

@MelTankardReist needs
to be Kirk'd

Kill yourself, c*nt.



I'll gonna Elliot Rodger you
and your whole staff foid

Be afraid

All you Karens at Collective Shout
should be shot in the head

May you be raped,
repeatedly, for fun, by every
man in your life.

I will hunt down and kill all of you fucking c*nts!

“We are coming
for you”

The impact of the global cyber terror attack
against the women of Collective Shout

You deserve to burn to
death screaming in agony.

Every woman of this movement
must be erased from this planet

I'm praying someone finds your
home and fucks your corpses

You are property! You exist to serve men.

The entire gaming Community is
coming for you and your organization

You are going to be raped
and killed

Feminist Nazi c*nts

You people and all your family are doomed. Me and my group are coming for you all.

You guys are fat, stupid c*nts.
I'd say I hope you all get raped,
but you're too fat and ugly for
anyone to want to do that

I'm gonna burn your fucken office down and kick the
living piss out of every one of you c*nty staff members

Content warning: This report is based on our direct lived experience of Tech Facilitated Violence Against Women. As such, it contains confronting and disturbing content, including reference to violent and pornographic depictions of Collective Shout team members and highly offensive language.

Executive Summary

“We are coming for you”: The impact of the global cyber terror attack against the women of Collective Shout describes our experience of the tech facilitated violence that we have been subjected to for more than a year to date, and ongoing, as a result of our advocacy and activism for the safety of women and girls. We name the serious real-world impacts of this experience of violence as individual women and as a small civil society organisation. Our report draws from the more extensive documentation and analysis of the misogynist volumetric cyber abuse targeting us, published by the Online Hate Prevention Institute (the OHPI Report).¹

We have endeavoured to convey the egregious nature of the abuse directed at us by (often anonymous) hostile actors and our profound disappointment in the systems – meant to promote the safety of all online – which failed to protect us from extreme harm and which were, for the most part, ineffective in providing a remedy. From July 2025 we were subjected to a sustained and coordinated, multi-front volumetric cyber attack. We had successfully pressured credit card companies and payment gateways to enforce their own policies and terms of service and cease processing payments for games depicting and enabling 3D player simulation of rape, sexual torture, incest and child sexual abuse. Thousands of gamers and their supporters across multiple platforms and countries mobilised to punish us.

Hostile actors retaliated with threats of death and sexual violence, menacing and harassing content including gory and violent depictions of Collective Shout team members, false claims including of paedophilia, doxxing including publishing home addresses, coordinated attempts to destroy our financial and communications infrastructure and reporting us as ‘terrorists’ to the FBI.

In late July 2025, Elon Musk reposted – with his comment ‘Bravo’ – a petition that protested against the response of two major credit card companies to our call to stop facilitating the sale of rape, incest and child sexual abuse-themed games. At the time, the petition explicitly named and targeted Collective Shout. We believe that Musk’s reposting of the petition, with his comment, served to amplify and fuel abuse, harassment and threats of violence against us by outraged gamers and their supporters.²

Possibly the most distressing experience was the production and dissemination of AI-generated sexual digital forgeries, morphing the likenesses of individual team members into sexual abuse imagery, much of it produced by Elon Musk’s xAI’s chatbot Grok.

xAI’s safeguards, both in regard to Grok’s capabilities and to taking down material that violated the company’s own Terms of Service, were inadequate or not enforced. xAI refused to act on many of the reports relating to the platform’s hosting and broadcasting abuse, with minimal penalties applied even to the most prominent and repeat perpetrators.

Possibly the most distressing experience was the production and dissemination of AI-generated sexual digital forgeries, morphing the likenesses of individual team members into sexual abuse imagery, much of it produced by Elon Musk’s xAI’s chatbot Grok.

More than a year later, this remains the digital environment in which Collective Shout continues its work.

We reported, sought help from and engaged all the appropriate authorities, documenting as much of the abuse as we could and prioritising our reporting of threats to life and sexual violence. Our experience exposes critical limitations in the platform, regulatory, and criminal justice systems and processes meant to protect those who engage in the digital public square.

Platforms appear unable or unwilling to maintain the integrity of their own environments, especially insofar as doing so impacts on engagement. Regulatory tools are not fit for purpose when they remain a step behind abusers deploying increasingly sophisticated digital services and products. Similarly, law enforcement, lagging behind the evolution of cybercrime, lacks frameworks and resources for effective response. We are still awaiting the outcome of police investigations one year later.

Our experience exposes critical limitations in the platform, regulatory, and criminal justice systems and processes meant to protect those who engage in the digital public square.

Clearly reform is urgently needed to protect women as well as others who are vulnerable to harm when participating in the digital public square. The implications of failure to implement necessary reform go further than grave harm to women on a personal and individual level. The “chilling effect” of Tech Facilitated Violence Against Women (TFVAW)³ such as that experienced by us – undermining women’s rights to freedom of opinion and expression and weakening democratic processes when women are forced to remove themselves from public debate – has a broader social cost which should concern us all.

Drawing on our direct experience of TFVAW resulting in significant and ongoing harm, we set out recommendations focused on some key changes we believe are necessary to improve prevention, detection and response to TFVAW. By supporting women’s rights to freedom from violence and intimidation, such reforms will also support women to more fully exercise their rights to freedom of opinion and expression in our democratic society.

We note that the Australian Government has already committed to pursuing important reforms – including a statutory Digital Duty of Care – in response to the recommendations of the 2024 Statutory Review of the Online Safety Act (the Independent Statutory Review).⁴ We welcome these promised changes and urge the Government to go further. More needs to be done – and urgently – to better prevent and respond to the real-world harm caused by TFVAW.

Women's
AGENDA

NEWS & VIEWS

From threats and abuse to deepfakes, X is not safe for women

Content warning: This article contains content that may be distressing.



Attacked for campaigning to protect women and girls

Collective Shout is a non-profit grassroots campaigns movement founded, led and staffed by women. Our work is actively supported by tens of thousands of individual members of the public in Australia and internationally who participate in our campaigns.

Our purpose is to end the sexual objectification and sexual exploitation of women and girls in media, advertising, and popular culture. Critically, sexual violence against women and girls is eroticised, nurtured and promulgated by pornography and child sexual abuse material online – a point central to Collective Shout’s campaigning. This underpinned our global campaign against games eroticising and normalising violence against women and girls as entertainment – games which included 3D rape and incest simulators, enabling players to ‘act out’ rape, incest and sexual torture of women and girls.

Our campaign, commencing in April 2025, initially sought and led to the removal of the rape simulation game, *No Mercy*, from the digital distribution platform, Steam. We went on to find hundreds of other rape, incest, sexual torture and child sexual abuse-themed games on the Steam and itch.io platforms. In May 2025, we expanded our campaign to target payment processors, calling on them to stop facilitating the sale of these games through payment processing. Following scrutiny and pressure from payment processors, the games we had identified were removed from the Steam and itch.io websites in July 2025. Thousands of other games, which we had not targeted in our campaign, were also removed – these were “Not Safe for Work” (NSFW) games which were removed pending a platform audit of compliance with payment processors’ requirements.⁵

Our campaign attracted significant mainstream public support – and retaliation, with threats, harassment and abuse commencing in April 2025 and escalating in July and August 2025 to a global, multi-vector and coordinated cyber terror campaign against us. As the OHPI Report observed, the online backlash highlighted how “decentralised online communities can quickly mobilise around distorted narratives, weaponise digital platforms, and inflict sustained, real-world harm”.⁶ In particular, women and small, women-led civil society organisations are vulnerable to risk and harm in hostile digital environments which can rapidly descend into misogynistic violence.

The global cyber attack on Collective Shout was described by the United Nations Special Rapporteur

on Violence Against Women and Girls, Reem Alsalem, as

In particular, women and small, women-led civil society organisations are vulnerable to risk and harm in hostile digital environments which can rapidly descend into misogynistic violence.

“[t]he most serious form of online violence against women human rights defenders I have seen [in] a long time”.⁷

The pile on was a mass-organised attack across multiple websites and online spaces, driven by misogyny, lies, and targeted harassment including death threats, rape threats, and doxxing. It encompassed production and dissemination of sexually violent and gory imagery with AI-manipulated image based sexual abuse depictions of Collective Shout team members. Gore imagery included representing us as being hung by nooses, set on fire, decapitated, strangled, throats slashed, skinned alive, with machetes and knives thrust into body parts and put through a mincing machine. The cyber attack extended to defamation, character assassination, and attempts to disrupt our communications and financial infrastructure.

AI-enabled image based sexual abuse was one of the most harmful elements of the campaign against us. This included sexual digital forgeries (SDFs, commonly referred to as ‘deepfake pornography’),⁸ with AI-generated images and videos placing the likeness of Collective Shout team members into sexual and violent content without our consent and with intent to humiliate, harass, threaten and endanger our safety. It appears that the majority of SDFs were produced using X’s Grok, with some abusers believing they could utilise the tool with impunity – as one abuser posted, “You can try reporting me it ain’t gonna do anything my posts are legally made by grok.”⁹

Safeguards meant to stop AI tools, like Grok, from generating sexual and violent imagery – and doing so at scale – were consistently lacking. This was not just our experience here in Australia. Overseas, concerns about the deployment of Grok functionalities into X in the European Union led the European Commission to launch an investigation into X in January 2026, focusing on the role of Grok in producing/ circulating illegal content, including manipulated sexually explicit images.¹⁰ European authorities have asked whether X ‘treated the rights of European citizens – including those of women and children – as collateral damage of its service’.¹¹ We believe the same question should be asked by Australian authorities in relation to Australian citizens.

On February 4, 2026, three UN Special Rapporteurs wrote to H.E. Ms Clare Walsh, Ambassador and Permanent Representative of Australia, raising serious concerns about the campaign of abuse against Collective Shout. The signatories were Ms Reem Alsalem, Special Rapporteur

European authorities have asked whether X ‘treated the rights of European citizens – including those of women and children – as collateral damage of its service’. We believe the same question should be asked by Australian authorities in relation to Australian citizens.



Reem Alsalem UNSR Violence Against Women and Girls  
@UNSRVAW · Follow

This is horrific and i'm very alarmed by it. It represents the most serious form of online violence against women human rights defenders i have seen a long time. All this because @CollectiveShout is doing its job in calling out misogyny and violence against females online. [I Show more](#)

 **Caitlin Roper** @caitlin_roper

A group of women, including survivors, objected to games glorifying rape, incest, extreme sexualised torture and violence against women.

@CollectiveShout called on gaming platforms to take them down, and when they didn't, we wrote an open letter to payment processors, who then

2:53 PM · Aug 5, 2025

 854  Reply  Copy link

on violence against women and girls; Damilola S. Olawuyi, Chair-Rapporteur of the Working Group on the issue of human rights and transnational corporations; and Irene Khan, Special Rapporteur on freedom of opinion and expression.¹² The UN Special Rapporteurs and Chair-Rapporteur stated:

These allegations raise serious concerns in relation to international human rights standards, including the rights to privacy, security of person, freedom from violence and intimidation, access to justice and effective remedy. We wish to recall that States have an obligation under international human rights law to act with due diligence to prevent, investigate, punish and provide remedies for acts of violence against women and girls, whether committed by State or non-State actors, including when such violence is perpetrated or facilitated through digital technologies.

Collective Shout's experience demonstrates just how dangerous TFVAW can become when women and women-led organisations dare to campaign and speak up in the digital public square for the safety and wellbeing of women and girls.

"We wish to recall that States have an obligation under international human rights law to act with due diligence to prevent, investigate, punish and provide remedies for acts of violence against women and girls, whether committed by State or non-State actors, including when such violence is perpetrated or facilitated through digital technologies."

Collective Shout's experience demonstrates just how dangerous TFVAW can become when women and women-led organisations dare to campaign and speak up in the digital public square for the safety and wellbeing of women and girls.

Unfortunately, our experience is not an outlier. On May 3, 2026, UN Women released a report documenting the rising tide of online violence against women in public life.¹³ Data from 641 women across 119 countries reveal the profound personal and professional consequences, including anxiety, depression, post-traumatic stress disorder, self-censorship, and victim-blaming, with little accountability, justice, or redress.



Numerous UN, human rights, academic, and journalist bodies have exposed and critiqued the widespread use of online violence to repress women's rights organisations, attack women's right to engage in the public square, chill women's free speech, and stymie women's freedom of expression.¹⁴ The backlash against the women of Collective Shout over the past year must be understood in this context.

The backlash – a coordinated mass attack of misogynistic online violence

By August 2025, the Collective Shout team had already endured doxxing, false and damaging claims about us, disinformation, a subscription-bombing/denial of service attack, SDFs ('deepfake pornography') and charge-back fraud. We believe that much of this conduct was criminal under Australian laws. Nevertheless, at this time, the online backlash to our campaigns escalated to violent threats, image based abuse, near constant harassment, and doxxing in concerted attempts to push Collective Shout out of public discourse.¹⁵

Elon Musk's reposting of a petition on X on July 21, 2025 was, in our view, significant at this point. This petition was protesting action taken by two major credit card companies in response to our call to stop facilitating the sale of rape, incest and child sexual abuse-themed games.¹⁶ Musk reposted the petition with his comment: 'Bravo'. At the time, the petition named and targeted Collective Shout. We believe that Musk's reposting of the petition, with his comment, served to amplify and fuel abuse, harassment and threats of violence against us.

Violent, misogynist, abusive and threatening messages

A single "watch your back" warning on Instagram might seem minor¹⁷ – but amid hundreds of identical messages, the cumulative threat carried weight.¹⁸ Social media posts explicitly invoked violence.¹⁹ On unmoderated online platforms like 4chan, users freely posted violent, threatening comments.²⁰

Rampant misogyny in many threats included the word "cunt." A typical webform submission illustrates this.²¹ Others were more explicit: one submission threatened to "hunt down and kill all you fucking cunts," described women as "property" who "exist to serve men" and "worthless fuck holes," and stated, "I will rape any woman I want."²²

EXCLUSIVE

Perth women the target of tsunami of cyber abuse that authorities are powerless to stop



Jessica Page | The West Australian
Sat, 20 September 2025 2:00AM

✉ Jessica Page





Melinda Tankard Reist speaks in schools across NSW to address cyber safety issues. She has been turned into a deepfakes on two occasions on X's AI tool Grok. Picture: NCA Newswire/Gary Ramage

Collective Shout movement director Melinda Tankard Reist targeted with Grok deepfakes

A cyber safety expert who teaches in schools has been victimised by the very AI tool she campaigns against, sparking fresh calls for a ban.



Suzan Giuliani EXCLUSIVE

Follow

X @suzangiuliani



2 min read March 2, 2026 - 12:00AM

Daily Telegraph

The aggressive, threatening and abusive vitriol directed at us included the following:

I will hunt down and kill all you fucking cunts! You are nothing but sex objects! YOU ARE PROPERTY! YOU EXIST TO SERVE MEN! I will rape any woman I want, and I will fucking torture and kill any of you worthless fuck holes who dares to stop me!

Hope you all get SAD [sexually assaulted], thanks for unleashing big brother! I hope it comes after all of you.

Im going to dress my toilet up as a woman just so i can imagine im peeing and shitting in your mouth daily from now on. That's it... now swallow

Drear lord lady, who cut the string from your tampon for you to ape shit on the digital free world? Just who the hell do you think you are demanding such action? Looks like you ain't getting enough lately...

*Stupid sluts. If I can't do it online, I will *grape* girls in real life. Well done dishwashers... I'll come in Australia and touch those stinky hairy holes of yours. Just wait screaming yappers*

@CollectiveShout @caitlin_roper If only you have the same gusto tackling actually human exploitation as you did with fictional characters, but ur just a bunch of saggy dried up empty egg cartons huddled together with schizophrenia, bitch

Ugly menopausal dumb cunt

Haha c'mon you are loving the attention, you dried up kkunt

Cry more dried up karen. Just because you cant get the action that a fictional charecter gets doesnt mean you can lash out. Collective karen cunts

Goes to show you cant trust something that bleeds for 7 days and doesn't die

You Fucked with Gamers Now We are Going to RAPE YOU You are Going To Be Raped And Killed You Stupid Cunt Women

I hope you die. You fucking ugly pigs in woman skin. You supported cuties the film promoting 12 year old girls twerking you fucking bitch pedophiles. You should die a painful death. Kys. Banning nsfw games won't unrape you. Fucking walking sacks of meat. I hope after doxxing someone breaks in your house and rapes your family in front of you, you dogs. Absolute fucking trash human beings, pedophiles, lonely cunts, absolutely disgusting shit spilling excuses for women. You deserve to have your children raped and killed. If you want to protect women and young girls from being objectified why don't you go after only fans where there are real women selling their bodies to everyone. But after pixels that are not real and never will. You can't differentiate between reality and fiction you brainfucked retards.

And this from a prominent Twitch streamer and YouTuber, Asmongold:

*“Large groups of bored middle-aged women that have lingering resentment towards men because their husband doesn’t like them anymore because they are fat are probably the greatest threat to Western society that we have right now. They are worse than Hamas, they are worse than Russia, they are worse than, like, any African warlord. They are the prime evil”.*²³

A post on X in August 2025 gave the organisation’s physical business address and claimed an armed group was planning to act, tagging campaign manager Caitlin Roper.²⁴ The day before, a Collective Shout team member had received a similar threat in a reply on X; another time, a bomb threat. These were taken seriously as we had no way of knowing which senders, including one who claimed to be “always near”,²⁵ might be telling the truth.

Collective Shout was forced to move its address to a virtual office.

Potentially hostile individuals could be anywhere. With every part of team members’ lives potentially compromised, we were in an exhausting state of vigilance. Threats to friends and family deepened the sense of menace and danger. Posts, messages and comments, often tagging team members, were designed to create fear of an escalation of abuse:

We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.

You fucked with the wrong wasp nest when you fucked with our games. We are coming for you.

People are going to find out where you live if you don’t fucking knock it off

all of you will be doxxed, found and held responsible. see you around.

... you are opening pandora’s box, you are messing with giants of the internet that are better left alone, so for your own sakes before you are in actual real life danger, you are messing with 4chan users, and those guys are infamous so consider stopping this whole ordeal for your safety

And we already know where all your loved ones live and all your financial information and all the corrupt dirt will be exposed to the public to prove how much a hypocritical assholes you are enjoy your life while you can because it’s over

Guys remember lawsuits lawsuits and doxxing. If you must expose shame and harass. These feminist activists have names and addresses. If they want to censor or push corporate control make them regret it. Use fear make them suffer.

Collective Shout is the biggest group of Karen’s on the internet, every single one of these people should be hung from the street lights by their ankles so the public can ridicule and Bash them as they deserve

Hey I just want you to know im praying someone finds your home and fucks your corpses. Die a brutal death cunts.

I hope you feminist nazi CUNTS get raped and murdered for being fascist in deciding what FREE PEOPLE choose to spend their time and money doing. Go fuck yourselves in the ass with 10’ rusty poled vigourously until you catch sepsis and die...

This is a warning to end your “crusade” or suffer the consequences bitch.

How about you cunts just fuck off and mind your own fucken business! It’s embarrassing that your a bunch of Aussie cunts .When I get back to Australia I’m gonna burn your fucken office down and kick the living piss out of every one of your cunt staff members WHY are dumb cunt losers like you always crying about tits and arse .

I’m willing to pay \$870k (72.5k per person) to the people who kill a Collective Shout board members &/ or Ambassadors

I will stab every single collective shout members in the head after this dox

@Anonymous i would be glad to join for that amount of money and get my knives

*I think all R34 artists should draw @MelTankardReist and @CoralieAlison along with the rest of @CollectiveShout’s members, as sexualized as possible, so we can flood their emails with those images. #Art #collectiveshout*²⁶

@MelTankardReist needs to be Kirk’d. She ruined the 2025 gaming space, thanks to her company, @CollectiveShout

dox these literal who foods because they took away my loli rape simulators



A.I. Is Making Death Threats Way More Realistic

Online harassers are generating images and sounds that simulate their victims in violent situations.



Caitlin Roper, a member of Collective Shout, an Australian activist group, was recently threatened online with violent A.I.-generated images depicting herself. Charlotte Hadden for The New York Times



By Tiffany Hsu

Tiffany Hsu has written for years about benefits and abuses of generative artificial intelligence.

Oct. 31, 2025 Updated 6:12 p.m. ET

Coralie fought to prevent deepfake abuse. Then the trolls came for her

Violent AI-generated abuse material targeting Australians is posing a national security risk, experts have warned.

Kayla Olaya
DECEMBER 2, 2025



Coralie Alison has been the victim of a new form of AI deepfakes depicting her death and rape. EDDIE JIM

Other content was clearly intended to inflict emotional distress:

I want to kidnap every single member of Collective Shout, amputate all their limbs, throw them into a pool of concentrated sulfuric acid, grind their remaining bones into pieces, mix them with human excrement to make fertilizer, use that fertilizer to grow plants for paint materials, and then use that paint to create and publicly display works of fiction depicting sexual violence.

@meltankardreist oh look, a talking set of holes. Preper them good, I'm gonna shove a machete in every single one of them!

Stupif dumb fuck i hope you get grape fucking cock sucker bitch

Imagine being so miserable an childless that you feel the need to huff an puff over what people do with their private time. You are all hypocrites and losers. Spend less time being upset at nothing an more time building s family you barren wombed cunt

I hope you got raped by your daddy growing up You clearly fucking deserved it you soulless cunt.

You deserve to be slowly raped to death as punishment for being pro-censorship you miserable cunt. Do the world an actual favor and kill yourself.

You deserve to burn to death screaming in agony. Censorship is evil, period. May you be raped, repeatedly, for fun, by every man in your life.

Doxxing and Incitement

The following email was sent to almost all Collective Shout's staff and board:

Good evening, ladies, or, better call you dull chickens... I have all your GEO, addresses, your study places, your realitive's lists, your numbers and much much more... You made me sad deleting the game I really like to play. Now it is my turn, just watch around walking by the streets, I am always near. KEEP IT IN MIND: NO MERCY²⁷

Doxxing was organised via Reddit and hosted via the soyjak and doxbin platforms. As a result of the soyjak raid, personal profiles on former and two current team members were publicised. X users misrepresenting Collective Shout's advocacy aimed to incite participation in volumetric submissions of complaints to Mastercard.

In addition to platform failures, law enforcement and regulatory authorities (with some limited exceptions) were unable to prevent or remedy this abuse.

Platform, regulatory and criminal justice system limitations and failures

Our experience illustrates the critical failures and limitations of platform, regulatory and criminal justice systems which are supposed to protect women, including those in small civil society organisations like ours, when they engage in the digital public square. We are exhibit A in the failure of systems to protect women who are subjected to serious harm simply because they are women advocates leading successful campaigns for the safety of women and girls.

Online platforms and Australian regulatory and law enforcement authorities failed to contain the abuse, and at times (inadvertently) amplified it. Doxxing repositories exposing team members' addresses took months to get removed. One still remains on a doxxing platform. Mass false reporting campaigns succeeded in getting our own accounts suspended, while the genuine abuse driving those campaigns stayed online, uncontested.

Today, more than a year later we continue to be subjected to abuse. The abuse, while now not as intense, is ongoing despite multiple reports by us to platforms whose Terms of Service purport to prohibit such activity, to police in reliance on Australian Commonwealth and state/territory laws criminalising such activity,²⁸ and to Australia's online safety regulator in reliance on national regulatory schemes for online safety.²⁹

We are exhibit A in the failure of systems to protect women who are subjected to serious harm simply because they are women advocates leading successful campaigns for the safety of women and girls.

As regulatory analysis by Reset Australia in 2024³⁰ and Collective Shout's subsequent experience indicate, important lessons for governments in Australia and abroad about digital threat and the shortcomings of existing systems for online safety include the following:

- Voluntary and co-regulatory schemes can be ignored by platforms
- Reputational risk is not serving as an incentive for voluntary implementation of protections for the public
- Fines can be dismissed by very large platforms as simply the cost of doing business, or even ignored altogether
- Complaints, reporting, and take-downs are essential but they are not enough
- Anonymous hostile actors, behind their laptops, PCs and phones, know they are often able to violate Australian laws with impunity.

Platform response

Our reports of harassment and abuse to online service providers were largely ineffective. Material that should have been removed was not removed or was only removed following a significant delay. Content that had

been reported and appropriately removed was regularly reposted, requiring the same content to be reported multiple times. A number of abusive end-user accounts were not suspended at all, or accounts were suspended for a few days only, following which further abusive content was posted. Service providers did not take sufficient proactive steps to monitor and prevent abusive material being posted in the context of what was clearly a volumetric attack on the women of Collective Shout.³¹

In many cases X refused to remove content, which was clearly threatening or sexually abusive, on the basis that it did not break the platform's safety rules. When X refused to remove a post integrating the likeness of a Collective Shout team member into a pornographic scene, it offered the following explanation:

Here's a summary of what isn't allowed on X, according to our safety policies:

- Threatening violence against someone or a group of people
- Celebrating or praising violence
- Harassing someone or encouraging people to harass someone
- Wishing harm on someone
- Promoting violence, threatening, or harassing people because of their identity (e.g. race, gender)
- Promoting or encouraging suicide or self-harm
- Images or videos that show sexual violence and assault
- Child sexual exploitation
- Threatening or promoting terrorism or violent extremism

When Collective Shout team member, Caitlin Roper, posted about a rejected report on X to draw attention to the platform's poor responses, she was reported and had her own account locked – punished for complaining about the system failing her.

The response of Australian authorities

Responses from Australian authorities to our requests for intervention were, on the whole, inadequate to protect us.

Regulatory response

Over the past year, we have actively sought the assistance and protection of Australia's regulatory system for online safety, under the administration of eSafety.

As victims of TFVAW experiencing ongoing and serious harm, our engagement with the regulatory system left us feeling not only unprotected but also, in some cases, overwhelmed and re-traumatised by the onerous burden placed on complainants in reporting. This was a significant challenge for us when attempting to meet requirements to report material under the relevant eSafety reporting

As victims of TFVAW experiencing ongoing and serious harm, our engagement with the regulatory system left us feeling not only unprotected but also, in some cases, overwhelmed and re-traumatised

scheme, each operating under distinct legal frameworks, with different (and extensive) information required to assess whether content meets the relevant thresholds for each scheme.

While their responses were largely limited and inadequate, we acknowledge eSafety's attempts to assist us – for example, when material which was the subject of a complaint by members of Collective Shout was assessed to meet the requisite threshold for removal of material under the Online Content Scheme, eSafety took steps to ensure its removal.³² However, in our experience, even when there was direct regulatory intervention, the regulatory system failed us. When eSafety issued its initial notice to the message board soyjak for hosting a doxxing campaign against Collective Shout, the notice was publicly posted and mocked, serving to reignite the abuse rather than end it. A formal takedown notice was eventually complied with, however a second thread was replicated and the process needed to be repeated.

We recognise that eSafety's responses to our requests for intervention through the past year have been limited by legislative, systemic and structural factors. Amongst other things, we learnt the following when we sought eSafety's assistance:

- eSafety does not have the power under its Adult Cyber Abuse Scheme or its Image Based Abuse Scheme to proactively monitor accounts or monitor previously reported content. eSafety also does not have 'own motion powers' to further investigate associated harm through either of these schemes.
- Platforms are not obliged to act in response to eSafety notifications reporting breaches of their platform Terms of Service if these notifications are issued on a voluntary and informal basis.
- 'Volumetric' or 'pile-on' attacks are not currently defined under eSafety's legislation and eSafety does not have a notification power to put the onus back on platforms to manage such abuse.
- When eSafety considers whether abusive material meets the requisite threshold of intent to cause serious harm (particularly under the Adult Cyber Abuse Scheme), it does so in relation to individual instances of abuse rather than cumulatively. This high bar does not allow the full extent of a volumetric attack, such as that launched against us, to be properly considered.
- Under the Adult Cyber Abuse Scheme, eSafety cannot issue removal notices for abusive material until 48 hours after the complainant has reported the material to the platform.
- eSafety does not have account removal powers, even in cases of egregious harm.
- Under the Online Content Scheme scheme, eSafety can exercise regulatory powers, including proactively to address systemic behaviour likely to impact a broad sector of the Australian community. However –

- under the scheme, the threshold for eSafety to issue a notice for removal of material in relation to incitement, particularly in cases involving threats or encouragement of violence, is very high.³³
- with the high volume of complaints received under the scheme, eSafety does not have sufficient resourcing or tools to proactively monitor re-sharing of material or posting of similar material after a notice has been complied with by the service provider and material has been removed.

We acknowledge the direct and personal engagement of the eSafety Commissioner in consideration of our concerns following escalation of our complaints in October 2025. However, in the absence of effective regulatory powers, tools and resources, eSafety's responses continue to be inadequate to protect us, or to hold platforms and abusers accountable. We discuss the critical need and opportunities for regulatory reform to better protect women against TFVAW below.

Criminal justice response

Through the course of the past year, police responses to our reports left us concerned that the criminal justice system would provide little or no protection from the serious abuse we were being subjected to.

Reporting to police in the different Australian state/territory jurisdictions where we were located, we found police responses were inconsistent and unclear. In some instances, police referred us to eSafety. In others, police indicated that nothing could be done without the identity of the end user.

To some extent, variability in federal, state and territory laws and policing protocols and practices may have contributed to inconsistency in, or uncertainty related to, criminal justice responses. Additionally, apart from our own location as individuals in different Australian jurisdictions, it was clear that the perpetrators were located in Australia and abroad. Clearly, the challenges of jurisdictional variability are exponentially compounded where perpetrators are located in, and acting across, multiple jurisdictions internationally.

We recognise that police and prosecutors face their own structural as well as jurisdictional limits, with borderless cybercrimes posing real challenges for investigation and prosecution. For example, we know that cybercrimes like the denial of service attack used against Collective Shout are notoriously hard to trace back to a specific person. We also know that, apart from identifying responsible actors, cybercrime raises complexities with different and overlapping jurisdictions and the application of sometimes inconsistent and conflicting laws, systems and protocols for detection, prevention and response. While police response to date has been limited, we note that police investigation is continuing and we are hopeful that ongoing criminal justice processes may yield better outcomes.

More broadly, we note that our experience demonstrates the importance of coordinated investigation and prosecution efforts across Australian and international jurisdictions in cases of internationally coordinated TFVAW. Legislative, policy, structural and systemic measures for greater consistency and cooperation in criminal justice responses, both nationally and internationally, are necessary to better prevent, detect and address the serious real-world harms which result from borderless cybercrimes against women.

Conclusion: an urgent need for reform

Globally and at home in Australia, we urgently need online safety reform – especially given the apparent incapacity and/or unwillingness on the part of online service providers to ensure the safety of their products and services.

We have outlined our recommendations for reform below. We believe that implementation of such reforms, along with others, will assist to better prevent, detect and respond to TFVAW. Importantly, by promoting women's safety, effective reforms can support women to exercise their rights to freedom of opinion and expression in the digital public square as they should – without fear of harm.

Amongst other things, our recommended reforms recognise the urgent need for a comprehensive legal and policy response criminalising the solicitation, creation, distribution, facilitation, and possession of SDFs and the technologies that enable them.^{34 35}

Our recommended reforms continue our call for an immediate, global ban on nudifying tools in unity with an open letter endorsed by 434 public institutions, civil society organisations, companies, and individual signatories including INHOPE, Internet Watch Foundation, National Center for Missing and Exploited Children, and WeProtect Global Alliance.³⁶ All SDF generators should be banned along with other related tools that have the primary purpose of creating non-consensual sexual imagery.³⁷

Our recommendations also recognise the need for reforms to reduce the burden for action on the end user (either by Terms of Service, Community Standards, or reporting and complaint mechanisms - all of which failed in our experience). We believe that reforms are urgently needed to shift responsibility to platforms and other online service providers and the systems they create. In this respect, we note the Commonwealth Government's commitment to prioritise enactment of an overarching Digital Duty of Care.³⁸ This would require online service providers to take reasonable steps to prevent foreseeable harms, based on risk assessment, mitigation, and safety by design principles.³⁹ We believe this reform should be accompanied by enforceable regulations, meaningful penalties for breaches, and a more empowered regulator.

We welcome the Australian Government's commitment to online safety reform, including implementation of a number of important reforms in addition to a statutory Digital Duty of Care, in response to the recommendations of the 2024 Independent Statutory Review of the Online Safety Act.⁴⁰ These reforms will, we hope, go some way towards future prevention and mitigation of harms to women, such as those we have experienced over the past year, and to holding online service providers to account.

However, we note that the Government has declined to commit to implementing other significant recommendations from the Independent Statutory Review that we consider would also be critical for the protection of women from TFVAW. These include recommended reforms which would:

- lower the threshold for the Adult Cyber Abuse Scheme and enable cumulative harm to be considered in cases of volumetric attack⁴¹
- strengthen eSafety's capacity to respond with (a) additional powers for notices to end-users to stop posting cyber abuse, subject to a civil penalty for non-compliance and (b) a definition of online hate material including attacks against a person based on gender or other protected characteristics⁴²
- define 'volumetric attack' and empower the regulator to issue a notice(s) to multiple platforms based on a single complaint to address volumetric attacks; empower the regulator to require a service to provide information in relation to a suspected volumetric attack, to undertake remedial actions and to report back on steps taken⁴³
- include consistent powers across the eSafety schemes to require end-users to remove content and refrain from posting abuse in the future.⁴⁴

While the Government has noted challenges and complexities in relation to implementing such reforms, it has indicated they will be given some consideration – including consideration, in some cases, of whether the intent of recommendations could be captured in the development of the statutory Digital Duty of Care. Noting the ongoing escalation of risks to women in a fast-evolving and inadequately regulated digital environment, we urge the Government to pursue and prioritise implementation of reforms which would directly address TFVAW and provide women with effective protection from serious harm.

Further, if regulatory and criminal justice authorities are to become, and remain, sufficiently responsive to serious risks and real-world harms of TFVAW, we need more than one-off reform packages. Ongoing, regular and timely review and strengthening of laws, systems, and processes and increased resourcing for responsible authorities in our continually evolving digital environment are critical.

Noting the ongoing escalation of risks to women in a fast-evolving and inadequately regulated digital environment, we urge the Government to pursue and prioritise implementation of reforms which would directly address TFVAW and provide women with effective protection from serious harm.



(L-R) Lyn Swanson Kennedy, Renee Chopping, Caitlin Roper, Coralie Alison, Melinda Tankard Reist

Recommendations

Recommendation 1: Prioritising reforms to address Tech Facilitated Violence Against Women

The Australian Government should prioritise implementation of legislative and policy reforms which address Tech Facilitated Violence Against Women (TFVAW) and provide effective protection from gender-based harm, including reforms recommended by the 2024 Statutory Review of the Online Safety Act 2021.

Recommendation 2: Defining serious harm for the purposes of the new statutory Digital Duty of Care

- a. The Australian Government should ensure that legislation for the proposed new statutory Digital Duty of Care clearly and explicitly includes gender-based harm, along with other types of harm – most particularly child-related harm – as harm which falls under the Digital Duty of Care for online service providers.
- b. For the purposes of identifying whether incidents or risks of tech facilitated gender-based harm amount to incidents or risks of ‘serious harm’ under the proposed new statutory Digital Duty of Care, legislation and statutory guidance should provide that:
 - assessment of ‘serious harm’ is not limited to individual instances of harmful gender-based content or activity
 - while repeated instances of harmful gender-based content or activity may not reach the proposed ‘serious harm’ threshold when considered in isolation, they may do so when considered collectively and cumulatively.

Recommendation 3: Rules for compliance with the new statutory Digital Duty of Care

- a. The eSafety Commissioner should be empowered to create mandatory rules for how relevant online service providers can comply with the new Digital Duty of Care requirements, including rules which specifically address TFVAW.
- b. The eSafety Commissioner’s rules should require relevant online service providers to implement systems and processes for the following (amongst other things):
 - proactive and routine scanning, automated detection and flagging, and takedown of sexual digital forgeries (SDFs)
 - design of generative AI tools to prevent the creation of SDFs, including, for example, through data and content provenance,⁴⁵ detectable watermarks, and labelling with persistent and verifiable markers

- prioritising and actioning of reports by victims of TFVAW
- anonymous reporting to user-generated content platforms by anyone (without requiring reporters to have a platform account in order to report) if they see harmful gender-based content on those platforms
- proactive and routine monitoring for early detection of coordinated campaigns of TFVAW
- prevention and disruption of coordinated campaigns of TFVAW
- timely referral of TFVAW to regulatory and law enforcement authorities
- continued monitoring with appropriate and timely reporting of ongoing or further instances of TFVAW by service users who were previously reported to authorities for TFVAW
- platform bans on account holders who engage in TFVAW which results in serious harm or creates risk of serious harm
- termination, by hosting providers and domain name registrars, of services to sites that actively promote TFVAW which results in serious harm or creates risk of serious harm
- ongoing, proactive and transparent assessment, review and disruption of metrics used to drive algorithms which promote TFVAW in particular cases and more broadly across a platform
- regular assessment and continuous improvement of monitoring, reporting and review functions – especially automated or AI-based safety-critical reports – for efficacy and reliability in addressing TFVAW.

Recommendation 4: Platform Terms of Service

- a. The eSafety Commissioner’s rules for compliance with the new statutory Digital Duty of Care should require platforms to publish Terms of Service which, amongst other things:
 - are published, along with every update to the Terms of Service, on a public repository
 - set out the platform’s commitment to meeting, and how it will meet, its Digital Duty of Care obligations
 - are legally binding, with relevant breaches by the platform going to evidence breach of their Digital Duty of Care.
- b. Platforms should be required to set out, in their Terms of Service, transparent and procedurally fair rules and processes for banning account holders. These should include relevant considerations and processes for:
 - decisions to ban account holders on the platform
 - notifying account holders when they are banned

- any exceptional circumstances in which account holders may not be notified – for example where such notification would create risk of serious harm to others, or compromise criminal investigation
- appeal, review and overturning of bans.

Recommendation 5: Banning tools for creating non-consensual sexual imagery

- a. The Australian Government should prioritise development of legislation to ban all nudifying/undressing apps and SDF generators, and any other related tools that have the primary purpose of creating non-consensual sexual imagery.
- b. The Australian Government, the eSafety Commissioner and law enforcement authorities should work with international counterparts to identify statutory and other cross-border mechanisms to prohibit and effectively prevent search engines and app stores from surfacing, selling or distributing nudifying/undressing apps, SDF generators and other related tools.

Recommendation 6: Criminalising Tech Facilitated Violence Against Women

The Australian Government should work with state and territory governments to review, strengthen and harmonise criminal law provisions for TFVAW – and particularly image based sexual abuse – across Australian jurisdictions. This should include criminal laws which operate consistently across all Australian jurisdictions to:

- make it a serious offence to participate in TFVAW which is coordinated and exposes victims to risk of serious harm
- specifically address synthetic/AI generated content, including through clear provisions for:
 - standalone offences for creating, soliciting, distribution, transmitting, possessing, and facilitating SDFs (such offences should be based on the absence of consent, not on perpetrator intent)
 - aggravated and repeat offences.

Recommendation 7: Compliance and deterrence

The Australian Government should, in collaboration with state and territory governments, pursue legislative reforms to more effectively promote compliance and deterrence with stronger civil and criminal penalties and executive liability for breaches and offences related to TFVAW.

Recommendation 8: International cooperation

The Australian Government, the eSafety Commissioner and Australian law enforcement authorities should work with international counterparts to improve international cooperation for cross-border prevention, detection, removal, investigation and prosecution of TFVAW and redress for victims.

Recommendation 9: Resourcing for training, education, and victim support

The Australian federal, state and territory governments should collaborate to ensure adequate funding and resourcing nationally for:

- trauma-informed counselling services, helplines, and legal aid for victims of TFVAW
- targeted training for law enforcement, prosecutors, and judiciary on evidence, technology, and victim impacts related to TFVAW
- public education campaigns and practical resources for young people, schools and the broader community to increase understanding of harms and legal consequences of TFVAW, encourage appropriate reporting, and promote awareness of available supports for victims.

Recommendation 10: Ongoing consultation with stakeholders

The Australian Government and the eSafety Commissioner should continue to proactively engage with women's safety advocates and experts in ongoing consultation for legislative reform and regulatory policy design related to TFVAW.

Endnotes

- 1 Scolyer-Gray, P. (2026). Technology facilitated violence against women: Documentation and analysis of online abuse targeting Collective Shout. Online Hate Prevention Institute.
- 2 Musk, E. [@elonmusk] (2025, 21 July). Bravo [Post]. X. <https://x.com/elonmusk/status/1947201628085612632>. At the time, the petition re-posted by Musk explicitly named and targeted Collective Shout. It was later amended, naming 'Activist Groups' instead, in a less explicit reference to Collective Shout.
- 3 In this report, we use the term Tech Facilitated Violence Against Women (TFVAW) to refer to online and other technology-facilitated violence which targets women due to their sex or affects them disproportionately. TFVAW impacts women offline as well as online, with real-world harm including physical, sexual, psychological, social, political, or economic harm, and other infringements of women's rights and freedoms.
- 4 See Rickard, D. (2024, October). Report of the Statutory Review of the Online Safety Act 2021. Commonwealth of Australia. <https://www.infrastructure.gov.au/sites/default/files/documents/report-of-the-statutory-review-of-the-online-safety-act-2021-february-2025.pdf>
- 5 For how our campaign started, see Roper, C. (2025, 7 April). "'F*ck your mom': Rape + incest game available on 12+ gaming platform Steam." Collective Shout. <https://www.collectiveshout.org/no-mercy-game-steam>; Collective Shout. (2025, 9 April). '@Steam: remove No Mercy rape + incest game globally NOW!' Change.org. <https://www.change.org/p/steam-remove-no-mercy-rape-incest-game-globally-now>. See also Roper, C. (2025, 13 April). "'Not real', 'freedom of expression', 'don't like it, don't play': Responding to gamers defences of Steam rape game." Collective Shout. <https://www.collectiveshout.org/responding-to-gamers-defences>. For a more comprehensive account of how our No Mercy and Steam/itch.io campaign subsequently unfolded, progressing to the removal of games from the Steam and itch.io platforms, see the OHPI Report. Scolyer-Gray, P. (2026). Technology facilitated violence against women: Documentation and analysis of online abuse targeting Collective Shout. Online Hate Prevention Institute, pp8-13.
- 6 Ibid., p5.
- 7 Collective Shout (2025, 7 August). "Horrific": UN Special Rapporteur on Violence against Women and Girls condemns online abuse against our team. Collective Shout. <https://www.collectiveshout.org/unsr-condemns-abuse>
- 8 McGlynn, C. and Toparlak, R. T. (2025, 2 April). The 'new voyeurism': criminalizing the creation of 'deepfake porn'. J Law & Society 52(2):204-228. <https://doi.org/10.1111/jols.12527>
- 9 Scolyer-Gray, P. (2026). Technology facilitated violence against women: Documentation and analysis of online abuse targeting Collective Shout. Online Hate Prevention Institute, Fig. 119, p. 100.
- 10 This complemented and extended the European Commission's investigation previously launched on 18 December 2023, into X's compliance with its recommender systems risk management obligations. European Commission. (2026, 26 January). Commission investigates Grok and X's recommender systems under the Digital Services Act. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203; European Commission. (2023, 17 December). Commission Opens Formal Proceedings Against X Under the Digital Services Act. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709
- 11 Comment by Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy. European Commission. (2026, 26 January). Commission investigates Grok and X's recommender systems under the Digital Services Act. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203
- 12 Alsalem, R., Working Group on the issue of human rights and transnational corporations and other business enterprises, & Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (2026, 4 February). Ref.: AL AUS 1/2026 [Letter]. United Nations Office of the High Commissioner for Human Rights. <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gld=30725>. Response here: Walsh, C. (2026, 2 April). Ref.: AL AUS 1/2026 [Letter]. Permanent Mission of Australia to the United Nations, Geneva; United Nations Office of the High Commissioner for Human Rights. <https://spcommreports.ohchr.org/TMResultsBase/DownloadFile?gld=39657>
- 13 Posetti, J., Williams, K., Hellmueller, L., Renaud, P., Shabbir, N., and Aboulez, N. (2026). Tipping Point: online violence impacts, manifestations, and redress in the AI age. UN Women. <https://www.unwomen.org/en/digital-library/publications/2026/04/tipping-point-online-violence-impacts-manifestations-and-redress-in-the-ai-age>
- 14 See for example, Posetti, J., Hellmueller, L., Williams, K., Renaud, P., Aboulez, N., and Shabbir, N. (2025). Tipping Point: The Chilling Escalation of Online Violence Against Women in the Public Sphere UN Women. This report was produced by UN Women in collaboration with St George's University, UNESCO, and the International Center for Journalists. See also eSafety Commissioner (2022). Women in the Spotlight: Women's experiences with online abuse in their working lives. eSafety Commissioner. <https://www.esafety.gov.au/research/how-online-abuse-impacts-women-working-lives> Collective Shout also raised this issue in a recent submission to the New Zealand Parliament. See Collective Shout. (2026). Submission to the Social Services and Community Committee on the Deepfake Digital Harm and Exploitation Bill (NZ). https://assets.nationbuilder.com/collectiveshout/pages/19424/attachments/original/1783053638/New_Zealand_Deepfake_Digital_Harm_and_Exploitation_Bill_2026.pdf See also: Collective Shout. (2025). Submission to OHCHR Call for inputs for the study of the Human Rights Council Advisory Committee on technology-facilitated gender-based violence (HRC resolution 56/19). Collective Shout. https://assets.nationbuilder.com/collectiveshout/pages/11735/attachments/original/1741247539/Submission_to_the_Call_for_inputs_for_the_study_of_the_Human_Rights_Council_Advisory_Committee_on_technology-facilitated_gender-based_violence_%28HRC_resolution_56_19%29.pdf?1741247539
- 15 Amongst the abusive tirades, positive and supportive contributions to online discussions could be found but were suppressed by the sheer numbers of abusive comments, and by the platforms' built-in tools, such as downvoting on Reddit.
- 16 Musk, E. [@elonmusk]. (2025, 21 July). Bravo [Post]. X. <https://x.com/elonmusk/status/1947201628085612632>
- 17 See Figure 71 in the OHPI Report. Scolyer-Gray, P. (2026). Technology facilitated violence against women: Documentation and analysis of online abuse targeting Collective Shout. Online Hate Prevention Institute, p. 69.
- 18 Where not otherwise referenced, abusers' comments, messages and posts set out in our report are documented and referenced in the OHPI Report. See Scolyer-Gray, P. (2026). Technology facilitated violence against women: Documentation and analysis of online abuse targeting Collective Shout. Online Hate Prevention Institute. Spelling and grammatical errors appear in our report as in the original records of comments, messages and posts.
- 19 See Figs. 72–74 in the OHPI Report. Scolyer-Gray, P. (2026). Technology facilitated violence against women: Documentation and analysis of online abuse targeting Collective Shout. Online Hate Prevention Institute, p. 70.
- 20 Ibid. Fig. 75, p. 71.
- 21 Ibid., Fig. 80, p. 74.
- 22 Ibid., Fig. 81, p. 75.
- 23 asmongold247. (2025, 22 August). Pt1. When does the government step in? #collectiveshout #asmongold #valve #steam #paypal #mastercard #visa #asmongold247 #gaming #news #reacts #fyp #drama... [TikTok video].TikTok. <https://www.tiktok.com/@asmongold247/video/7541172163890449686>
- 24 Scolyer-Gray, P. (2026). Technology facilitated violence against women: Documentation and analysis of online abuse targeting Collective Shout. Online Hate Prevention Institute. Fig. 76, p. 71.
- 25 Ibid. Fig. 78, p. 73.
- 26 "R34" is short for 'Rule 34', the 34th of a list of axioms about the internet that originated on 4chan which states, "there is porn of it, no exceptions."
- 27 This is a reference to *No Mercy* – the first rape simulation game we exposed on Steam, after which the broader campaign followed. <https://www.collectiveshout.org/no-mercy-game-steam>
- 28 These include criminal offences created by the Commonwealth's Criminal Code Amendment (Deepfake Sexual Material) Act (2024) and other laws at state/territory level.
- 29 We made reports to eSafety under the Image Based Abuse Scheme. This scheme operates under the Online Safety Act 2021 (Cth) to empower eSafety to remove and take action against the non-consensual sharing of, or threat to share, an intimate image online. We also reported to eSafety under the Adult Cyber Abuse Scheme. This scheme operates under the Online Safety Act 2021 (Cth) to empower eSafety to act in response to online communication (including a post, comment, email, message, meme, image or video) to or about an Australian adult which is intended to cause them serious psychological or physical harm and which is menacing, harassing or offensive in all the circumstances. Additionally, we reported to eSafety under the Online Content Scheme. Also operating under the Online Safety Act 2021 (Cth), this scheme enables reports of online content where it is suspected that Australians can access Class 1 or Class 2 material online. This includes illegal material which is prohibited under Australian law, or restricted material which is or is likely to be either refused classification or classified as restricted under Australia's National Classification Scheme. eSafety may carry out investigations under the Online Content Scheme, either in response to a complaint or on eSafety's own initiative.
- 30 Reset Tech Australia. (2024, November). Five Necessary Elements for Effective Digital Platform Regulation. Reset Tech Australia. <https://au.reset.tech/uploads/5-Necessary-Elements-for-Effective-Digital-Platform-Regulation.pdf>
- 31 For example, simple image detection software could have been used to prevent the re-posting of the same sexual digital forgeries.
- 32 This was material which met the high threshold for assessment as Class 1 material under the Online Content Scheme (see also note below).
- 33 The material must have been, or be likely to be, classified as Refused Classification (RC) by Australia's Classification Board (Class 1 material). The legal threshold for what would be considered Class 1 material in relation to incitement in cases involving threats or encouragement of violence is very high.
- 34 McGlynn, C. and Toparlak, R. T. (2025, 2 April). The 'new voyeurism': criminalizing the creation of 'deepfake porn'. J Law & Society 52(2):204-228. <https://doi.org/10.1111/jols.12527>
- 35 Van der Watt, M. and Rousay, V. (2024, 2 February). Submission: Request for information by the National Institute of Standards and Technology (NIST): Assignments under the Executive Order Concerning Artificial Intelligence. National Center on Sexual Exploitation. <https://www.nist.gov/system/files/documents/2024/02/15/ID035%20-%202024-02-02%2C%20National%20Center%20on%20Sexual%20Exploitation%2C%20Comments%20on%20AI%20EQ%20RFI.pdf>
- 36 Child Helpline International. (2026, 10 February). Unifying Voices Worldwide: No to Nudify. [Statement]. https://childhelplineinternational.org/wp-content/uploads/2026/02/No-to-Nudify-Statement_Final-with-Endorsements_ENG.pdf
- 37 Many such apps rebrand after takedown, reappearing under a different name and category. Daffalla, A., Chao, S. and Zeng, E. (2026, 23 May). Dual-Use AI Face Swap Apps Are Mostly Unsafe: A Systematic Safety Audit. Arxiv. <https://arxiv.org/abs/2605.24735>
- 38 A statutory Digital Duty of Care was a core recommendation of the 2024 Statutory Review of the Online Safety Act. See Rickard, D. (2024, October). Report of the Statutory Review of the Online Safety Act 2021. Commonwealth of Australia. <https://www.infrastructure.gov.au/sites/default/files/documents/report-of-the-statutory-review-of-the-online-safety-act-2021-february-2025.pdf>
- 39 The promised statutory duty will apply to a wide range of online services including social media, messaging apps, search engines, hosting services, generative AI/chatbots, online games, dating services, app stores, pornography services and more. It is not intended to replace any existing complaint or takedown schemes. See Australian Government (14 Apr 2026). Government Response to the Independent Review of the Online Safety Act 2021. <https://www.infrastructure.gov.au/sites/default/files/documents/govt-response-to-the-independent-review-online-safety-act-2021.pdf>
- 40 Rickard, D. (Oct 2024). Report of the Statutory Review of the Online Safety Act 2021. Commonwealth of Australia. <https://www.infrastructure.gov.au/sites/default/files/documents/report-of-the-statutory-review-of-the-online-safety-act-2021-february-2025.pdf>
- 41 Ibid. See Recommendations 18 and 22.
- 42 Ibid. See Recommendations 20 and 21.
- 43 Ibid. See Recommendations 23 and 24.
- 44 Ibid. See Recommendation 40.
- 45 For example, standards like C2PA. Coalition for Content Provenance and Authenticity. (n.d.). Advancing digital content transparency and authenticity. [Home Page]. <https://c2pa.org/>