TCF submission to Education and Workforce Committee

Parliamentary inquiry into the harm young New Zealanders encounter online

30 July 2025

Introduction

1. Thank you for the opportunity to make a submission to the inquiry into the harm young New Zealanders encounter online, and the roles that government, business and society should play in addressing those harms. This submission is provided on behalf of the New Zealand Telecommunications Forum (TCF).

2. The TCF is the telecommunications sector's industry body which plays a vital role in bringing together the telecommunications industry and key stakeholders to resolve regulatory, technical and policy issues for the benefit of the sector and consumers. TCF member companies represent 95 percent of New Zealand telecommunications customers. Our members include network operators, retail service providers and the tower companies that own and operate cell towers.

3. Our submission covers:

    a. The role that telecommunications networks play in enabling internet access (the pipes rather than the platform)

    b. The online safety tools telcos offer and other tools parents can use

    c. The benefits connectivity provides for young people and their families

    d. The need for risk-based regulation (if regulatory approaches are being considered).

The role of telecommunications in internet access

4. Telecommunications networks are the pipes and wireless signals that transport data and enable access to the internet. Services are provided to customers by internet service providers (ISPs) and mobile providers. The platforms and websites that allow users to create, host or access content online operate on top of telecommunications infrastructure; these are

called over the top (OTT) services. Telecommunications networks forward packets of data but, under the end-to end principle, do not see what is in the packets. Encryption makes it impossible for ISPs to see the content of most internet traffic, including social media and OTT messaging platforms.

The services offered

5. TCF members offer home (broadband) internet and landline services, and mobile services such as internet, voice calling and instant messaging (SMS and MMS). Some of our members offer email services and bundle other products and services with their connections such as PayTV or music streaming services.

6. While telecommunications network providers do not control online content, our members provide services (and are involved in initiatives) to help keep young people safe online. These include:

    a. Offering advice for parents about devices and online safety. For example:

        i. The 2degrees First Phones programme (in partnership with Netsafe)

        ii. Spark's advice for Connected Families on how to keep in touch without a smart phone, devices that are suitable for kids, and protecting your child's privacy. Spark has recently launched a mobile plan designed for kids.

    b. Supporting Netsafe and other NGO initiatives, including Netsafety Week and other digital wellbeing initiatives (these change over time).

    c. Home filtering tools with lists of pre-categorised web addresses that can be applied on a home router or network to filter out unwanted content. For example, Spark offers Net Shield and One NZ has Smart Wifi.

    d. Applying the Digital Child Exploitation Filtering System to prevent access to objectionable child sexual abuse material, blocking harmful websites on the International Watch Foundation list, and supporting the DIA's 11 voluntary principles to counter online sexual exploitation and abuse.

    e. Partnering with government, law enforcement and banks to help reduce the risks of users (including young people) being scammed. The TCF is a member of the recently launched Anti-Scam Alliance.

Parental controls

7. Parents can control access to content by using parental control and other settings in the devices and applications a child is using. The advantage of device level controls (applied to smart phones, tablets and gaming consoles etc) is that they work directly through the device and with any network the device is connected to - the home network, the mobile network, a public wifi network, or hotspotting off a friend's connection. Some examples include:

a. Parental controls built into Apple and Android devices, or applied via apps. These allow parents to manage content restrictions, as well as screen time, in-app purchases, and the ability to install applications.

b. Switch on Safety, a filter parents can apply by changing the DNS settings on their child's device.

c. Google apps such as Search, Chrome and YouTube have filtering and other safety settings such as YouTube kids and teen profiles. Bing and Duckduckgo are other popular search engines for children that have safe search options in settings.

8. In contrast, network blocking by ISPs is a blunt tool which blocks entire websites and applies to all users of a connection. Network blocking requires a trusted party to validate and inform ISPs on what should be blocked and ISPs need legislative safeguards to protect them from legal action by the owners of the blocked sites. Technically, network blocking is easy to bypass by motivated end users so is best for scenarios where the consumers want to be protected from inadvertently accessing the content - such as scam websites - rather than blocking mainstream websites or services.

Benefits of connectivity for young people

9. While the inquiry is looking at online harm, the Committee also needs to consider the many benefits that connectivity brings to young people and their families. These include:

    a. Everyday safety and communication:

        i. Calling or texting parents or caregivers in emergencies or for check ins

        ii. Location sharing apps that let parents see where their children are

        iii. Using mobile phones to contact emergency services

        iv. Parents being able to contact their children to update them on changes to after school plans

        v. Connecting vulnerable young people with a support community and support services

        vi. Connecting with friends.

    b. Education and learning:

        i. Accessing school portals for homework, timetables and grades

        ii. Collaborating on school projects using tools such as Google Docs or Microsoft Teams

        iii. Watching educational videos on platforms like YouTube.

c. Transport and navigation:

   i. Checking real-time bus or train timetables via apps or websites

   ii. Using maps and navigation tools to find safe walking routes or public transport options

   iii. Checking balances and topping up travel cards online.

Risk-based regulation

10. The online harms under examination include online bullying, exploitation, additive use, mental health impacts, educational impacts, and exposure to harmful content.

11. Telecommunications services such as voice calling, SMS and MMS text messaging are generally low-risk as they do not host or promote user-generated content. They also provide an essential communication channel between parents and children.

12. Any regulatory efforts should be focused on higher-risk platforms such as social media platforms, content-sharing apps and other applications with significant social functionality, where harmful interactions are more likely.

13. If regulation is being considered by the Committee it is important to think about the services that would be in or out of scope, to avoid unintended consequences and ensure that essential services remain accessible. We suggest the following not be included in any regulatory proposal that may limit online access or communications by young people:

    a. Messaging services (SMS, MMS and email)

    b. Landlines and mobile voice services

    c. Business communication tools used in education or enterprise settings

    d. Health and education services that support young people.

Concluding remarks

14. The TCF and its members are committed to supporting safe and positive digital experiences for young people in New Zealand. While our members are the pipes not the platforms, if the Committee is considering SMS, MMS, mobile access or network blocking we would like to be part of the conversation. Network blocking is a blunt instrument, which can be bypassed by motivated users. There are practical limitations and process issues to be aware of.

15. We are available to speak to the Committee and answer any questions you may have. Please contact kim.connolly-stone@tcf.org.nz in the first instance.

[ends]