29 November 2023

Hon David Seymour
Minister for Regulation
david.seymour@parliament.govt.nz

Dear Hon Mr David Seymour,

Netsafe briefing to incoming Minister for Regulation - online harm in New Zealand

Congratulations on your election and appointment to be our first Minister for Regulation. You're likely to be scanning briefings from officials to inform your thinking on priorities. As you do, please consider our briefing on online harm in New Zealand, alongside briefings from your department and officials.

We very much look forward to working with you to ensure a safer internet for all users at the same time as exploiting the benefits of new technology.

Thank you also for your leadership in recent months regarding fraud prevention and scams and supporting Epsom constituents to be more scam savvy.

The attached briefing to incoming ministers tells you about Netsafe, the work we do with government and community, and rising levels of online harm in New Zealand. In this letter we highlight a number of issues we have raised with the ministers responsible for the Internal Affairs, Education and Justice portfolios. Some of these issues we have also raised with you at different parts of the year.

Making progress in each of these areas will require cross-portfolio support. As an architect of the new Minister for Regulation role we hope you can support Netsafe to get the Act upgraded or some secondary legislation such as regulations to modernise approaches to tackling online harm.

Netsafe is part of an eco-system that deals with online harm, cyber safety and security Netsafe is part of a broader eco-system that includes online safety, cyber safety and cyber security. Our focus is primarily on online safety - the people and behavioural side of the online world.

Online safety services include incident management, counselling, education, victim remediation and helping people to navigate social media responsibly. We also partner with the community to run campaigns and programmes to support groups of New Zealanders being targeted online.

The digital safety part of the eco-system includes dealing with child sexual abuse material (CSAM), violent extremist content and unsolicited commercial electronic messages (spam). Digital safety is handled by the Digital Safety Team at the Department of Internal Affairs (DIA), Police, and Classification Office. Netsafe has a role referring CSAM and other objectionable content to the agencies withenforcement and other functions in this area. It also has trusted flagger relationships with the online platforms most commonly used in New Zealand, which provide rapid escalation options to get harmful content removed.

Online safety and digital safety are distinct from cyber security. Cyber security is a subset of national security policy. Cyber security means protecting people and their computers, networks, programs, and data from unauthorised access, disruption, exploitation or modification. Government agencies workingin this area currently include Cyber Emergency Response Team (CERT), the National Cyber Security Centre (NCSC), and the National Cyber Policy Office (NCPO). Cyber security has in the past been part of the National Security and Intelligence Portfolio.

There are of course overlaps between the three parts of the eco-system, and online safety and cyber security are linked. Safety starts outside the device and in particular it is important that youth and seniors develop skills around media and online literacy and good digital citizenship. Netsafe therefore works with the Cyber Emergency Response Team (CERT) and Network for Learning to support onlinesecurity in the community and schools.

Online harm and education

Netsafe provides support and resources for schools, kura and parents dealing with young people and online harm. From our work we know that young people are particularly vulnerable to cyberbullying and online abuse. We are seeing a dramatic increase in sextortion, and a number of issues made worse through online platforms, such as youth suicide, body image issues, posting and boasting about criminal activities, and the spread of misinformation and disinformation.

More services are required to educate and support young people and their digital lives. We have asked the Minister of Education to help make this happen, by making changes to the curriculum for schools and kura, and through Vote Education funding for programmes and resources.

On the curriculum side, we need to update and improve the focus on online safety and social media literacy. There is very little in the existing curriculum that prepares young people to adequately engage (and stay safe) in a complex online world. We think the proposed ban on phone use during school term (in the National manifesto) could complement the suggested update to the curriculum, to educate students about social media use, technology, and screen time. This issue also has some urgency because the age of criminality under the Harmful Digital Communications Act applies from the age of 10.

On the programme and resources side, the Government needs to invest in anti-cyberbullying programmes in schools and kura, support the development of new resources for teachers (including Netsafe's micro-learning moments), and fund research to address content that sexualises children or depicts self-harm and suicide violence against children.

The Harmful Digital Communications Act (and the Justice portfolio).

Netsafe is the approved agency under the Harmful Digital Communications Act 2015 (HDCA). The HDCA was passed by the last National Government, to address online bullying, harassment, abuse and and intimidation. We provide a seven-day-a week helpline, community presentations, resources for the victims of harm online, proactive advice on how to stay safe online, and an alternative dispute resolution service to resolve complaints between individuals and with the internet industry (eg platforms).

We have advised the Minister of Justice that the HDCA is urgently in need of an update to address new forms of online harm. The limitations of the existing legislation include its focus on individuals, not groups as targets of online harm. There have also been advances in technology being used to cause online harm. For example, the HDCA does not explicitly prohibit abuse using artificial intelligence (AI), which is becoming increasingly common. AI allows the creation of deep fake or synthetic intimate images depicting real people in situations that are not real. These can then be shared online and used for threats or blackmail.

Netsafe is of the view that updating the HDCA would be a better course compared to the proposals from the previous Government as part of its Safer Online Services, Media and Platforms change agenda. Those proposals did not seek to reform any laws where content is already objectionable and harmful or provide more support for victims. This necessitates strengthening the HDCA and existing structures dealing with illegal content and activities.

We have also briefed the Minister of Justice on:

- concerns about the contribution of social media to youth offending (an issue that has to date fallen between the cracks of agency responsibility)
- the need to educate youth about the implications of social media being an aggravating factor at sentencing
- the dramatic increase in the amount of stalking and harassment online (harassment is currently covered in a piecemeal way across different pieces of legislation)
- gaps in victim recovery programmes for people who experience online harm
- the need for better training for law enforcement personnel, to be able to deal with image based sexual abuse.

At Attachment A is our list of safety issues facing the community provided to the Minister for Justice and suggested improvements to primary and secondary legislation.

Netsafe funding contracts

Netsafe is currently funded by the Ministry of Justice (to carry out functions under the HDCA, until 2026) and the Ministry of Education (to provide support and resources to schools and kura, until 30 June 2024). Our relationships with these agencies are critical to meeting education needs, anensuring wecan effectively play our part in the broader justice system that the HDCA is a part of.

At the end of the last parliamentary term, the previous Government made a rash decision to transfer Netsafe's funding contracts to DIA and for this to take effect in July 2024. We understand this decision was collateral damage resulting from a broader piece of work to align cybersecurity work across government, and a throwaway comment related to cyber safety, without any benefits analysis or consultation with the Ministry of Justice, Ministry of Education or Netsafe.

We ask that the new Government reverse the decision, so that Netsafe continues to contract with theMinistries of Justice and Education. DIA should not control both the agenda and core funding for online safety. While DIA has grouped its censorship, spam and objectionable content functions under the heading digital safety, it does not have experience with the portfolio specific online safety work we do.

More importantly, there is a distance and independence between Netsafe and Government involvement in the censorship and objectionable and regulatory environment that needs to be maintained.

We are seeking your support to have the decision of the previous Government reversed.

A meeting to discuss

Netsafe would very much appreciate a meeting with you to introduce ourselves and discuss online harm in Aotearoa New Zealand. Barb Wright, our Executive Assistant can be contacted at barbw@netsafe.org.nz and by phone +64 21 925 910 can make meeting arrangements.

Congratulations again and I look forward to working with you and the incoming Government.

Regards

Brent Carey
Chief Executive Officer
Ph 021 925 140

Appendix A: Key issues arising from the Justice portfolio

The key online harm issues for the Justice aspects of the portfolio are the need to update and strengthen the HDCA, increasing harm reports, support for victims of online crimes and enhancing alternative dispute resolution practices, social media and youth offending, victim support, and stalking and harassment. We discuss each below.

Stalking and harassment

We are seeing a dramatic increase in the amount of stalking and harassment online, which can lead to physical and sexual violence. At the moment harassment is covered in a piecemeal way, across different pieces of legislation, including the Harassment Act, the Family Violence Act and the HDCA. Since 2020, successive Ministers of Justice have acknowledged the legislation needs to be reviewed, but work has stalled. We recommend you add stalking and harassment to your law reform programme.

Victim recovery

There is a gap at the moment in victim recovery programmes for people who experience online harm. Survivors of online harm (many of whom are repeat victims) are asking Netsafe to do more to support them recover from online harm.

If Netsafe was funded to place greater focus on victim remediation Netsafe would like to partner with the likes of the Victims Support agency and other victim-centric Justice sector agencies to develop guides (in various languages) that are not victim blaming, and help victims understand their rights and get access to recovery materials and support so they can rebuild their lives.

Justice responses to image-based sexual abuse often fall short of expectations

We need trauma-informed approaches to policies and practices across all sectors responding to image based sexual abuse. Better training and education of law enforcement is needed.

The HDCA needs to be revisited again to consider whether the Act could be more victim-centric when it comes to image based abuse.

Finally consideration should be given to inclusion in law of an expansive definition of what constitutes an "intimate image" in line with different cultural norms and standards.

The Harmful Digital Communications Act urgently needs an update.

The HDCA has a number of limitations and is in need of updates. The limitations include its focus on individuals, not groups as targets of online harm. There have also been advances in technology being used to cause online harm. For example, the HDCA does not explicitly prohibit abuse using artificial intelligence (AI), which is becoming increasingly common. AI allows the creation of deep fake or synthetic intimate images depicting real people in situations that are not real. These can then be shared online and used for threats or blackmail.

Netsafe recommends a review of the HDCA and has attached a high level summary of some potential topics that could be considered as part of the scoping for any review.

The previous Government's Safer Online Services, Media and Platforms discussion paper does not seek to reform any laws where content is already objectionable and harmful, or provide more support for victims. This necessitates strengthening the HDCA and existing structures dealing with illegal content and activities. This would be a better course compared to the untested Safer Online Services, Media and Platforms change agenda.

Harm reports to Netsafe are at record numbers. Complaint forecasts to the end of the financial year 30 June 2024 have us on track to record more than 7000 HDCA complaints. This will see us exceed our 3.9 million appropriation by approximately $200,000. We have signalled this to the Ministry at the end 0508 638 723| netsafe.org.nz.

of quarter 1 and sought assurance that the Ministry of Justice will seek funds from its broader appropriation in which the Netsafe contract sits to pay for peak complaint demand.

Netsafe suggestions for issues to consider as part of a review of the HDCA.

The following suggestions for issues to consider as part of a review of the HDCA have been discussed with the Ministry of Justice.

General improvements

- Most phone calls are technically digital communications as defined in the HDCA. Clarity is needed on whether these should be caught by the legislation.

Potential Loopholes:

  - Airdrop, encrypted data, live stream and disappearing messages are considered digital communications even though they are fleeting and the digital evidence no longer exists or is not readily accessible
- Data that is being shared or has been shared by a private account, that can only be accessed by the account holder or friends
- A threat to share (communicated digitally) is treated the same as content that has been shared.

Individuals and groups:

There are a number of areas where the Act's focus on individuals is a problem:

- Harmful speech targeted towards groups is a potential gap in the legislation because it may not identify any one or particular individual. Consideration of whether the Act should include redress for members of a group who have suffered harm more generally but where an individual is not specifically targeted is needed.
- Small businesses where the content is damaging to a specific individual (eg sole trader) and they suffer harm.
- School leaders cannot consent to engage in the dispute resolution progress on behalf of a student. But they can do so in their own right.

Other

- There is nothing explicitly requiring a connection/ nexus to New Zealand in the legislation which raises jurisdiction and demand for services issues. People in New Zealand as tourists or the wider Pasifika diaspora asking Netsafe for help from overseas. Dealing with people who are overseas is challenging from an evidentiary and service level position.
- There is no Privacy Act carve out for dealing with harmful digital communication matters (section 29).
- Make it clear that the existing prohibition on posting intimate visual recordings without consent clearly covers synthetic or deep fake images where a victim could be identified.
- There are repeat reporters (victims of online harm) who report issues to Netsafe but don't engage with the courts processes beyond Netsafe. We keep issuing case summaries, but they refuse to go to the District Court for remedies. Should there therefore be discretion to not have to produce a case summary unless it is necessary for a Court proceeding?
- Police taking civil cases. To our knowledge, the Police have never taken a civil case against an individual under the HDCA and therefore are not using all the enforcement provisions of the HDCA.
- Mis/dis/malformation is plentiful but is rarely a breach of the communication principles in the HDCA.
- False allegations is typically in the top three comms principles breached. For example, accusations of rape, paedophilia, drug use, infidelity, fraud. Netsafe has no powers to 0508 638 723| netsafe.org.nz investigate. It is not typically a breach of platform community standards without evidence; so can't usually offer any redress except via the district court processes.
- Consider the use of restorative justice solutions and other more victim centric processes. Also consider making the Youth Court (not the District Court) an option for people under 18 years old wanting to resolve their HDCA matters.
- Consider prescribing (under section 7(b)) additional functions such as tackling harms related to body dysmorphia and eating disorders, adult content in video games and cyberflashing.