

Submission in response to the Australian Government's public consultation on Enhancing Online safety for children

Executive Summary

1. This submission is made by NetSafe in response to the Australian Department of Communications public consultation on online safety for children¹.
2. As New Zealand's sole active cybersafety organisation NetSafe is strongly positioned to understand and comment on online challenges and remedial measures.
3. NetSafe agrees that a growing number of Australian children will be accessing the internet and social media through mobile devices and that this trend increases the frequency with which children are exposed to online challenges.
4. NetSafe also agrees that cyber bullying behaviours amongst children are the primary online challenge to address, but notes that it is one of many types of digital challenge that accompany children's increased use of evolving technology.
5. The unique nature and specific characteristics of online bullying behaviours requires a dedicated response. However, NetSafe notes that this should be as part of a 'joined up' approach to child safety that explicitly considers the relationship between (1) online and offline bullying behaviours and between (2) online bullying and other online behavioural concerns.
6. NetSafe notes that often young people's management of, and response to, cybersafety risks can challenge conventional wisdom. However, a significant number of young people report negative experiences from their exposure to inappropriate content and communications and need support.

¹ Online Safety for Children Public consultation on key election commitments. Department of Communications, Australia, January 2014.

7. NetSafe agrees that high levels of harm can be caused by cyber-bullying. However, NetSafe notes that to be effective, the response to online bullying needs to cater for the full spectrum of digital communications that have the potential to cause a level of harm.
8. NetSafe supports the need for a dedicated focus on building safer internet experiences for children. It also notes that interventions that can make the online environment safer for children could also benefit adults, and where appropriate, policy provisions should be aligned.
9. NetSafe notes that, first and foremost, the response to e-Safety challenges should focus on creating a safer online experience for children i.e. prevention. Further, that an appropriate balance needs to be struck between those strategies designed to protect, and those designed to empower children and their families to better manage the challenges they experience.
10. For example, Netsafe agrees that there is often a disconnect between children and the significant adults in their online lives. It is therefore appropriate for an e-Safety response to include initiatives that equip adults and peers to better support young people manage challenge.
11. Regardless of how successful efforts to reduce levels of cyber-bullying are, incidents will still occur. In NetSafe's experience, remedies for reducing the impact of cyber-bullying on victims can be effective and are relatively straightforward to implement.
12. The parallels between the model proposed in the discussion paper² for managing complaints about online bullying and the provisions of the New Zealand Harmful Digital Communications Bill are clear. NetSafe notes that there appear to be important differences between the two approaches that could limit the effectiveness of the proposed model.
13. NetSafe notes that the discussion paper's definition of what constitutes harmful content and communications could be more clearly defined. NetSafe believes that this is important as these definitions provide the basis for designing an effective overall e-Safety programme and for meaningful stakeholder engagement.
14. NetSafe's operational experience indicates that it is important to recognise that cyber-bullying is a problem that government, consumers and industry have a shared interest in solving. NetSafe believes that greater emphasis could be given to the role of multiple sectors in the proposed e-Safety response.

² Ibid.

15. NetSafe acknowledges the range of high quality e-Safety programmes and initiatives currently being delivered by government agencies, NGOs and industry. It also notes that these should be complemented and extended by any new proposals.
16. NetSafe's general position is that it recognises the central role an appointed Commissioner could play as a coordinating body for Australia's existing, and future, online safety interventions.
17. NetSafe's view is that the responsibilities proposed for the e-Safety Commissioner are broader in scope than what is appropriate for one organisation to carry out. Further, NetSafe believes that the four proposed models for establishing an e-Safety Commissioner (p 7-8) are not separate and exclusive options i.e. 'form follows function' with different types of organisations having different roles to play in the overall e-Safety response.
18. NetSafe believes that focussing on the leadership role envisaged for the Children's e-Safety Commissioner (p 4) is appropriate. For discussion purposes only, NetSafe has put forward a model for the Commissioner's role that is centred around leadership, advocacy and coordination.

NetSafe looks forward to the opportunity to support this submission and directly respond to any questions that it raises.

Martin Cocker
Executive Director
NetSafe

Introduction

NetSafe, an independent non-profit organisation

NetSafe is New Zealand's only active cybersafety organisation. It began work in 1998 and was incorporated as a society governed by an elected board of six trustees in 2001. With over 100 members from across the public, NGO and commercial sectors NetSafe is both representative of, and accountable to, the community that it serves.

NetSafe provides education and support to all New Zealanders

NetSafe's sole purpose is to support the development of a safer and more secure online environment to encourage all New Zealanders to take advantage of digital opportunities. NetSafe directly supports consumers, families, schools and businesses as they navigate through a range of online 'digital challenges' and helps them reduce their exposure to risk or to minimise harm when things do go wrong.

NetSafe directly provides educational content and a mixture of workshop and consultation services to the community. In addition, its contact centre manages an average of 500 requests for support each month. A significant proportion of which are complaints related to harmful, aggressive and bullying online communications (or 'harmful digital communications'). In addition, NetSafe actively advocates on behalf of New Zealander's safety and security needs to see that these are reflected in government's legislative and policy programmes.

The New Zealand Government's Harmful Digital Communications Bill

The Department of Communications discussion paper³ references New Zealand Government's Harmful Digital Communications Bill⁴ ('the Bill'). The Bill is directly relevant to this consultation process as it identifies the potential emotional harm that can be caused by harmful digital communications and proposes to mitigate this by offering to victims a quick and efficient means of redress. It proposes a new civil enforcement regime to quickly and effectively deal with harmful digital communications, creating new criminal offences and making amendments to existing criminal legislation.

A key component of the civil regime is the appointment of a civil enforcement agency (an 'Approved Agency') to resolve complaints through mediation, persuasion and negotiation. The New Zealand Law Commission recommended that NetSafe was given statutory recognition as an 'Approved Agency' in

³ Ibid.

⁴ Introduced to the New Zealand House of Representatives on 5 November 2013.
<http://www.legislation.govt.nz/bill/government/2013/0168/latest/096be8ed80c76cca.pdf>

its briefing⁵ to the Minister of Justice, Hon. Judith Collins. This recommendation reflects the alignment of NetSafe's current role and relationships with the functions envisaged for an 'Approved Agency' i.e. NetSafe already works with partner organisations to provide direct support to people targeted by harmful digital communications.

On 21 February 2014 NetSafe made a submission as part of the New Zealand Government's public consultation on the Harmful Digital Communications Bill. The full text is available online⁶.

NetSafe collaborates with Australian organisations to address shared problems

NetSafe works with a range of national and international industry, NGO and public organisations to extend and strengthen the suite of internet safety content and services available to New Zealand's internet users. Through this work Netsafe has developed many valued relationships with Australian organisations working on children's e-safety issues. The mutual benefit derived from these Trans-Tasman relationships has been clear.

About this submission

In te ao Māori the concept of 'ako' means to both to teach and to learn. It is with this spirit of reciprocity that NetSafe makes this contribution to the consultation process.

NetSafe's sole purpose is to promote confident, safe, and responsible use of digital technologies. A key aspect of this is the provision of education and support services that enable children to grow into confident and capable contributors to the digital society and economy. Underpinning this submission is NetSafe's acknowledgement of the Australian Government Agency's clear commitment to developing online safety for children.

At the time of writing the New Zealand government reserves its decision on the appointment of the Approved Agency⁷. In the interim, NetSafe is able to bring to this submission process the perspective of an organisation already immersed in the issues that the Australian Government seeks to address in its discussion paper.

⁵ Ministerial Briefing Paper, Harmful Digital Communications: The adequacy of the current sanctions and remedies. Law Commission - Te Aka Matua o te Ture, August 2012.
http://lawcom.govt.nz/sites/default/files/publications/2012/08/ministerial_briefing_-_harmful_digital_communications.pdf

⁶ <http://netsafe.org.nz/downloads/NetSafe-Select-Committee-Submission-on-HDC-Bill-21-Feb2014.pdf>

⁷ Harmful Digital Communications, Cabinet Social Policy Committee. Office of the Minister of Justice, October 2013.

In developing this submission NetSafe has drawn on its own operational experience, the development process of the Harmful Digital Communications Bill, research and other evidence sources. It does not directly address the specific questions posed in the discussion paper. Instead, this submission provides a high level response to the key themes and ideas that NetSafe believes are most salient to the issues the Australian Government wishes to address.

The content of the submission is structured around three broad areas of discussion:-

1) Children and online challenge

Children are accessing the internet with increasing frequency via multiple access points and with a continuing trend towards mobile access. Young people are being increasingly confronted by an evolving range of online or 'digital challenges'. The response to these challenges should, first and foremost, focus on creating a safer online experience for children.

2) Harmful Digital Communications are a real and complex challenge

Regardless of how successful efforts to reduce levels of cyber-bullying are, incidents will still occur. It is possible to take action to reduce emotional harm caused by digital communications. However, current remedies are not sufficient and there is a role for a legislative response that is pragmatic, reflects the nature of the internet environment and complements and extends non-legislative mechanisms.

3) Leading, advocating and coordinating are the roles of an e-Safety Commissioner

Cyber-bullying is a problem that government, consumers and industry have a shared interest in solving. It is important to begin by clearly defining all the functions required to deliver an effective, coherent e-Safety response. This provides the basis for determining what organisations are already fulfilling those functions and where the gaps are, including what the role of the Commissioner should be.

Notes on the terminology used in this submission

While cyber-bullying is increasingly used to describe abusive or harmful electronic communications, the term itself has a fairly specific definition. As the New Zealand Law Commission noted in its briefing on the subject, “in the offline world, ‘bullying’ usually implies a repeated behaviour carried out in the context of adolescent peer relationships. An implied power imbalance exists between aggressor and victim”⁸. This aligns with the definition provided in the discussion paper (p 3).

Some harmful communications may not meet all the criteria of bullying. For example, a single online act can be rapidly duplicated by other users, creating the ‘repetition’ seen in bullying behaviours, but without a one-to-one relationship between bully and victim.

In general this submission uses the terms ‘cyber-bullying’ or ‘online bullying’ to describe the range of intentionally harmful communications that occur within the context of relationships between young people. However, as the concept of ‘harm’ is the centrally import idea in the discussion, this submission also uses the broader term ‘harmful digital communications’. This term is also used in the context of the New Zealand Government’s Harmful Digital Communications Bill.

⁸ New Zealand Law Commission, 2012

Detailed comments

1) Digital, social, mobile and always on | Children and online challenge

Children access the internet with increasing frequency via multiple access points and with a continuing trend towards mobile access.

1. NetSafe agrees with the assertion in the discussion paper that a growing number of Australian children will be accessing the internet and social media through mobile devices.
2. This trend increases the frequency with which children are exposed to online challenges such as cyber-bullying and along with this the potential number of incidents occurring.

Going online, children are presented with a range of digital challenges for them to navigate.

3. NetSafe agrees that online bullying behaviours are the primary issue to address. As noted in the discussion paper some reports indicate over 50% of teens have experienced cyber-bullying. In NetSafe's own research on the range of online challenges instances of cyber-bullying or harassing behaviour were the most distressing type of challenge young people reported experiencing.
4. Critically, the rapid developments in digital technology create new, or evolve existing, risks to young people. These are primarily related to conduct concerns; including harmful communications, inappropriate 'digital footprints', and criminal enterprise in an increasingly digitally reliant world i.e. cyber-bullying is one of many types of digital challenge that accompany children's increased use of evolving technology.

It is no longer possible to think about these challenges as being exclusively online or offline.

5. NetSafe's operational experience, that online and offline bullying or harassing behaviours are closely linked, is supported by research findings. For example:-
 - Often children targeted by online harassment know the perpetrator in person from before the incident; and
 - Many of them also report an aggressive offline contact by the perpetrator.
 - Those who are bullied offline are many times more likely to experience online bullying; and conversely
 - Children who are online victims may be online perpetrators as well.

6. NetSafe agrees that the unique nature and specific characteristics of online bullying behaviours requires a dedicated response. However, this must be as part of a 'joined up' approach to child safety that considers the relationship between:-
- Online and offline bullying behaviours
 - Online bullying and other online risk taking or behavioural concerns.

In many cases children can merge their prior knowledge with technical skill to develop cyber-risk management strategies.

7. Current understandings of young people's management of, and response to, cybersafety risks challenges many assumptions. It indicates that, for example, young people:-
- Are able to merge prior knowledge with technical skill to develop cyber-risk management strategies
 - Often choose to undertake risky practices because they believe the benefits outweigh the risks
 - Are differentially vulnerable to negative outcomes (both within and across developmental stages)
 - Children frequently choose to manage the challenges they experience through self action or socially with their peers and not through a 'significant adult'.

Regardless, a significant number of young people report negative experiences from their exposure to inappropriate content and communications.

8. In research carried out by NetSafe, 'ignoring' was the most common self-management strategy. Unsurprisingly, this approach was seldom associated with the positive resolution of an incident. In the same study, the most effective strategy reported by children was 'social support', involving both peer and (more significantly) adult assistance.
9. However, as noted in the discussion paper⁹ and above, there is often a disconnect between children and the significant adults in their online lives. An implication of this is that the response to the online safety risks should maintain a focus on equipping adults and peers to better support young people to manage challenges. A legislative response to harmful content and communication is necessary, but not sufficient, to address the issues i.e. a package of legislative and non-legislative measures is required.

⁹ Page 3 - Online Safety for Children, Department of Communications, 2014

10. An example of one programme working toward that goal in Australia is the Alannah and Madeline Foundation's recently launched 'e-Smart Homes' programme. The programme focuses on empowering parents and carers to educate themselves and teach their children about safe and responsible use of technology.

The harm caused by cyber-bullying can range in severity.

11. The discussion paper illustrates the high levels of harm that can be caused by cyber-bullying by noting cases where it is indicated as a factor in youth suicide. This is supported by the experience of New Zealand's Chief Coroner, Judge Neil MacLean. In 2012 he expressed concern about the emergence of bullying, and cyber-bullying in particular, as a "background factor" in New Zealand's high youth suicide rate¹⁰.
12. However, to be effective the response to online bullying needs to cater for the full spectrum of digital communications that have the potential to cause some level of harm i.e. responses need to be proportionate. Most of the complaints NetSafe receives require relatively light intervention, for example, in the form of advice and guidance. At the other end of the scale the most complex and/or egregious complaints require significantly more expertise and resource to address.

Harm caused by digital communications has the potential to affect anyone that goes online.

13. NetSafe supports the intent of the discussion paper to focus on building safer internet experiences for children. In NetSafe's experience young people are disproportionately targeted by cyber-bullying with approximately 50% of the complaints it receives being from, or on behalf of, this demographic.
14. "The victims of harmful digital communications are often children and young people, who are particularly vulnerable and require appropriate protections"¹¹. At the same time an increasing numbers of adults are complaining about harmful digital communications i.e. the other 50% of reports. NetSafe believes that many of the interventions that can make the online environment safer for children would also benefit adults i.e. where appropriate, there are advantages to aligning the policies aimed at supporting young people and adults.

¹⁰ Section 2.73 - Law Commission, 2012.

¹¹ Page 2 - Harmful Digital Communications Bill, New Zealand Government, 2013.

The response to these challenges should, first, focus on creating a safer online experience for children.

15. There are a broad range of interventions that could be implemented to help create a safer online environment for children. The success of the overall approach is dependent on striking an appropriate balance between those strategies designed to protect¹², and those designed to empower young people and their families to manage challenges¹³. This approach is implicit in the discussion paper and, NetSafe believes, needs to be explicitly stated in future versions.

2) Harmful Digital Communications | A real and complex challenge

Regardless of how successful efforts to reduce levels of cyber-bullying are, incidents will still occur.

16. It is NetSafe's experience that people can become victims as a result of risk-taking behaviour, an error of judgment, or being targeted regardless of the safety and security precautions they have taken.

Remedies exist that can help to minimise emotional harm caused by cyber-bullying

17. In NetSafe's experience, remedies for reducing the impact of cyber-bullying on victims can be effective and are relatively straightforward to implement. The discussion paper focuses on facilitating the 'takedown' of online content. This uncontested removal¹⁴ of online content can have an immediate and significant positive impact on the victim, simply because a major stressor has been removed.

18. However, this approach has limits to its effectiveness including:-
 - a. It cannot be facilitated if the communication was sent via a channel such as email
 - b. Removing content from one online service does not prevent it being posted immediately to another, perhaps, less responsible service from which its removal is not as easily facilitated
 - c. The accused party does not participate in the resolution process.

¹² Policies, practices and services external to the users that contribute to a safer online environment. These minimise the impact of intentional and unintentional actions, for example, by blocking inappropriate content or preventing inadvertent compromise of a network.

¹³ Promotional approaches that support development of competencies required to self-manage online challenges.

¹⁴ NetSafe prefers this term to 'takedown' as it includes approaches that achieve the same result without an enforcement order, such as persuasion and negotiation.

Clear legal definitions can provide a foundation for action.

19. The discussion paper provides general descriptions of what types and forms of online content and communications could be considered harmful. For example, in the context of creating a civil penalty regime:-
 - a. “material that is harmful to a child” (p 5)
 - b. “harmful, aggressive and bullying material” (p 9)
 - c. “the material would be likely to cause harm or distress to the child” (p 15)
 - d. “material which is potentially harmful or distressing to a child” (p 19)

20. NetSafe believes that the discussion paper’s definition of what constitutes harmful content and communications could be more clearly defined. First, in terms of their broad scope and then specifically in relation to any legislative solution to cyber-bullying issues. In particular, differences between harmful content communicated to a child and harmful content accessible to a child could be more clearly defined.

21. To illustrate this point using the New Zealand context; the Films, Videos, and Publications Classification Act 1993 provides the legal framework for classification of harmful material accessible to a child. Whereas the Harmful Digital Communications Bill 2013 was developed to address a clearly defined need being to “mitigate harm caused to individuals by digital communications and to provide victims of harmful digital communications with a quick and efficient means of redress”¹⁵ i.e. harmful content that is communicated to a person.

22. In the New Zealand context legally defining harm and what constitutes harmful communications is fundamental to the overall functioning of the proposed resolution process in the Bill. It also has a broader role as a:-
 - a. Clear public statement of what behavior is acceptable in the eyes of society.
 - b. Foundation for a range of prevention activities. For example, by informing development of schools’ bullying prevention policies and processes.

23. In summary, the clear definition of terms is a pre-condition for designing an effective overall e-Safety programme and for meaningful stakeholder engagement.

¹⁵ Clause 3 - Harmful Digital Communication Bill, New Zealand, 2013

Solutions tailored to individual cases facilitate more meaningful resolutions for all involved.

24. The discussion paper proposes a model in which an appointed e-Safety Commissioner receives and assesses complaints of cyber-bullying, facilitate rapid removal of content, take enforcement action against online content hosts, and initiate court proceedings.
25. The design of this model clearly parallels that described in the New Zealand Bill. However, a fundamental difference between the two models is the apparent dependence of the proposed Australian model on 'Notice and Takedown' of harmful content and communications. Issues with this approach already highlighted in this submission include:-
 - a. Potential conflation of the approach for managing the communication of harmful content to a child and for the hosting of harmful content accessible to a child (refer to points 19-23)
 - b. Limitations of uncontested removal of content as a remedy (refer to point 18).
26. In terms of the limitations of the uncontested removal of content as a remedy; non-legislative approaches, such as the uncontested removal of content, have an essential role in harm reduction, but are not enough on their own.
27. In the New Zealand context, a package of measures is proposed to implement new, and strengthen existing, remedies. These include:-
 - a. Strengthening support mechanisms
 - b. Engaging with the online content hosts
 - c. Involving both parties to a complaint in its resolution.

This approach is designed to increase the scope of available remedies and their potential effectiveness. It aims to create a regulatory regime that can deliver a proportionate response to better meet the needs of both parties to a complaint.

28. NetSafe believes that this reflects how legislation can complement and extend non-legislative mechanisms by involving the participation of multiple stakeholders.

New legislative remedies need to be pragmatic and reflect the nature of the internet environment.

29. The effectiveness of a legislative approach is largely predicated on the participation of diverse cohorts of stakeholders, many of which may not be compelled through an enforcement regime. For example, the discussion paper discusses penalties and enforcement measures for online content hosts located both in and outside of Australia, and recognises the challenges of encouraging regulatory compliance to sites that are outside of Australia's jurisdiction.

30. This also provides an illustration of how legislative approaches need to reflect the specific characteristics of the online environment, and avoid falling into the trap of trying to ‘control the internet’.

The key to success is recognising that cyber-bullying is a problem that government, consumers and industry have a shared interest in solving.

31. NetSafe’s operational experience demonstrates that productive working relationships with online content hosts can be established and maintained even with those providers portrayed as ‘bad actors’. Such relationships are critical when many channels through which cyber-bullying can occur are primarily governed by online content hosts’ Terms and Conditions.
32. In NetSafe’s experience, online content providers share an interest in solving problems related to cyber-bullying. Relationships built on mutual trust and understanding are invaluable as practical tools for encouraging cooperation across borders.
33. Further, online content providers in overseas jurisdictions are generally respectful of the rule of law and attribute weight to the authority of foreign jurisdictions i.e. ‘persuasive power’. However, online content providers will assess the legitimacy of an organisation approaching them on the basis of a range of factors such as its expertise, independence, its record and the neutrality of its actions.

3) Leading, advocating and coordinating | Roles of an e-Safety Commissioner

34. The discussion paper describes the position of an e-Safety Commissioner that could take on the role of leading government policy, building and maintaining a complaints system for cyber-bullying, and exploring the creation of a legislative cyber-bullying offence.
35. NetSafe’s general position is that it recognises that an appointed Commissioner could play a central role as a coordinating body for Australia’s existing and future online safety interventions.
36. The discussion paper provides an overview of e-Safety initiatives current delivered by different Australian organisations. NetSafe recognises the high quality of these programmes by including them in its work with New Zealand internet users, for example the:-
- Arrangements for removal of online content, including the *Cooperative Arrangement for Complaints Handling on Social Networking Sites*, and the Online Content Scheme from the *Broadcasting Services Act 1992* (p 10-11)

- Australian Government’s online safety programmes and resources, including the Australian Communications and Media Authority’s *Cybersmart* programme, and the Department of Communication’s Australian Children’s *Cybersafety and E-Security Project* (p 26-27)
 - Australian Federal Police’s *ThinkUKnow* programme (p 27)
37. NetSafe also collaborates with Australian non-governmental organisations (such as the Allannah and Madeline Foundation) and ICT industry members. Through this work, NetSafe has become familiar with a number of Australian initiatives and the broad landscape of online safety in Australia.
38. In summary, NetSafe’s experience of collaborating with Australian online safety organisations, indicates that there are a wealth of existing quality online safety resources and strong organisations from across sectors working in this field.
39. NetSafe’s generally agrees that proposed functions for the Commissioner (p 5) are important aspects of a coherent e-Safety response. However, NetSafe’s view is that when taken together these responsibilities are broader in scope than what is appropriate for one organisation to carry out.
40. Further, NetSafe believes that the four proposed models for establishing an e-Safety Commissioner (p 7-8) are not separate and exclusive options i.e. different types of organisations have different roles to play in the overall response.
41. For example, a non-government organisation with expertise in online child safety may be well-suited to facilitating the “rapid removal of material that is harmful to a child from large social media sites” but not “establishing a funding programme for schools to deliver online safety education”.
42. In the New Zealand context, NetSafe:-
- a. Delivers education and support services direct to New Zealander internet users
 - b. Provides a point of coordination for cybersafety initiatives
 - c. Is a conduit for communication between New Zealand residents and other organisations, including industry, NGOs, government, law enforcement and education
 - d. Provides subject matter expertise to government and industry.

43. Further, NetSafe was recommended to be the Approved Agency by the Law Commission because of the requirement for that agency to function as a co-ordination and conduit point i.e. the Approved Agency was designed to work alongside industry, government, and NGO partners, and to maximise the opportunities that each of those relationships provides.
44. Similarly, as there already exists in Australia a number of agencies and organisations with a role in delivering e-Safety-related programmes, the government should seek to coordinate and build on these programmes for the most efficient use of resource i.e. the Australian government could consider bolstering existing frameworks of cyber safety education and institutions such as the Australian Communication and Media Authority, and further strengthen working relationships with organisations from other sectors working in this area.
45. NetSafe believes that the focus on the leadership role envisaged for the Children's e-Safety Commissioner (p 4) is appropriate. For example, NetSafe puts forwards a model for discussion in which the Commissioner has the role of leading, advocating and co-ordinating:-
- a. Leading through the development and maintenance of cross-sector relationships to increase overall effectiveness of cyber challenge prevention and response. Leading the government's cross-agency e-Safety programme of work. Identifying opportunities to to strengthen the overall response.
 - b. Advocating on behalf of the community's safety and security needs to see that these are reflected in legislative or government policy changes.
 - c. Coordinating the government's inter-agency and cross-sector activity to strengthen the e-Safety response.
46. To be effective the e-Safety Commissioner's role must be structured in such a way that it can work equally with Government, NGOs, and Industry partners in recognition of the multi-stakeholder nature of e-safety.