DIGI response to questions on notice Inquiry into the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024, hearing 21 October 2024

Senator Hanson Young

Do your members have a position on duty of care in other jurisdictions?

Our members are subject to the Online Safety Act UK (2023) which contains a range of duties of care on search engine services and services that allow users to post online or interact with each other. These duties in broad terms require providers to identify and manage the risks of harms from illegal content and content harmful to children. This law only passed on 26 October, 2023, and the regulator, Ofcom, is currently consulting on codes that outline how services can meet the statutory duties. DIGI's members do not have a detailed position on the UK approach given the Act has had a short period of operation and the details of how services can meet the duties of care are still under development. We do, however, note that a strength of the UK approach is that it is focused on a clearly defined set of services and adopts a proportionate approach to the management of the risks of harms on digital services, which we consider should be key pillars of online safety regulation more generally. As noted in our opening statement, this is not the approach of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 which covers a very broad range of services, regardless of their risk profile.

I'd like you to take on notice the criticism by CyberCX, in relation to the fact that a number of your members take too long—including X—to take down disinformation.

In its submission to the Committee, CyberCX, expressed the view that there is 'an apparent lack of intent, ability or interest from social media companies to proactively identify and take action against inauthentic activity on their platforms". We disagree with this opinion. Our members make significant investments in combatting disinformation campaigns including those propagated via inauthentic behaviors as is documented in their transparency reports under the *Australian Code of Practice on Disinformation and Misinformation*. CyberCX based its conclusion on two examples, of inauthentic behaviors observed on X (f.k.a Twitter) and Meta. However, in both of the example cases CyberCX provided, the platforms in question removed the activity and suspended accounts engaging in inauthentic behaviour.

X advises that it reviewed the accounts described by Cyber X as the Green Cicada Network, took them down and remediated the wider network. This is consistent with X's long-standing commitment to fighting platform manipulation. X's platform manipulation and spam defenses are primarily proactive or automated and operate significantly faster than enforcement based on user reports. Meta advises that it has been taking enforcement action against Spamouflage since 2019.

The CyberCX submission does not suggest that there were steps that could have been taken to disrupt these operations more quickly. As CyberCX noted in its submission, combatting inauthentic behavior is challenging as "there are a lack of frameworks for measuring the effectiveness of information operations, the absence of which makes it difficult to assess the direct impact of malicious activities and identify suitably effective response options". DIGI members are committed to continuing to develop their response to disinformation to respond to changes in the threat landscape including the increasing use of AI to propagate inauthentic behavior.

You're representing the code; you're saying the code is working; you're saying your members aren't profiting from mis- and disinformation. I think that is not true. I think that is absolute rubbish, and if you think I'm wrong I'd like some evidence that shows that. It's up to you how you get it, but I'd like you to take that on notice.

Signatories to the *Australian Code of Practice on Disinformation and Misinformation* commit to implementing safeguards and combat the risk of disinformation and misinformation. We consider it is in the commercial interests of platforms to fulfill these commitments and take action to mitigate serious risk and harm as these do not align with a long-term, sustainable user experience on platform services.

Under Objective 2 of the code, there is a commitment to disrupt advertising and monetisation to mitigate the risk of harm from disinformation and misinformation. Measures to disrupt monetisation could include:

A. Promotion and/or inclusion of the use of brand safety and verification tools;
B. enabling engagement with third party verification companies;
C. assisting and/or allowing advertisers to assess media buying strategies and online reputational risks;
D. providing advertisers with necessary access to client-specific accounts to help enable them to monitor the placement of advertisements and make choices regarding where advertisements are placed; and /or
E. restricting the availability of advertising services and paid placements on accounts and websites that propagate Disinformation or Misinformation.

Further detail on how signatories implement their commitments can be found in the annual transparency reports on the DIGI website at www.https://digi.org.au/disinformation-code/. You can also find copies of the most recent transparency reports attached.

Disinformation and harmful misinformation are multi-faceted social problems that cannot be fixed with technical and legal safeguards alone; this is why we are a proponent of multi-stakeholder approaches that continue to ensure strong accountability and responsibility on the part of online platforms, while also situating platform-level responses in a wider context.