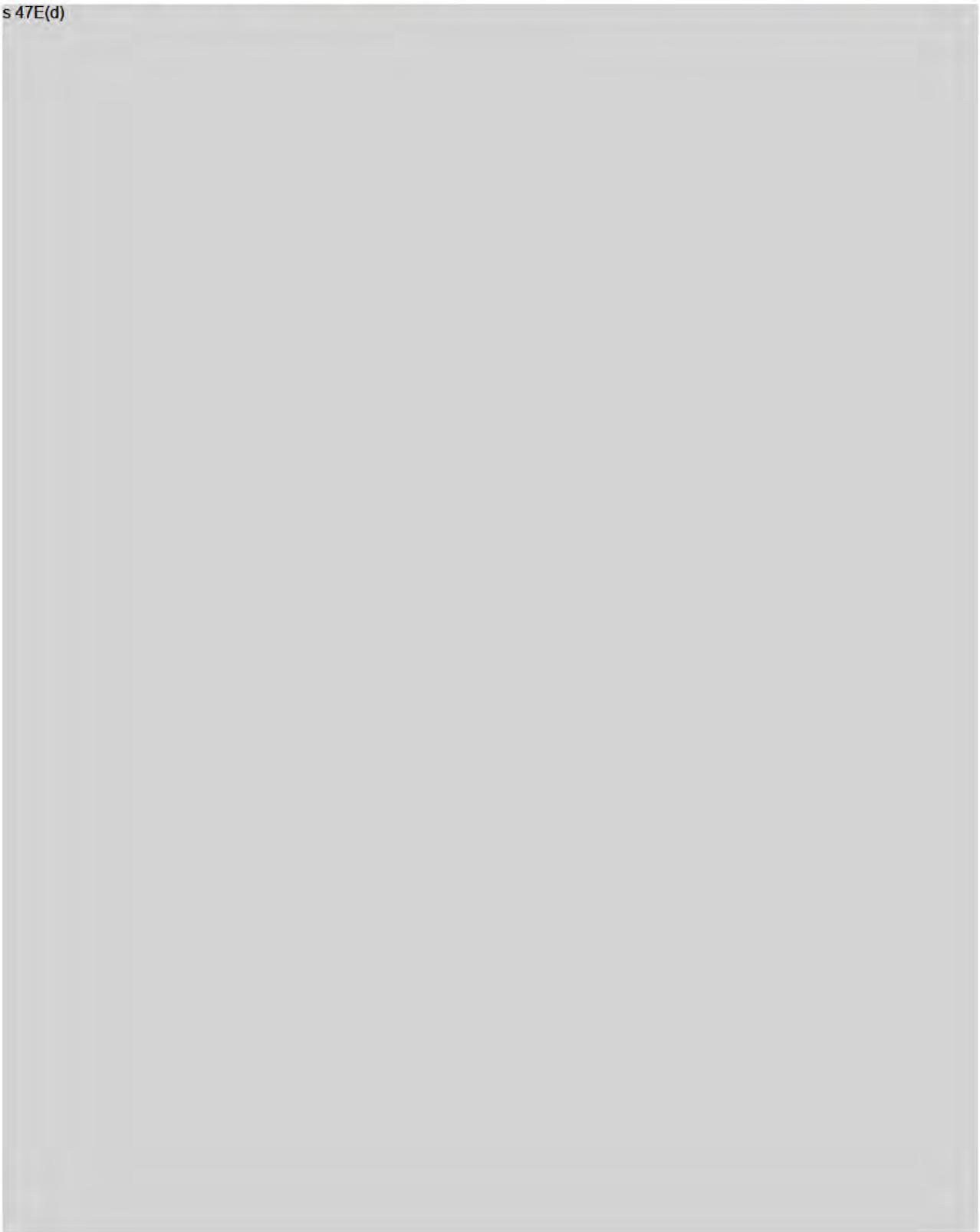
From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Friday, May 3, 2024 1:53 PM
To: s 22 @esafety.gov.au>
Cc: s 22 @esafety.gov.au>
Subject: Fwd: Contact with X [SEC=OFFICIAL]

We are getting feedback from AGS on what they need for the hearing - on Monday - but getting guidance.

Get Outlook for iOS

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Friday, May 3, 2024 8:20 AM
To: Toby Dagg s 47E(c), s 47F @esafety.gov.au>; Kathryn King s 47E(c), s 47F @eSafety.gov.au>
Subject: Fwd: Contact with X [SEC=OFFICIAL]

s 47E(d)



s 47E(d)

[redacted]

Get Outlook for iOS

From: s 47F [redacted] @dfat.gov.au>
Sent: Thursday, May 2, 2024 11:05 PM
To: Julie Inman Grant s 47E(c), s 47F [redacted] @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F [redacted] @esafety.gov.au>
Subject: Contact with X [SEC=OFFICIAL]

OFFICIAL

Hi Julie, Toby,

s 47E(d)

[redacted]

s 47E(d)

s 47F

s 47F
Ambassador
Cyber Affairs and Critical Technology
Department of Foreign Affairs and Trade
P: s 47F | M: s 47F | E: s 47F @dfat.gov.au

EA: s 47F | Ph: s 47F M: s 47F
E: s 47F @dfat.gov.au

From: Julie Inman Grant
To: s 22 Toby Dagg; Kathryn King; s 22
Cc: s 22
Subject: RE: Correspondence from ACMA Deputy Chair Creina Chapman - response to harms from mis- and disinformation [SEC=OFFICIAL]
Date: Tuesday, 7 May 2024 8:13:26 AM
Attachments: image001.png
image002.png
image003.png
image004.png

OFFICIAL

s 47E(d)

From: s 22 @esafety.gov.au>
Sent: Tuesday, May 7, 2024 8:02 AM
To: Julie Inman Grant; s 47E(c), s 47F @eSafety.gov.au; Toby Dagg; s 47E(c), s 47F @esafety.gov.au; Kathryn King; s 47E(c), s 47F @eSafety.gov.au; s 22 @eSafety.gov.au; s 22 @eSafety.gov.au; s 22 @eSafety.gov.au; s 22 @eSafety.gov.au>
Subject: RE: Correspondence from ACMA Deputy Chair Creina Chapman - response to harms from mis- and disinformation [SEC=OFFICIAL]

OFFICIAL

Good Morning Julie,

s 47E(d)

s

From: Julie Inman Grant; s 47E(c), s 47F @eSafety.gov.au>
Sent: Monday, May 6, 2024 6:14 PM
To: Toby Dagg; s 47E(c), s 47F @esafety.gov.au>; Kathryn King; s 47E(c), s 47F @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 @esafety.gov.au>
Subject: FW: Correspondence from ACMA Deputy Chair Creina Chapman - response to harms from mis- and disinformation [SEC=OFFICIAL]
Importance: High

OFFICIAL

Hi, This is interesting. Creina Chapman wrote to s 47F of YouTube about mis and disinformation around the Wakeley Stabbing incident. You'll see s 47F has copied me and provided valuable information about YouTube's action in terms of all the steps they've taken to remove the Wakeley video content.

s 47E(d)

Julie

From: s 47F @google.com>
Sent: Monday, May 6, 2024 5:51 PM
To: Misinformation <misinformation@acma.gov.au>
Cc: Creina Chapman and Assistan s 47F @acma.gov.au>; s 47F @infrastructure.gov.au; s 47F @digi.org.au>; Julie Inman Gran s 47E(c), s 47F @eSafety.gov.au>
Subject: Re: Correspondence from ACMA Deputy Chair Creina Chapman - response to harms from mis- and disinformation [SEC=OFFICIAL]

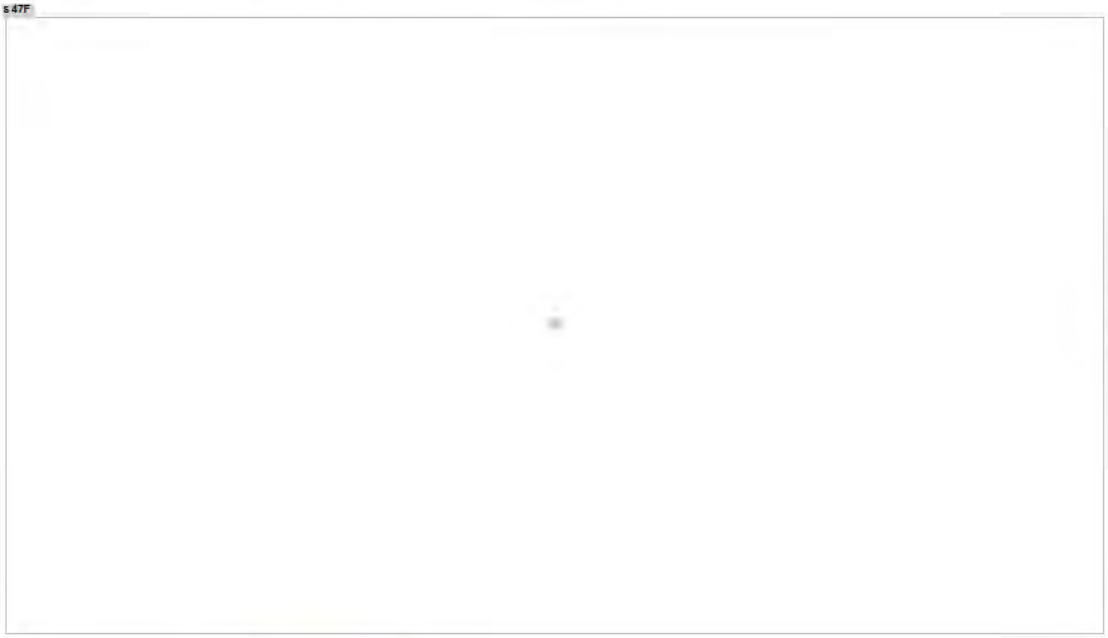
Dear s 47F

Please find attached Google's response to ACMA Deputy Chair Creina Chapman. Thank you for allowing us additional time to respond.

We have cc'd the eSafety Commissioner on this email given our response touches on matters within her area of responsibility.

Kind regards,

s 47F



s 47F
YouTube
Government Affairs and Public Policy - Australia and New Zealand
s 47F

On Thu, Apr 18, 2024 at 4:12 PM Misinformation <misinformation@acma.gov.au> wrote:

Dear s 47F

Please find attached correspondence from ACMA Deputy Chair Creina Chapman.

Regards,
s 47F
Senior Regulatory Officer
Disinformation and Platforms
Australian Communications and Media Authority

s 47F
s 47F @acma.gov.au
acma.gov.au

The ACMA acknowledges First Nations peoples as the Traditional Owners and Custodians of Australia. We respect and celebrate First Nations peoples as the original storytellers and content creators of the lands on which we work and honour the enduring strength and commitment of Aboriginal and Torres Strait Islander peoples to the land, waters and their communities. We pay our respects to Elders past, present, and emerging.

From: Julie Inman Grant
To: Toby Dagg; Kathryn King; s 22 ; s 22
Subject: Jewish Association accused of 'incitement to violence' https://www.theaustrali
Date: Thursday, 9 May 2024 7:07:24 AM

Note also that s 47F is asking NSWPol to use 474.17 to target X and social media users who spread the misinformation and "criminal defamation" that he was the Bondi killer.

Jewish Association accused of 'incitement to violence'
https://www.theaustralian.com.au/nation/muslim-organisation-accuses-australian-jewish-association-of-incitement-to-violence/news-story/ecf61628d4be0acb5bf4720b26046aae

Get Outlook for iOS

From: Julie Inman Grant
To: Toby Dagg; Kathryn King; s 22
Subject: NGO Suing X over CSAM & trafficking [SEC=UNOFFICIAL]
Date: Saturday, 11 May 2024 9:06:39 AM

---

https://www.linkedin.com/posts/dawn-hawkins-84575917_x-twitter-kosa-activity-7194682444069883904-X-Y5?utm_source=share&utm_medium=member_ios

Get Outlook for iOS

From: Julie Inman Grant
To: DL - eSafety Commissioner and Staff
Subject: eSafety Staff Update [SEC=OFFICIAL]
Date: Monday, 13 May 2024 5:30:00 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png

OFFICIAL

Dear eSafety Colleagues:

As you may know, the case against X Corp in the Federal Court has moved forward, and we expect more interesting developments to come.

On 22 April, the Federal Court granted an interim injunction requiring X Corp to immediately hide Class 1 material on X that was subject to eSafety's removal notice of 16 April 2024. On 24 April, the Federal Court granted a further interim injunction and this was in effect until the court hearing held last Friday 10 May with the injunction extended again until today.

This morning the Federal Court did not grant the eSafety Commissioner's application to extend the injunction further. The matter will return to Court for a case management hearing on Wednesday, 15 May 2024 at 9:30am. You can read eSafety's statement on the website.

You can also read about other Federal Court proceedings involving eSafety at www.esafety.gov.au, which is a new addition to our website.

Thank you

I have said this before – and it bears repeating – that our work on this case has only been possible with the tireless effort of teams across eSafety. I want to call out the exceptional, and ongoing, work of our Legal, Strategic Communications and Investigations teams amongst so many others, as well as our Managers, EMs and General Managers, Kathryn King and Toby Dagg.

The Senior Executive Group appreciates the support given by you all and we want to assure those working on the matter that you have our support in return. This has been a mammoth task and I am truly grateful that we have a cohesive team of such high calibre.

I would like to recognise Toby, in particular, for his laser-sharp focus on the breadth of issues we have needed to prepare for and address through very detailed investigations and affadavits.

The quality of our work is recognised more broadly also and we are honoured this week to have a visit from the Minister for Communications the Hon Michelle Rowland who will be visiting our Sydney office on **Friday, 17 May**. All Sydney staff, and those visiting from Melbourne and Canberra, are encouraged to work from the office on the day and take the opportunity to speak with our Minister during a catered morning tea at the Level 5 Kitchen between 11.30am-12pm. The Minister has been a tremendous support to all of us and we would really appreciate a visible show of support, in kind!

Speaking of Support

As there has been elevated media and public interest in this case and higher levels of online commentary throughout this process, please be mindful of looking at or engaging with negative or harmful online discourse. Should you experience negative or distressing interactions online please do raise these with your Executive Manager or Manager – our doors are always open. Above all, look after yourselves and remember that you can access the Employee Assistance Program at any time if you require support.

As I noted in an earlier email, we also ask that you continue to be mindful of your personal safety and security at this time. If you have any physical safety concerns, please do not take any unnecessary risks and contact Kathryn King or s 22

Given the high workload across many teams at present we will postpone our May All staff meeting for now and will look to set this up following Senate Estimates, which we anticipate will be particularly spicy this time around!

We have been limited about what we have been able to share about the case but will make a concerted effort to share what we can, when we can as things progress. We must continue to stay focused on all of the other mission-critical streams of work we have underway.

Once again, thank you for your support and essential work to help keep Australians safer online. I am constantly reminded by

others that the work we are doing is ground-breaking – and we should never lose sight of that!

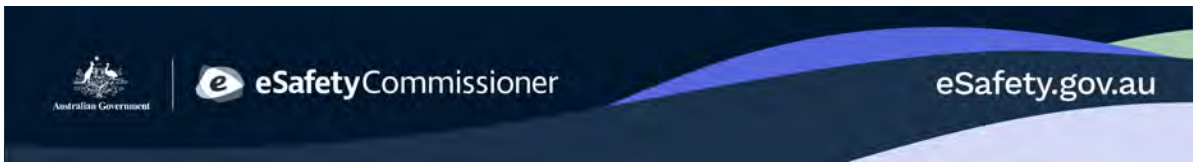
All the best.

Julie

Julie Inman Grant
Commissioner

s 47E(c), s 47F

Executive Assistant: s 22 @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.

From: Julie Inman Grant in Teams
To: Toby Dagg
Subject: Julie sent a message
Date: Monday, 13 May 2024 11:02:55 PM

Hi,

Your team-mates are trying to reach you in **Microsoft Teams**.

Julie sent a message in chat with Julie + 2

[Image] Press release from the Coalition Government on the OSA 2021...

Reply in Teams

Install Microsoft Teams now

☐ iOS ☐ Android

From: Julie Inman Grant
To: Zoe Robinson; Hannah Tonkin; James Cockayne; s 22 ; Toby Dagg
Cc: s 47F
Subject: RE: Dates for CBA meeting [SEC=OFFICIAL]
Date: Thursday, 16 May 2024 7:19:13 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

OFFICIAL

Zoe, all. s 22 who runs our regulatory branch will likely back me up if I'm not available – the combination of the X corp litigation and Senate Estimates and related meetings means that my schedule that week is up in the air. In the event we can connect remotely too, that might give me a better chance to join in. Many thanks, Julie

---

From: Zoe Robinson s 47F
Sent: Thursday, May 16, 2024 7:08 AM
To: Hannah Tonkin s 47F James Cockayne s 47F ; s 22 @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Cc: s 47F Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 47F
Subject: Re: Dates for CBA meeting

> Some people who received this message don't often get email from s 47F Learn why this is important

I will lock that time in with CBA and we can go from there.

Zoe

Get Outlook for iOS

From: Hannah Tonkin s 47F
Sent: Wednesday, May 15, 2024 1:52:34 PM
To: James Cockayne s 47F ; Zoe Robinson s 47F ; s 22 @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Cc: s 47F Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au) s 47E(c), s 47F @eSafety.gov.au>; s 47F s 47F
Subject: RE: Dates for CBA meeting

Hi all,

I can possibly do Fri 31st at 2-3pm but I would need to reschedule another meeting so please let me know if others are free then – thanks.

Kind regards,

Hannah

Dr Hannah Tonkin *(she/her)*
Women's Safety Commissioner
NSW Department of Communities and Justice
M s 47F
E s 47F

Office of the Women's Safety Commissioner

I acknowledge the traditional custodians of the land and pay my respects to Elders past and present.

From: James Cockayne s 47F
Sent: Wednesday, May 15, 2024 11:57 AM
To: Zoe Robinson s 47F ; Hannah Tonkin s 47F ; s 22 @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>
Cc: s 47F Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au) s 47E(c), s 47F @eSafety.gov.au>; s 47F s 47F
Subject: Re: Dates for CBA meeting

With apologies s 47F . And unfortunately I don't feel there is a suitable alternate from my office on this.

You should of course feel free to proceed without me and loop me in on my return.

Alternatively, if there is more info you can share about the CBA approach I am happy to provide input by correspondence.

James

Dr James Cockayne *(he/him/his)*
NSW Anti-slavery Commissioner
M s 47F **E** s 47F
W dcjnsw.info/antislaverycommissioner

From: Zoe Robinson s 47F
Sent: Wednesday, May 15, 2024 11:22:39 AM
To: James Cockayne s 47F ; Hannah Tonkin s 47F ; s 22 @eSafety.gov.au>; Toby Dagg s 47E(c), s 47F @esafety.gov.au>

Cc: s 47F Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au) s 47E(c), s 47F @eSafety.gov.au>; s 47F s 47F

Subject: Dates for CBA meeting

Dear All,

Can you confirm which date/time best suits you:

Wednesday 29th @2.30pm – 3.30pm
Friday 31st between 11 and 3pm

Thank you

Zoë Robinson | Advocate
Office of the Advocate for Children and Young People
s 47F
Ground Floor
219 -241 Cleveland Street
Strawberry Hills NSW 2012
www.acyp.nsw.gov.au

We respect Aboriginal peoples as the first peoples and custodians of NSW. This beautiful email banner was designed by our 2021 Chair of the Youth Advisory Council Lua Pellegrini.

My hours can vary due to travel or alternative arrangements – please respond to the email in your time and when it suits you and your work hours.

From: Julie Inman Grant
To: Kathryn King; Toby Dagg; s 22
Subject: FW: Political Alert - Transcript of Budget In Reply Address (FED) [SEC=OFFICIAL]
Date: Friday, 17 May 2024 4:27:12 PM
Attachments: 136B1012.PDF

OFFICIAL

As discussed:

TACKLING ONLINE CRIME

Tackling crime in our communities also means doing the same online.

There's been an uptick in young Australians committing, filming and uploading their crimes to social media.

A Coalition Government will make it an offence to post criminal acts online.

Those convicted will be banned from using digital platforms and liable for up to two years' imprisonment.

As a father of three children who all grew up in the digital age, I'm troubled by the material our children are exposed to.

That's why I announced in my Budget Reply last year that a Coalition Government will ban gambling advertising during the broadcast of sporting games.

However, I'm more worried by the criminal dark underbelly of the internet.

At the fingertips of our children is a concerning volume of sexually explicit and violent material, as well as content designed to indoctrinate.

We welcome the Government's belated decision to back our policy for an age verification trial.

But unlike Labor, a Coalition Government will include social media platforms like Instagram and TikTok in such a trial.

-----Original Message-----
From: CCH Parliament <politicalalert@cch.com.au>
Sent: Thursday, May 16, 2024 7:36 PM
To: politicalalert@cch.com.au
Subject: Political Alert - Transcript of Budget In Reply Address (FED)

Please find attached: TRANSCRIPT OF BUDGET IN REPLY ADDRESS (FED)

Leader of the Opposition, Peter Dutton, delivers the Budget In Reply Address.

136B1012 Total number of pages 19 SUPPORT: politicalalert@cch.com.au or 02 6273 2070. MAILBOX: https://www.cchparliament.com.au

THE HON PETER DUTTON MP

LEADER OF THE OPPOSITION
FEDERAL MEMBER FOR DICKSON

****CHECK AGAINST DELIVERY****

16 May 2024

ADDRESS TO THE HOUSE OF REPRESENTATIVES
BUDGET IN REPLY
PARLIAMENT HOUSE, CANBERRA

……

INTRODUCTION

Tonight, I want to outline part of my vision for Australia.

To get our country **Back on Track**.

To keep our nation safe and secure.

To make life easier and better for all Australians.

Because this Labor Government has made life so much tougher for Australians.

Because this Labor Government has set our country on a dangerous course.

Almost two years ago, Prime Minister Albanese was elected promising a reduction of $275 each year in your power prices, cheaper mortgages, and that you would be better off under a Labor Government.

All those promises have been broken.

And this Government has been focused on the wrong priorities.

It started with the Prime Minister's Voice referendum.

Not only did it waste $450 million which could have helped with the cost-of-living pressures you're now facing – the referendum also divided the nation.

And let's not forget that the Prime Minister called 'No' voters 'Chicken Littles' and 'doomsayers'.

Today, millions of Australians are struggling to pay their bills.

Even going to the supermarket and petrol station has become stressful for so many.

Prime Minister – Australians are genuinely hurting under your Government – they're not 'Chicken Littles'.

Electricity bills haven't gone down by $275 as was pledged on 97 occasions – they've skyrocketed.

The Treasurer will give you a $300 rebate, but he knows full well that your annual electricity bills have increased by up to $1,000 since Labor formed government.

Interest rates have gone up 12 times under Labor.

A typical Australian household with a mortgage is $35,000 worse off.

And that's if you're lucky enough to own a home.

Under this Prime Minister, the great Australian dream of home ownership has turned into a nightmare.

Even finding somewhere to rent is near impossible.

The Government has brought in an additional 923,000 migrants in just two years.

But on the available data, it has only built 265,000 homes.

Then there's Labor's tax on the family car and ute.

You're having to fork out thousands-of-dollars more simply for choosing some of Australia's most popular vehicles – like a Toyota Rav4 or Ford Ranger – all because the Government is trying to force you to buy an electric vehicle.

All of this has happened in just two years.

Paul Keating famously said, 'When Governments change, the country changes.'

Prime Minister Albanese and his Government have changed our country.

But as so many Australians can attest to, not for the better.

You, your family, your children, and our country can't afford another three years of this Government.

I know how to make the decisions to get our country **Back on Track**.

Tonight, I will remind Australians of the Coalition's economic plan to lower your cost-of-living and restore confidence to our economy.

I will also outline several policies which Australians can expect from a Coalition Government under my leadership.

Policies to get power bills down and to shore-up our nation's future energy security.

Policies to help alleviate our housing crisis and revive the dream of home ownership.

Policies to improve workforce participation and health services.

And policies to make our communities, our society, and our country better and safer.

But first, I will respond to the Treasurer's Budget.

RESPONSE TO THE BUDGET

As I've said previously, we're an Opposition which supports good policy and stands against bad policy.

Since Labor formed government, we've backed more than 180 Bills which have passed parliament.

But we've opposed some Bills where Labor and the Greens have collaborated to pass legislation which is not in our country's best interest.

Just as we endorsed some sensible measures in Labor's first two Budgets, we do the same for its third Budget.

In particular, the $3.4 billion for medicines on the Pharmaceutical Benefits Scheme.

And the extension of emergency payments to support women and children fleeing domestic violence which the Coalition established in 2021.

In my 22 years in parliament, I've seen good and bad Budgets.

But the Budget handed down on Tuesday is one of the most irresponsible I've seen.

Inflation is a huge problem for Australia.

On comparative inflation, Australia is worse than the US, Singapore, Germany, Spain, Japan, the Netherlands, Italy, South Korea, Canada, France, and the entire Euro area.

The reason interest rates have gone up 12 times is because the Government can't control its spending – and because of its reckless energy policy.

In three Labor Budgets, the Government has lifted spending by a staggering $315 billion – or $30,000 per Australian household.

The Reserve Bank Governor has sounded the alarm on inflation being home-grown.

In the last 48 hours, every credible economist has issued scathing assessments of this Budget because Labor has us in an inflationary hole and is still digging.

Make no mistake, any further increase to interest rates and inflation also now rests squarely on the shoulders of this Prime Minister and Treasurer.

Magic pudding spending and $13.7 billion on corporate welfare for billionaires doesn't help the economy, or make your life easier.

Let's also be clear about Labor's $300 energy rebate which will cost the economy $3.5 billion.

We will support this relief because we know Australians are hurting.

But the Government is treating the symptom, not the disease.

Labor's 'renewables only' energy policy is the reason your power bills continue to skyrocket.

Here's some facts which show the troubling state of our economy:

More than 16,000 businesses around the country have gone insolvent since the 1st of July 2022.

Productivity has plunged by 5.4 per cent on this Government's watch.

Household buying power has gone down by 7.5 per cent.

Last year, Australians suffered the biggest increase in average tax rates of any citizens in the developed world.

There's been double-digit increases for your essentials like electricity, gas, milk, bread and rent.

Tragically, so many more Australians are living in cars and tents.

And because of spending in this Budget, the economic outlook is one of deficits as far as the eye can see.

THE COALITION'S ECONOMIC PLAN

To alleviate cost-of-living pressures, we need to get inflation down.

To get our economy **Back on Track**, we need a back-to-basics economic plan.

That's what a Coalition Government will deliver.

First, we will rein-in inflationary spending to take the pressure off inflation.

As a start, we will not spend $13.7 billion on corporate welfare for green hydrogen and critical minerals.

These projects should stand up on their own without the need for taxpayer's money.

Second, we will wind-back Labor's intervention and remove regulatory roadblocks which are suffocating the economy and stopping businesses from getting ahead.

For example, we will not force large firms to spend more than a billion dollars a year policing the emissions of every small business they deal with – as Labor is trying to do.

We will condense approval processes and cut back on Labor's red tape which is killing mining, jobs, and entrepreneurialism.

Only yesterday, Santos indicated it will have to let go 200 employees because of slow project approvals.

I want mining to boom in Western Australia and around the nation.

More mining means more revenue.

More revenue means more roads, schools and hospitals.

A turbocharged Western Australian economy means more national prosperity.

We don't need to give out billions-of-dollars of taxpayer's money to get mining projects started.

Third, we will remove the complexity and hostility of Labor's industrial relations agenda which is putting unreasonable burdens on businesses.

For example, we will revert to the former Coalition Government's simple definition of a casual worker and create certainty for our 2.5 million small businesses.

Fourth, we will provide lower, simpler and fairer taxes for all – because Australians should keep more of what they earn.

You will hear our tax plan detail ahead of the election.

Fifth, we will deliver competition policy which gives consumers and smaller businesses a fair go – not lobbyists and big corporations.

And sixth, we will ensure Australians have more affordable and reliable energy.

Our economic plan – with its tried and tested principles – will restore competitiveness and rebuild economic confidence.

Small businesses are the lifeblood of our communities.

I've run a small business, as have many of my colleagues – unlike most Labor parliamentarians.

The Coalition understands small business.

Tonight, I announce that we will extend the value of assets eligible for the instant asset write-off to $30,000 and make this ongoing for small businesses.

This will simplify depreciation for millions of small businesses by cutting red tape, boosting investment in productive assets, lowering business costs and prices.

ENERGY

A respected senior journalist recently wrote, 'Energy is not part of the economy. It is the economy.'

The Government's 'renewables only' policy continues to drive-up power prices.

Electricity and gas prices have gone up by 18 and 25 per cent respectively.

You can see this rise in your household power bills.

But the energy bills of farmers, businesses and manufacturers have also skyrocketed.

And that means the cost to make anything – from food to furniture – has also gone up.

That's why you're paying more at the supermarket and shops.

If energy is not affordable or reliable, more manufacturers will shut-up-shop or move offshore.

That's why there's been a three-fold increase in the number of manufacturers who have closed their doors over the last two years.

For all the Government's talk about a 'Future Made in Australia', their current approach has no chance if energy isn't cheap and consistent compared to other countries.

Renewables have a role to play in our energy system.

But we can't rely on weather-dependent energy alone.

We need power 24/7 – especially for our hospitals, factories and freezers that need to operate around the clock.

Concerningly, the Government's 'renewables only' policy will see 90 per cent of that 24/7 power switched off over the next ten years.

How are things progressing for the Government's plan for 5 gigawatts of renewables per year?

Well, just last year, only 1.3 gigawatts were committed – almost 75 per cent off target.

Re-wiring our country will cost at least $1.3 trillion.

Who will bear that cost?

You will. Farmers will. Manufacturers will. Businesses will.

If you think you're paying high prices for power today, they will only get much higher under a 'renewables only' roll-out.

Our nation has three energy goals:

Cheaper power. Consistent power. Cleaner power.

We won't achieve these goals under Labor's 'renewables only' policy.

But we can achieve all three.

By following the other top 20 economies in the world which use zero-emission nuclear power, or are taking steps to put it in their mix.

And by ramping-up domestic gas production for affordable and reliable energy in the more immediate term.

After two years of interventions into the gas market, skyrocketing prices, and repeated warnings of shortfalls, Labor's new gas strategy is just words on paper.

There's little chance of Labor bringing new gas supply into the system because it's ideologically opposed to gas.

And because it wants to win Green votes over in inner city seats.

Unlike Labor, a Coalition Government will:

- speed up approvals;
- unlock gas in key basins, like the Beetaloo basin;
- defund the Environmental Defenders Office which is halting vital projects through lawfare;
- ensure gas is delivered to where it's needed by reinstating the National Gas Infrastructure Plan; and
- commit to an annual release of offshore acreage for exploration and development in the Northern Territory and Western Australia.

On nuclear power, some 50 countries are exploring or investing in zero emission, next-generation technologies for the very first time.

We hold the largest deposits of uranium on the planet.

Do the Prime Minister and Minister Bowen have it right, and the rest of the developed world have it wrong?

The Government have ordered nuclear-powered submarines.

I simply pose this question:

Why is the technology which is safe for our submariners unsafe for our citizens?

Because of nuclear power, residents in Ontario, Canada pay up to a quarter of the cost of what some Australians pay for electricity.

With nuclear power, we can maximise the highest yield of energy per square metre and minimise environmental damage.

We do that by putting new nuclear technologies on- or near- the brownfield sites of decommissioned or retiring coal-fired power plants using the existing grid.

There's no need for all of the proposed 58 million solar panels, almost 3,500 wind farms, and 28,000 kilometres of new transmission poles and wires.

Bob Hawke was a strong leader who strongly supported nuclear power.

As does John Howard, along with the Australian Workers Union, and many others who have a vision for our country – including some 65 per cent of Australians aged 18 to 34-years-old.

Making Australia a nuclear-powered nation is right for our country and will secure a future of cheaper, consistent and cleaner electricity.

We need the right policy – for you and for our nation.

HOUSING

Beyond Labor's energy crisis, we're also facing a housing crisis.

The great Australian aspiration of home ownership has become out of reach for so many.

It's wonderful that parents who have the financial means can help their kids into a home.

But I will never accept a situation where the only people who can afford to buy a home are those with the support of their parents.

The Coalition has already recommitted to allowing Australians to access up to $50,000 of their super to buy their first home.

And extended this policy to separated women to help restart their lives.

The money initially withdrawn from super will need to be returned when the house is sold to support retirement.

But we need to do more.

For almost 20 years, I've chaired my local Salvation Army Red Shield Appeal.

Two weeks ago at our annual fundraising breakfast, I heard a heartbreaking account of a man in his 70s having to live in his car.

Such a soul-destroying experience is sadly not an uncommon story.

Australians are struggling to find homes to rent and buy – and not always due to a lack of money.

Amidst this housing crisis, Labor is bringing in 1.67 million migrants over five years – more than the population of Adelaide.

We celebrate the contributions of migrants over many decades who have helped build the achievement of modern Australia.

But by getting the migration policy settings right, the Coalition can free up more houses for Australians.

The Prime Minister has promised to build 1.2 million homes by 2029.

But on the Government's current trajectory, they will fall short by 400,000 or 33 per cent.

The Prime Minister is making the housing crisis worse.

Australians need homes now.

We're at an 11-year low of building approvals and to help Australians now we need to prioritise Australians for existing homes.

The other impact Australians are feeling from the Albanese Government's poor management of the migration program is from congestion on our roads and pressure on existing services which are stretched, like seeing a GP.

Tonight, I announce several measures a Coalition Government will implement to meet our housing crisis head-on by alleviating pressure on the housing market.

We believe that by rebalancing the migration program and taking decisive action on the housing crisis, the Coalition would free up almost 40,000 additional homes in the first year.

And well over 100,000 homes in the next five years.

First, we will implement a two-year ban on foreign investors and temporary residents purchasing existing homes in Australia.

Second, we will reduce the permanent migration program by 25 per cent – from 185,000 to 140,000 for the first two years in recognition of the urgency of this crisis.

The program will then increase to 150,000 in year three and 160,000 in year four.

We will ensure there are enough skilled and temporary skilled visas for those with building and construction skills to support our local tradies to build the homes we need.

Similarly, we will return the refugee and humanitarian program planning level to 13,750 – closer to the long-term average.

The humanitarian program will remain one of the most generous in the world on a per capita basis.

Third, we will reduce excessive numbers of foreign students studying at metropolitan universities to relieve stress on rental markets in our major cities.

We will work with universities to set a cap on foreign students.

And we will enhance the integrity of the student visa program by introducing a tiered approach to increasing the student visa application fee and applying it to foreign students who change providers.

The usual CEOs and big businesses may not like this approach.

But my priority is restoring the dream of home ownership.

WORKFORCE

While reducing migration numbers to ease pressure on housing, a Coalition Government will encourage thousands of people to engage more in the labour market.

We recommit to increasing the amount older Australians and veterans can work without reducing pension payments.

We will double the existing work bonus from $300 per fortnight to $600.

It's estimated this will benefit over 80,000 pensioners and veterans who choose to work.

We will look to further expand the work bonus arrangements beyond this commitment in consultation with older Australians and veterans and in consideration of labour market conditions.

Pensioners will continue to accrue unused pension work bonus amounts up to a maximum of $11,800 which can exempt future earnings from the pension income test.

We will also lift the number of hours those on student visas can work by 12 hours a fortnight.

HEALTH

Amidst our cost-of-living crisis, people's health and well-being are suffering.

That's why we committed to restoring the number of Medicare-subsidised psychological sessions from 10 to 20 – and on a permanent basis.

As a Health Minister, I increased hospital funding year-on-year.

I also established the $20 billion Medical Research Future Fund which, to this day, provides billions-of-dollars to medical research projects.

Indeed, when I became Health Minister in 2013, we inherited a bulk billing rate of 73 per cent and increased it to 84 per cent.

When we left government, bulk billing was 88.5 per cent.

What Labor tried to hide in its Budget is that bulk billing has decreased to 77 per cent – an 11 per cent drop.

The health of all Australians – particularly given our ageing society – is always a priority for the Coalition.

Last year, I committed to an investment in best-practice for women's health issues, including endometriosis.

Tonight, I welcome the Government's commitment of $50 million in this budget for longer consultations for endometriosis and pelvic pain.

The Coalition will continue to support measures for women's health, particularly in primary care.

More needs to be done to support women's health, including for menopause and peri-menopause.

We will continue to develop and support good policy to this end.

Concerningly, Australia is facing a looming shortage of GPs – some 11,000 by 2031.

We need more GPs – especially in our suburbs and regional areas.

Junior doctors who enter general practice earn about three-quarters of the salary of their counterparts in hospitals.

Working with the Royal Australian College of General Practitioners and Australian Medical Association, a Coalition Government will invest $400 million to provide junior doctors who train in general practice with incentive payments, assistance with leave entitlements, and support for pre-vocational training.

We also want better outcomes for Indigenous Australians.

Led by Senators Liddle and Nampijinpa Price, we will provide practical solutions to improve education, health and safety outcomes for indigenous women and children – especially in our most disadvantaged remote communities.

LAW AND ORDER

In recent times, our nation has been rocked by many shocking and tragic events.

The stabbings at Bondi where six people were murdered.

Knife attacks on a bishop in Western Sydney and a man in Perth by radicalised youth – incidents reinforcing the enduring threat of extreme Islamism.

Twenty-eight women killed in violent circumstances this year alone.

More than 150 hardcore criminals – including murderers and sex offenders – released from immigration detention into the community by this Government, with some having re-offended.

And since Hamas' barbaric terrorist attack on Israel, a 700 per cent increase in anti-Semitic incidents on our soil.

Australians are unsettled by crime on our streets, ruptures to our social cohesion, and threats to our national security.

A Coalition Government will provide much needed leadership in tackling knife crime.

We will work with states and territories to develop uniform knife laws across all jurisdictions.

Laws which give police the powers to stop and search using detector wands – like Queensland's 'Jack's Law'.

And laws which limit and restrict the sale and possession of knives to minors and dangerous individuals.

As a former police officer, the horrific scenes of beaten women and distraught children I encountered stay with me to this day.

As do the memories of taking women who were shaking with fear to shelters and safe homes – and helping them relocate with their children to safety.

It's why I've dedicated much of my career to protecting women and children.

It's why, as Home Affairs Minister, I established the $70 million Australian Centre to Counter Child Exploitation and recommit to doubling its size.

Recently Molly Ticehurst, a 28-year-old mother from New South Wales was murdered because her violent ex-partner was on bail.

Our bail laws need to be tightened.

And under a Coalition Government I lead, they will be tightened.

Offences relating to partner and family violence generally fall under state and territory legislation.

But there is also a role for the Commonwealth.

A Coalition Government will make it an offence to use mobile phone and computer networks to cause an intimate partner or family member to fear for their personal safety, to track them using spyware, or engage in coercive behaviours.

We will toughen the bail laws that apply to these new Commonwealth offences.

I've been a Minister for Immigration and Home Affairs.

They're demanding but rewarding jobs.

I granted thousands of visas to sick children, parents with medical conditions, victims of sexual assault, and refugees who have become wonderful Australians.

The public rarely hears about that side of the job.

But in these roles, you must also make tough decisions.

I cancelled more than 6,300 visas of dangerous non-citizen criminals – with a priority on those committing sexual offences against women and children – driven by my desire to stop these people harming Australians.

If a minister doesn't have the backbone to do that, they're letting our country and citizens down.

I made our country and citizens safer.

As Prime Minister, I will do it again.

It will take a Coalition Government – once again – to stop the people smugglers and to deport criminals.

It will also take a Coalition Government to turn the tide of anti-Semitism afflicting our country.

Anti-Semitism is not just a threat to one segment of our community.

It's a threat to our social cohesion and democratic values.

Some of the most strident anti-Semitic standard-bearers have come from our university campuses.

We will also provide the moral and political leadership which makes it abundantly clear that we expect the law to be enforced readily – not reluctantly – against those inciting hatred and violence.

TACKLING ONLINE CRIME

Tackling crime in our communities also means doing the same online.

There's been an uptick in young Australians committing, filming and uploading their crimes to social media.

A Coalition Government will make it an offence to post criminal acts online.

Those convicted will be banned from using digital platforms and liable for up to two years' imprisonment.

As a father of three children who all grew up in the digital age, I'm troubled by the material our children are exposed to.

That's why I announced in my Budget Reply last year that a Coalition Government will ban gambling advertising during the broadcast of sporting games.

However, I'm more worried by the criminal dark underbelly of the internet.

At the fingertips of our children is a concerning volume of sexually explicit and violent material, as well as content designed to indoctrinate.

We welcome the Government's belated decision to back our policy for an age verification trial.

But unlike Labor, a Coalition Government will include social media platforms like Instagram and TikTok in such a trial.

DEFENCE

Authoritarian regimes like China, Russia, Iran and North Korea are emboldened, expanding their militaries, conducting cyber-attacks, and engaging in foreign interference.

The Prime Minister and his Deputy rightly say we're living in the most precarious period since the Second World War – a view echoed by our intelligence agencies and allies.

Strenuous efforts are needed to maintain peace and deter acts of aggression – like those recently aimed at our navy and air force.

The 1930s taught us that appeasement and weakness of leadership do not end well.

In this critical period of risk, I will offer strong leadership backed by significant investment in defence.

Labor's priorities are wrong.

The Government has announced an additional 36,000 public servants in this Budget costing Australian taxpayers $24 billion over four years.

The Coalition sees areas like Defence as much more of a priority than office staff in Canberra given the precarious times in which we live and threats in our region.

We will reprioritise Canberra-centric funding and make an additional investment in Defence to rapidly enhance the capability of our men and women in uniform.

We're working with leaders in defence industry to identify projects and investments that can be made in Australia to keep us safe in an uncertain world.

CONCLUSION

I say to every Australian tonight, my vision is to get our country **Back on Track**.

To make your life easier.

To make us safe and secure again.

The job of the Prime Minister is to be strong, not weak.

To be fair and firm.

To be compassionate and definite.

To unite, not divide – especially through referendums.

As each day passes, this Government increasingly shows how disconnected it is from the views, values and vision of everyday Australians.

Labor has forgotten the main principle of governing:

It isn't the people who serve the will of the government – it's the government who serves the will of the people.

I came to this parliament having served my community as a police officer and as a successful small business owner employing 40 people.

I've had the honour of serving Australians on the front bench since 2004, in many portfolios, and under four prime ministers.

My team and I have the experience to get our country **Back on Track** and to support everyday Australians.

We live in the greatest country in the world.

But at the moment, Australia is being held back.

Australians are being left behind by this weak Labor Government with the wrong priorities.

Our country deserves so much more.

Ask yourself:

Are you better off today than you were two years ago?

Do you feel safer or more secure than you did two years ago?

'When Governments change, the country changes.'

Australians can't afford another three years of Labor.

At the next election, it will be time for a change.

A better change for you, your family and our country.

[ENDS]