

House of Representatives Standing Committee on Social Media and Online Safety, 20 January 2022

DIGI's opening Statement to the Committee

Thank you Chair, and to Committee Members, for your time and for the opportunity to appear before this Inquiry into Online Safety and Social Media. My name is Sunita Bose and I am the Managing Director of the Digital Industry Group, or DIGI for short. I'm joined today by my colleague Dr. Jenny Duxbury, DIGI's Director of Policy, Regulatory Affairs & Research.

By way of background, DIGI is a non-profit industry association that advocates for a thriving digitally-enabled economy in Australia, but one where online safety and privacy are protected. That's our vision, and we bring global and Australian technology companies – large and small – together in that vision.

Our founding members are Apple, eBay, Google, Linktree, Meta, Twitter, Snap and Yahoo. Our associate members are Change.org, Gofundme, ProductReview.com.au and Redbubble.

DIGI shares the Government's strong commitment to combating harmful content online. We've been a key partner to the Government in its policy agenda in this area, and I'll highlight two examples.

[Partnership area #1]

DIGI developed *The Australian Code of Practice on Disinformation and Misinformation* to give effect to Australian Government policy in this area, as part of its response to the Digital Platforms Inquiry. We launched this last February.

What does this code mean for Australians?

It's been signed by eight major technology companies, including the major social media platforms. Every company that signs it has agreed to safeguards to protect Australians from harmful disinformation and misinformation online. That includes:

- a. Publishing and implementing policies on their approach
- b. Providing a way for their users to report content that may violate those policies.
- c. Implementing a range of scalable measures that reduce its spread and visibility of mis- and disinformation online.

Signatories also agreed to annual transparency reports about those safeguards.

- d. The first set of reports were released in May 2021, and are available for anyone to read on our website.
- e. The goal behind these transparency reports is to improve public understanding of these challenges over time, and provide new insights into its scale and management.

Last October, DIGI strengthened the code with a facility for the public to make complaints about breaches of the code on our website. Complaints are assessed by an independent complaints committee. We've also appointed an independent reviewer to fact check the claims in signatories' future transparency reports.

As you'll see, our submission has eight recommendations in relation to online harms, and one of them relates to this code.

It is a self-regulatory code and, while we haven't yet seen the ACMA's report on the code that it provided to the Government in June of last year, we have proposed that the Government strengthen the code by empowering the ACMA to provide an appeals role should disagreements arise between complainants and the complaints committee's decisions.

[Partnership area #2]

Another area of DIGI's collaboration with the Government in online safety is our work to develop mandatory industry codes of practice under the Online Safety Act.

The development of these Codes is being led by DIGI and the Communications Alliance, supported by a steering group of other industry associations. The Online Safety Act codes need to be approved and registered by the eSafety Commissioner, so we are working closely with them on this effort throughout the process.

The codes effectively cover the entire Australian digital industry divided into eight industry sections. DIGI is leading the drafting of the chapters of the codes relating to social media services, search engines, and app distribution services.

Once in effect, these codes will standardise industry-wide protections for Australians in relation to Class 1 and Class 2 materials under the Online Safety Act.

So what does that mean for Australians?

The codes will provide a consistent framework for Class 1 and Class 2 materials online across the whole industry, to address the harm caused by that content.

There will be wide range of mandatory measures to address Class 1 materials, which will include obligations to that go well beyond just removing this content, which includes child sexual exploitation material, pro-terror content, and extreme crime and violence.

Class 2 materials must either be removed or have their access restricted for those under 18 years of age. Class 2 materials includes online pornography, X18+ and R18+ content.

The Class 1 code will be registered around July and the Class 2 code around December.

There will be a public consultation process, so that's an opportunity for anyone or any organisations – particularly those who have participated in this inquiry – to participate. We plan to proactively contact interested organisations, and run an inclusive process to make sure we get those codes right.

[Rec #7] As we outline in one of the recommendations of our submission, we believe that the measures under these codes will provide an industry-wide effective approach to protecting minors from many online harms, such as age-inappropriate content.

[Rec #5] We think these should be complemented with economy-wide privacy protections for minors in the Privacy Act. We think that there is an opportunity in the review underway to standardise and strengthen a single set of routine privacy protections that minors, or their guardians, can expect online no matter what digital service they might be using.

[Role of industry]

DIGI has a unique vantage point; we see the extensive work that our members undertake in combating online harms – as well as the work that the industry does together. While our members are best placed to speak about their specific work, DIGI has visibility into how important online safety is to each of them, and can offer a general industry perspective.

DIGI and its members believe that the digital industry has a crucially important responsibility to address online harm.

The management of online harms can never be a “set and forget” exercise; It requires continued and increasing investment in safety – including in *systems and processes* teams and technology – as well as research and partnerships into emerging patterns of abuse and evolving community standards. These are needed to inform continual iteration and improvement.

[Role of Government]

We also believe that Governments have a really important role to play in:

- defining those thresholds of harm
- standardising the protections consumers can expect
- holding industry accountable.

For those government safety nets to work, they need to be:

- effective in their goals of protecting Australians from harm online
- they need to be able to be practically implemented by industry
- reflective of people’s varied experiences online.

As noted, we’ve made eight recommendations to that end in our submission. In the interests of time, I won’t go through all eight – our submission is public and available for all to read, but I’ll just touch on a few of those.

[Rec #1 Streamlining online safety legislation]

One of the observations of those working in this area is that there is a huge amount happening across a range of areas.

The Online Safety Act comes into effect on Sunday. In train are the codes we mentioned, Basic Online Safety Expectations, the Restricted Access Scheme, the Age Verification roadmap, age verification under the Online Privacy Bill, the wider Privacy Act review. There’s

also the (Anti Trolling) Bill and the Review of the Model Defamation Provisions, both related to defamation online.

We've made some recommendations about how we simplify and streamline online safety legislation. We work with companies large and small and it's our view that clarity will aid compliance – particularly for start-ups, new entrants to the Australian market and those without a large local staff presence – who may be struggling to make sense of the complex regulatory environment in Australia.

[Rec #3 Hate speech]

And finally, one of the gaps we have identified in relation to Australian digital policy is in regard to hate speech.

While DIGI's relevant members all have long-standing policies prohibiting hate speech, there is no legal standard nor recourse in this area to incentivise strong action industry-wide.

Australia continues to adopt a narrow approach to hate speech under anti- discrimination laws and the Online Safety Act that's aimed at protecting individuals, rather than groups based on their protected characteristics.

DIGI believes that hate speech should be a broader category of harm that is not limited to religious, gender or race-based discrimination, but includes hate speech related to characteristics including (but not limited to) sexuality, gender identity, disability, and national origin.

We think a clearer legislative framework for hate speech will help relevant stakeholders, including all digital platforms, to better report, review and remove content that meets a defined Australian legal threshold.

There's much more I could say, but I'll leave it there and I look forward to answering your questions along with my colleague Jenny.

Answers to questions on notice

Provided February 3, 2022

CSAM

1. Your submission states that *"DIGI members have zero tolerance for CSAM..."*, but this committee has also heard evidence about the growing volume of CSAM material being identified on your members platforms. How do you reconcile this zero tolerance approach with growing reported volumes of CSAM?

Relevant DIGI members have and continue to make extensive investments in protecting the safety of children from child sexual exploitation material, and their approach reflects a zero tolerance for this abhorrent crime. While specific approaches at a platform-level can vary, in general their work includes

the following areas:

- They have strict policies against child exploitation and the sexualisation of children. These policies are enforced through human review teams who undergo extensive training on the appropriate protocols for the handling of CSAM material, often with machine learning and other technology that surfaces content for review.
- When CSAM is detected it is removed and reported, DIGI members report to the National Center for Missing & Exploited Children (NCMEC) in the United States which refers cases to law enforcement all around the world, including in Australia. They also directly cooperate with Australian law enforcement operations.
- Relevant DIGI members are active in several coalitions, such as the Technology Coalition, the ICT Coalition, the WeProtect Global Alliance, and INHOPE and the Fair Play Alliance, that bring companies and NGOs together to develop solutions that disrupt the exchange of child sexual abuse materials online and prevent the sexual exploitation of children.
- Relevant DIGI members deploy industry-developed and licensed technological tools such as Photo DNA (developed by Microsoft to identify known CSAM in still images) and CSAI Match (developed by YouTube to detect known video-based CSAM) and PDQ+TMK+PDQF (developed by Meta to detect edited versions of known CSAM in images and videos).
- Those that operate messaging platforms also enact safety by design features, such as default privacy settings for minors, and preventing minors from having unwanted interactions from adults.

DIGI notes that much of the data provided about growing amounts of CSAM are actually identified by the providers themselves, through the reporting processes described above. Should the data provided in the submissions from the Office of the eSafety Commissioner¹ and the Department of Home Affairs² be the basis upon which the Committee is basing its question, it is unclear to DIGI which platforms are the basis of these reports, and if the increase is attributable to DIGI's members. DIGI can only offer a perspective on how its relevant members approach CSAM, and has visibility into the extensive work and deep commitment that these companies have to address CSAM on their services. DIGI does not have visibility into how the wider ecosystem of digital and photo-sharing services – on both the dark and clear web – approach these challenges, nor the relationship between those activities and changes in reported volumes in CSAM.

DIGI sees an important upcoming opportunity to standardise protections industry-wide in relation to CSAM in the mandatory codes of practice being developed under the Online Safety Act. DIGI, Communications Alliance and a steering committee of industry associations are working with the Office of the eSafety Commissioner to have the first set of these codes registered around July 2022, and they will be released for public consultation prior to then. DIGI is drafting the chapters of the codes relating to social media services, search engines, and app distribution services. Once the Class 1 code is in effect, it will standardise industry-wide protections for Australians in relation to Class 1 content under Australia's classification code, which includes a range of material including CSAM.

2. Is a zero tolerance approach to CSAM consistent with product developments that impede automated scanning of content on your members platforms for known hashes of CSAM material?

DIGI understands this question as relating to licensed technological tools that have been developed by the technology industry to assist in the detection, disruption, and reporting of millions of child exploitation images. These industry-developed tools include: Photo DNA, developed by Microsoft to

¹ The Office of eSafety Commissioner's submission to the inquiry states: *"In the financial year 2020-2021, eSafety received more than 23,500 public reports. This was an increase of more than 60% on the previous financial year. Overwhelmingly, public reports concern child sexual exploitation material."*

² The Department of Home Affairs submission to the inquiry states: *"The Department of Home Affairs' submission to the inquiry that notes that the Australian Centre To Counter Child Exploitation (ACCCE) noted an increase in 2021 in Member of the Public (MoP) reports of children self-producing CSAM for financial incentives."*

identify known CSAM in still images; CSAI Match, developed by YouTube to detect known video-based CSAM; and PDQ+TMK+PDQF, developed by Meta to detect edited versions of known CSAM in images and videos. DIGI also interprets this question as relating to the relationship between end-to-end encryption and such technology.

It is our understanding that such technology can be used in encrypted services, and that relevant members are considering moves toward encryption slowly and thoughtfully to ensure that there can be actionable referrals of CSAM to law enforcement and the National Center for Missing & Exploited Children (NCMEC). For example, DIGI understands that some platforms are innovating in ways that enable actionable referrals on the basis of non-content signals, so they are not required to see the content and can still make referrals in an end-to-end encrypted environment.

Additionally, DIGI's members also directly cooperate with Australian law enforcement operations under the extensive national security legislation that affords powers with regard to encrypted services. DIGI believes there are a range of opportunities for industry to work with law enforcement to reduce the challenges regarding obtaining digital evidence in encrypted services, and we refer to the Center for Strategic & International Studies' report "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge" and its recommendations to improve the ability of law enforcement to obtain digital evidence in encrypted messages³.

3. Is a zero tolerance approach to CSAM consistent with product developments that assist child abusers to use social media platforms to share CSAM in private messages that neither the platform, nor law enforcement agencies are able to access?

From our vantage point in relation to relevant DIGI's members, we are seeing product features and developments aimed at preventing criminals from using social media and messaging platforms to groom children or to share CSAM.

For example, Instagram defaults users between the ages of 13 and 17 into private accounts upon sign-up, and uses a number of safety measures for users in this category, including making it harder to adults to comment or interact with them, steps to inhibit inappropriate interactions with adults in private messaging, and preventing teens from seeing age-sensitive ads. On Snapchat, default settings for all users prevent receiving a message from someone who is not your friend and location sharing is off by default, and there is no option for users to share location outside of their friend group.

DIGI understands that law enforcement agencies in Australia are able to access private messages under the extensive national security legislation that affords them with these powers, specifically in relation to encrypted communications. For example, the Assistance and Access Act 2018 (Cth), International Production Orders Act 2021 (Cth) and the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021(Cth) provide law enforcement agencies and intelligence organisations with far-reaching powers to access any network, system, device, or user accounts covertly and, where required, with the assistance of the service provider.

DIGI refers to its responses to Question 1 and Question 2 which also provide further context in relation to this question.

³ William A. Carter & Jennifer C. Daskal (2018), *Low-Hanging Fruit Evidence-Based Solutions to the Digital Evidence Challenge: A Report of the CSIS Technology Policy Program*, available at <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>

Safety by Design

4. Your submission states that “DIGI’s members believe in “safety by design”. Does DIGI believe that all of the products and services offered by your members have been developed consistent with the principle of safety by design?

DIGI’s members believe in “safety by design”, and many of them have worked with the Office of the eSafety Commissioner to guide and endorse their principles and assessment tools in this area. DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia, with a focus on Australian public policy relating to online safety and online privacy. DIGI does not undertake assessments of each of our members’ products and services and is therefore not in a position to offer a detailed perspective on this question, but it is our general view that safety by design is a central consideration in our members’ product development.

Disinformation/misinformation

5. Your submission also discusses how the [self-regulatory disinformation code](#) you have developed operates. Are there any mandatory or binding commitments for signatories under this code?

Yes, there are two mandatory code commitments under the *Australian Code of Practice on Disinformation and Misinformation* (ACPDM).

Under mandatory Objective #1, every signatory has agreed to safeguards to protect Australians from harmful mis- and disinformation. This includes:

- Publishing & implementing policies
- Providing users with a way to report content against those policies
- Scalable measures that reduce its spread & visibility

Under mandatory Objective #7, every signatory has agreed to annual transparency reports about those safeguards. The first set of reports were released in May 2021 on DIGI’s website. These will improve understanding of both the management and scale of mis- and disinformation in Australia. In October 2021, DIGI announced the appointment of an independent expert to fact check and attest signatories’ annual transparency reports going forward under the code, in order to incentivise best practice and compliance.

In addition to these two mandatory commitments, there are a series of opt-in commitments that platforms adopt if relevant to their business model.

- (Objective #2) Addressing disinformation in paid content.
- (Objective #3) Addressing fake bots and accounts.
- (Objective #4) Transparency about the source of content in news and factual information (e.g. promotion of media literacy, partnerships with fact-checkers)
- ...and (#Objective 5) political advertising.
- (Objective #6) partnering with universities/researchers to improve understanding.

6. Is it the case that the only binding commitments on signatories to this code are to implement policies on disinformation/misinformation, offer a complaints mechanism to end-users and publish an annual transparency report on what they are doing in this space? Are there penalties of any kind associated with the code?

Please refer to Question 5 in relation to the mandatory commitments under the code. DIGI notes that The Government asked the digital industry to develop a voluntary code of practice on disinformation, and specifically asked the industry to draw learnings from the European Union Code of Practice on Disinformation.

The EU code provides an opt-in model to reflect the highly diverse nature of the digital industry, allowing different businesses to focus where they are best placed to contribute. Unlike the EU, the Australian code has mandatory commitments that all signatories must adopt. Like the EU, it offers some additional commitments that companies can choose if they are relevant to their business.

In October 2021, DIGI announced the strengthening of the *Australian Code of Practice on Disinformation and Misinformation* through the appointment of an independent Complaints Sub-Committee comprised of Dr Anne Kruger, Victoria Rubensohn AM and Christopher Zinn to resolve complaints about possible breaches by signatories of their code commitments. DIGI also launched a portal on its website for the public to raise such complaints⁴. As part of these new governance arrangements, DIGI released publicly the terms of reference for the complaints facility⁵ on our website which includes significant detail about its operation, including penalties associated with non-compliance. An excerpt of the relevant section of these terms of reference is included below:

The Complaints Sub-committee can decide the resolution of a complaint about a potential material breaches of the Code based on the severity of the breach as outlined below:

- i) If not serious → direct discussion.* For a non-serious breach, such as a failure to publish a policy for a short period of time due to a technical issue, the Complaints Sub-committee will discuss the issue with the Signatory, with the aim of managing the risks of a repeat breach.
- ii) If more serious → a public statement explaining the issue and steps agreed:* If the Complaints Sub-committee determines a Signatory may have violated one or more mandatory commitments under the Code and the matter is serious enough to require corrective action and informing the public, the Complaints Sub-committee will discuss the issue with the Signatory and may issue a statement to be published on the DIGI website explaining its stance and steps agreed to resolve the issue. This would also be noted in DIGI's annual report on code administration. The relevant Signatory may also issue a public response on the matter, either on the DIGI website or via any other means it chooses.
- iii) If it appears more serious and would take time to resolve → an allowance period for that resolution to occur.* If the Complaints Sub-committee determines a Signatory may have seriously breached the Code and is willing to take corrective action but needs more time to do so, the Complaints Sub-committee may allow the Signatory reasonable time for this to take place. The time allowed will be limited to a maximum of three months.
- iv) If it appears more serious but needs investigation → an allowance period for that investigation to occur.* If the Complaints Sub-committee determines that the Signatory may have seriously breached the Code but cannot agree a response with the Signatory, they may allow a period of time to conduct that investigation before deciding on action. The time allowed for investigation and resolution will be limited to a maximum of six months.

⁴ DIGI Media Release (11/10/21), "Australian disinformation code of practice strengthened with independent oversight and public complaints facility", available at <https://digi.org.au/in-the-media/australian-disinformation-code-of-practice-strengthened-with-independent-oversight-and-public-complaints-facility/>

⁵ DIGI, *Terms of reference for Complaints Facility and Complaints Sub-committee | The Australian Code of Practice on Disinformation and Misinformation*, available at <https://digi.org.au/wp-content/uploads/2021/10/DIGI-TOR-for-Complaints-Facility-and-Complaints-Sub-committee--ACPDM--FINAL-NE-1.pdf>

v) If the Complaints Sub-committee determines the issue is serious, and the Signatory refuses to take remedial action or cooperate in an investigation or correction not possible → withdrawal of signatory status. *If the Complaints Sub-committee determines a Signatory has made a very serious breach of the Code, and the Complaints Sub-committee and Signatory cannot agree on how to resolve the matter within a reasonable time frame, the Complaints Sub-committee may withdraw signatory status. The Complaints Sub-committee will only withdraw signatory status where the Signatory has failed to file a transparency report within six months of the due date set by DIGI, or the issue is so serious that it substantially compromises the ability of the Signatory to meet its commitments in relation to Outcome 1 of the Code (sections 5.8, 5.10, 5.11 and 5.13 of the Code).*

These penalties have been designed with the broader aim of the complaints process being used to resolve the complaints from the public, so as to ensure compliance with the code and reduce Australians exposure to misinformation and disinformation.

7. Is it correct that the code excludes content authorised by an Australian political party altogether?

As part of a broader set of protections for freedom of expression in the *Australian Code of Practice on Misinformation and Disinformation*, the Code contains exceptions for the following specific types of speech:

- A. *content produced in good faith for entertainment (including satire and parody) or for educational purposes;*
- B. *content that is authorised by an Australian State or Federal Government;*
- C. *Political Advertising or content authorised by a political party registered under Australian law;*
- D. *news content that is the subject of a published editorial code which sets out content standards and or/complaints mechanisms.*

However, the code has an opt-in commitment for platforms that offer political advertising to enable their users to better identify the source of political advertising to provide transparency. DIGI notes that all of the major social media signatories have opted in to this particular commitment.

Furthermore, if harmful false or misleading political advertising is being propagated by malicious actors using trolls or bots on a platform, then it will be treated as disinformation, or if signatories determine that it is misinformation, political advertising may be removed under the code.

This approach is due to the fact that the Government asked for a code to cover the digital industry. The approach also serves to reduce the risk of the digital industry code's commitments being used by political parties to target the speech of political opponents, noting there is currently no general law about political speech and truth that applies to political advertising. We understand that Independent federal MP Zali Steggall has proposed legislation to prevent the spreading of falsehoods during federal elections to address this gap⁶.

DIGI also notes that political parties are currently exempt from the Privacy Act. The Privacy Act is currently under review, and DIGI shares concerns raised by other stakeholders noted in the review's discussion paper in relation to potential voter manipulation if this political party exemption is retained.

8. Does this code offer members of the public or civil society more broadly any avenues for review for the way platforms deal with specific instances of misinformation or disinformation on their

⁶ RMIT ABC Fact Check (13/10/2021), "Zali Steggall says it's 'perfectly legal' to lie in political advertisements. Is she correct?", available at <https://www.abc.net.au/news/2021-10-13/fact-check-is-it-perfectly-legal-to-lie-in-a-political-ad-/100511796>

platforms?

In October 2021, DIGI strengthened the code in a number of ways including the introduction of a complaints portal on its website where DIGI accepts complaints from the Australian public where they believe a signatory has breached the code's commitments. Eligible complaints are reviewed by an expert independent complaints committee comprised of Dr Anne Kruger, Victoria Rubensohn AM and Christopher Zinn.

The Code does not deal with the removal of materials that violate specific platform policies, nor misinformation matters that do not concern the signatories of the code. Complaints about individual items of content on signatories' products or services should be directed to the signatory via their reporting mechanisms, and the code requires all signatories to have such reporting mechanisms.

This approach is because the purpose of the code is to drive improvements in the measures that signatories take to deal with misinformation and disinformation, and the complaints handling approach is consistent with that aim. It is worth noting that this approach is consistent with the recommendations of the final report from the ACCC Digital platforms inquiry, which recommended an approach to complaints handling that focused on code breaches.

DIGI is yet to see the ACMA's report on the effectiveness of the ACPDM that it provided to the Government on June 30, 2021. Reviewing this report will assist DIGI in its efforts to continue to strengthen the code in line with expectations. DIGI intends to conduct a review of the code in 2022.

In the absence of seeing this report, and in advance of the review, over the course of September to November 2021, DIGI has made a recommendation to the Australian Government (via the ACMA, Minister's Office and the Department of Communications) for how the ACPDM can be strengthened, for which we are awaiting an outcome. DIGI has presented an identified gap in the governance arrangements outlined should disagreements arise between the complainants of the ACPDM and the Complaints Sub-Committee, and has proposed that the ACMA provide this appeals role. We believe an appeals process operated by the ACMA will provide an important safety net for consumers in relation to the ACPDM.

DIGI Engage

9. How many young Australians have participated in DIGI Engage youth summits?

For the last few years, DIGI has brought together young Australians, from all around the country, who are committed to stopping hate speech and extremism through its annual youth summit *DIGI Engage*. The *DIGI Engage* event series is a product of a longstanding, innovative private-public partnership between DIGI and The Australian Government, primarily through The Department of Home Affairs, related to our shared goals around countering violent extremism.

The objective of the event series is to build young people's capacity to counter divisive narratives to make them a powerful force against racism and societal polarisation. Hundreds of young people have participated in these immersive youth summits, and included below are the numbers of registered participants for each DIGI Engage event.

- 2020: 80
- 2019: 78
- 2018: 109

- 2016: 104

The Sydney-based event is free for all participants and also covers all participants' travel, accomodation and participation, noting that the event in 2020 was virtual due to the constraints posed by COVID-19.

10. How are participants selected?

Participants must apply to take part in *DIGI Engage* through an online application form. Applications are reviewed by DIGI, the social change agency Love Frankie who assist in the design and delivery of the event, and the Department of Home Affairs.

Generally, eligibility to participate in *DIGI Engage* involves the following criteria, which are reflected in the application forms:

- Living in Australia. However, for the June 2019 event which occurred three months after the devastating March 2019 Christchurch terrorist attacks, we enabled the participation of a small number of NZ delegates. The 2018 event had a regional focus with participation with delegates from the ASEAN region.
- Being between the ages of 18-30.
- Having demonstrated leadership experience in a community, workplace, school or online setting.
- Having a demonstrated interest in issues such as peace, security, countering racism, community-building, youth empowerment, resilience, social inclusion and cohesion and active citizenship.

The application process is generally promoted through outreach to youth organisations, universities, media outlets, civil society organisations, issue experts, event partner & speaker networks, DIGI's networks and social media advertising.

11. Are cohorts of youth at risk of radicalisation prioritised for participation in these summits? If so, what cohorts?

We aim to ensure that communities who are most vulnerable to extremist narratives are represented through emerging community leaders who represent or understand those communities. This is based on evidence that has found that some people are better than others at delegitimising hatred and violence, when they come from a community considered important by a potential perpetrator, such as their racial community or their friendship group⁷.

We generally seek a mix of two categories of participants who are either i) already influential online and in their communities, and have demonstrated leadership ii) are not yet influential but are applying to attend because they are aspiring community influencers. We also ensure that there is a diversity of participants in DIGI Engage, across gender, cultural groups and regional areas, and with a diversity of interests.

12. Your submission indicates that the summits deal with the “root causes of societal polarisation, hate speech and extremism”. What do you consider these root causes to be?

The objectives of *DIGI Engage* events are to empower key cohorts of young people (as described in

⁷ See Elizabeth Levy Paluck and Michael Chwe, (2016), *Stop Playing Defense on Hate Crimes*, available at <http://time.com/4583843/stop-hate-influencers/>

Question 11) with the knowledge, skills and confidence to counter societal polarisation, hate speech and extremism by:

- Imparting the skills, tools and best practices to engage meaningfully with racism, online hate speech and countering violent extremism (CVE) efforts, that participants can put into practice and share with their networks;
- Creating meaningful connections with individuals and stronger networks between a diverse cross section of people and organisations who are actively working to counter hate and violent extremism; and
- Providing high calibre speakers, mentors and content to inspire creative and collaborative solutions to these issue areas, and to glean valuable input from participants themselves.

Those speakers provide insight into the varying root causes of these issues based on their experiences, research and discipline area. The program often includes examination of the “push factors”, including macro-level socio-economic or political trends and the “pull factors” at a micro group or individual level.

13. Do these youth summits engage with the right-wing extremist ideologies that motivated the Christchurch terrorist? If not, why not?

Yes, this is a key focus of the events. The keynote address in the *DIGI Engage* 2020 event was a presentation called “A Bridge Between Black Commonalities and White Supremacy”, featuring Daryl Davis, the renowned black author and race reconciliator who came to fame by interviewing KKK leaders and members and has successfully persuaded 200 clan members them to renounce their racist ideology. Davis’ presentation was in collaboration with TM Garrett, a former white supremacist leader turned human rights activist, where they together empower participants with the skills to bridge divides and engage in difficult conversations with friends, co-workers and family members.

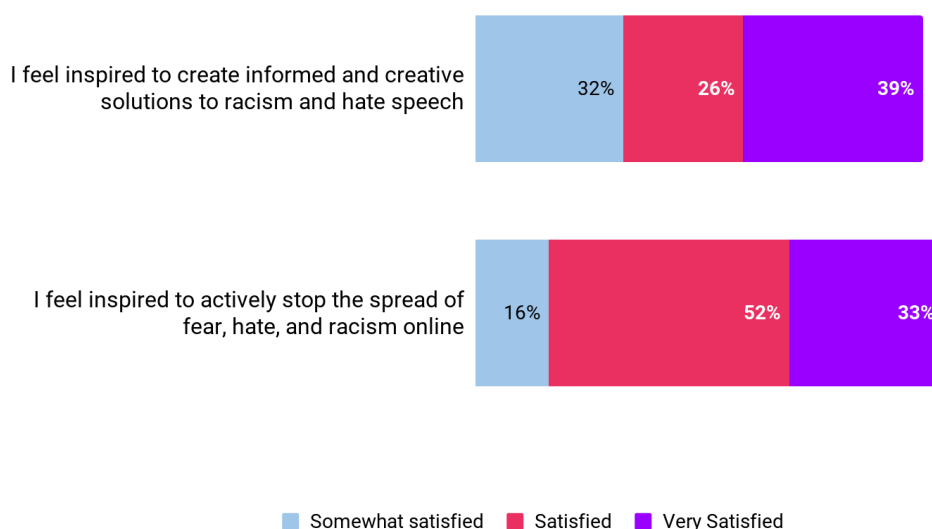
The keynote address in the *DIGI Engage* 2019 event was delivered by Arno Michaelis, the former founding member of what became the largest racist skinhead organisation in the world, who has since dedicated his life to helping people overcome far-right extremism and a co-founder of the peacebuilding organisation Serve 2 Unite.

14. Your submission indicates that these summits build the capability of young Australians to counter the root causes of these extremism online and offline. How does it do this?

See answer to Question 12 for the broad objectives of the *DIGI Engage* events. To illustrate how these objectives are achieved, the last DIGI Engage event held in person in 2019 included the following elements:

- A former extremist talking about their path to radicalisation.
- A panel with representatives from major online platforms, to build understanding how young people can take control of their online safety and improve their digital literacy.
- A research overview into the drivers of societal polarisation, and populations at risk of extremism.
- Workshops on counter-speech to deep-dive learnings of effective, and ineffective, interventions to divisive narratives, with participant interaction to put learnings in practice.
- An exploration of the concept of empathy, in bringing people together across divides.
- Practical ideas and diverse solutions for how participants might effect change in their communities.
- Rapid talks from a range of campaigners who have worked to influence others across political lines on a range of topics.
- A creative exploration of how music and the arts can bring people together across divides.

An evaluation of the most recent event found it was successful in its objectives, per the data below.



15. What academic research has informed the approach taken in these summits?

DIGI Engage is an evidence-based approach to countering violent extremism, based on a growing consensus among experts in this discipline on both the importance of social cohesion programs as a critical component of prevention, and the importance of engaging young people as part of the solution⁸.

DIGI partners with a specialist social change agency Love Frankie that specialises in evidence-based program design. DIGI and Love Frankie prioritise the participation of speakers and organisations whose work is grounded in academic research.

⁸ For example, see: Australian Strategic Policy Institute (ASPI), How communities and governments can come together to counter violent extremism, available at <https://www.aspi.org.au/opinion/how-communities-and-governments-can-come-together-counter-violent-extremism>; "However, one of the criticisms of CVE, both here and in the UK, is that they are more intelligence-gathering exercises. On top of that, CVE programs are, it's suggested, driven by a security-focused agenda, rather than a prevention-oriented one that supports youth in general, as well as vulnerable individuals."

See also: UNESCO, Preventing Violent Extremism, available at <https://en.unesco.org/preventingviolentextremism>; "It is not enough to counter violent extremism --- we need to prevent it, and this calls for forms of 'soft power', to prevent a threat driven by distorted interpretations of culture, hatred, and ignorance. No one is born a violent extremist – they are made and fueled. Disarming the process of radicalization must begin with human rights and the rule of law, with dialogue across all boundary lines, by empowering all young women and men, and by starting as early as possible, on the benches of schools."