NCIWR's submission on the inquiry into the harm young New Zealanders encounter online

The National Collective of Independent Women's Refuges | Ngā Whare Whakaruruhau o Aotearoa (NCIWR) is the largest family violence organisation in Aotearoa. We are a non-governmental organisation and have delivered services to women, children, families, and whānau affected by family violence for over 50 years. We represent both victims of family violence, specifically wāhine and tamariki who are the primary groups subjected to and impacted by family violence, and our 41 affiliated Women's Refuges who provide support and advocacy for our clients.

Introduction:

NCIWR recognises that digital abuse is part of a pattern of intimate partner violence, and many victims are exposed to egregious harm online. Intimate partner violence (IPV), inclusive of digital abuse, is ultimately about the (mis)use of personal and structural power by perpetrators. Accordingly, we understand digital abuse as part of a *pattern of behaviour* whereby perpetrators coerce, control, or abuse their partners, and rely on the sense of authority society gives them, and the lack of preventative methods or systems of accountability to justify this behaviour.[i]

Online harm, like in person harm, is a highly gendered phenomenon. Like other forms of gendered violence, it is most commonly perpetrated by men and most commonly perpetrated against women and gender minorities.[ii]

Our understanding of online harm reflects the established and ever-growing body of research into IPV that draws on concepts such as 'coercive control',[iii] and 'social entrapment',[iv] to explain perpetrators' accrual and subsequent misuse of power over victims.

Therefore, the role of digital tactics as part of a broader picture of IPV highlighting perpetrators' intentional use of digital technology to gain and exercise power over victims[v] is prioritised in this submission. This is in contrast to some research which focusses on *singular online behaviours* and paints a picture of mutual digital abuse among youth.[vi]

IPV enacted digitally may look different than in-person IPV, but they share a common cause; namely, a perpetrator's intentional use of violence against a victim.[vii] Research has illustrated how abuse enacted digitally can mirror, amplify, and extend abuse enacted in person, due to the efficiency, reach, and scale that digital technology offers.[viii] As one of the leading scholars in the field of digital abuse puts it: many digital tactics of abuse are in fact "contemporary iterations of traditional forms of abuse".[ix]

In sum, gender-based violence and misogynist views underpin the motives, worldviews, and actions of those who seek to harm women, young people, and children online. As such, any inquiry into online 'harm' needs to be examined through the lens of gendered harm (including gendered power imbalance), coercive control, and entrapment.

As such, there is also a need for a gendered violence perspective when advancing strategies to end online harm. Given the bidirectional relationship, countering 'online harm' is unlikely to be successful without a corresponding focus on countering the dynamics and behaviours of those who cause harm. Without a unified approach that holds individuals, organisations, and service providers to account for the perpetration of online harm, it will perpetuate.

NCIWR's research:

Risk information data collected from clients during their intake to Refuge services in 2024 shows the widespread prevalence of online harm. Younger clients (those aged 15-25) were slightly more likely to report digital abuse (82.5%) compared to those aged above 25 (79.3%).

That said, throughout this submission we will primarily draw from and share the experiences of young women that we collected in 2019 as part of a wider project on *Digital Abuse in the context of intimate partner violence*.

We interviewed participants who had experienced digital abuse by a partner. Thirteen young women aged between 16 and 26 (at the time of the interview) volunteered to share their stories. This project provided an opportunity for participants to share their experiences of online harm and offer their unique perspectives to provide information for other young people.

Participant	Age at start of relationship	Partner's age at start of relationship	Relationship duration
1	**13**	19	9 years
2	**13**	14	6 years
3	**15**	17	4 years
4	**15**	18	3 years
5	**15**	17	1 year
6	**16**	17	2 years
7	**16**	21	2.5 years
8	**18**	26	3 years
9	**18**	24	7 years
10	**19**	23	5 years
11	**20**	24	3 years
12	**21**	33	2 years
13	**24**	28	10 months

These young women experienced both life threatening physical violence and life altering online violence.

We found that the digital abuse these women described was not a stand-alone issue, nor a *solely* technologically derived problem. While the digital abuse was widespread and devasting, it did not involve complex or nefarious technologies, spyware, or tracking systems. While those exist, they were not reflected in these young victims' experiences; for the most part their perpetrators used everyday forms of technology.

The complexity of participants stories stems not from the technology itself, but from both:

- The insidious use of it as part of a wider pattern of coercion, control, and violence faced by young women, and
- The inadequate understanding and responses from systems to it as a serious and debilitating part of partner violence.

For these women, digital technology was used to enact (and served to intensify) the IPV perpetrated against them.

Terms of reference and the scope of inquiry:

We applaud the Education and Workforce Select Committee's initiative to launch an inquiry into the harm young New Zealanders encounter online.

The definition of 'online harm' is too broad

We wish to draw attention to the first aim in the 'Terms of Reference': *examine the nature, severity, and prevalence of **online harm** experienced by young people in New Zealand, including but not limited to online bullying, exploitation, addictive use, mental health impacts, educational impacts, and exposure to harmful content*.

The term *"online harm"* is vague, and it is therefore difficult to ascertain which forms of harm are being prioritised and why. It obscures the purpose of, and the intent behind, the inquiry. Although all forms of harm create risks and impacts for victims, the spectrum of what constitutes 'harm' in this instance is broad and unclear.

We are concerned as the examples of online harm given in the terms of reference (quoted above) may miss the opportunity to scrutinise this issue as an intentional effort to exert power and control. This would result in neglecting to understand the context we know gender-based online harm occurs in; as a purposeful pattern or campaign of abuse, where power and control are weaponised to entrap victims.

What is the source of the harm?

We also wish to draw attention to the first point in the 'approach to the inquiry': *consider the social, educational, and developmental benefits that online activity may offer to young people, and the extent these benefits are realised*.

Weighing up the balance of 'harm and benefit' is important, and we commend the inquiry for its attempts to do so. However, we are concerned that the current approach obscures the source of the problem – the purposeful perpetration of abuse, and shifts the problem solely to the devices used to cause harm, rather than the individuals who perpetrate abuse and the service providers who fail to disrupt the trajectories of risk and abuse.

It is important to conceptualise technology-related risk by attributing the source of harm to those who perpetrate abusive behaviour rather than to 'risky youth', 'curious youth', or 'technologically incapable youth'.

There has been a lot of media attention regarding Governments' intention to restrict or prohibit social media use for people under 16. While it is important to recognise that young people face online harm, we are worried this misses the real issue: that harm is caused by perpetrators' actions and by platforms failing to keep users safe, not simply because young people 'use social media'.

We can no longer easily separate our daily lives from our use of digital technology. Across the country, 91-93 percent of people access the internet,[x] and approximately 80% of households have an internet service. Digital technology is now acknowledged as important for full social participation in Aotearoa[xi], with young people utilising it in educational, vocational, and social environments. Connectivity is not a 'nice to have' it is essential for full and active participation in society.

What our digital abuse project found was that as young women's lives are increasingly digitally mediated, so too are the tactics of abuse that are used against them. Alongside their accounts of how perpetrators used digital technology as a weapon of abuse, however, the young women also detailed how they themselves were able to use it to build safety and support.

Participants gave examples of how they used their knowledge of digital mechanisms of safety to resist the reach of digital abuse tactics over their lives. Using the opportunities that technology presented, many participants were able to improve their own safety for themselves and those around them, and to take back some of the control their partners had appropriated over their lives. They spoke about how they used their own technological proficiency to limit the effectiveness of their partners' digital tactics.

As technology advances and victims' lives became more digitally mediated, their forms of resistance also became more digitally mediated. Victims' incorporation of digital capabilities into their resistance of violence underlines the inseparability of their physical selves and digital selves, and, by extension, the inseparability of their physical safety and their digital safety.

We hope that the focus will be on the scale and severity of online harm, the sources of the harm, and the regulations for service providers, not simply the spaces that are weaponised by predators and perpetrators to cause harm.

Gaps in the system:

Our digital abuse project showed that often perpetrators are much older that their victims, hold more social power, and have greater access to resources.

Many solutions to online harm aimed at young people involve educating young women on how to keep themselves safe online. While this is important and necessary, there is no equivalent education or approach that focuses on holding people who cause harm to account. Educational solutions need a gender-based perspective that teaches young people not to abuse others.

When solutions to mitigate online harm ignore the risks and impacts young women already face, they overlook the heavy burdens these young women carry and what they have to deal with when they are exposed to harmful content.

Lack of support for victims

One participant shared her story of abuse; her perpetrator used multiple websites with international reach to non-consensually share their video-recorded sexual encounter. She explained that most of the workload rested solely on her to undo and mitigate the harm he caused to her. In contrast there was no justice penalty, impact, or accountability for her perpetrator. The responsibility for his offending fell to her.

She detailed the sheer volume of tasks she had to take responsibility for, and the repetitive and cumulative frustration she felt when even after lengthy time investments, these proved insufficient to guarantee her any satisfactory resolution of the abuse.

Her safety workload included:

- dealing with her own emotional distress upon discovering the publicly accessible recordings of herself
- figuring out where to get advice from
- calling support services and helplines
- filing her complaint
- taking screenshots and screen-recordings of the intimate recordings
- finding information on pornography websites about how to have each one removed
- reporting it to the Police and following up with them when they did not act
- familiarising herself with aspects of criminal and civil law relating to non-consensual sharing of intimate content online
- trying to find counsellors or support groups
- trying to prove her eligibility for funded counselling
- finding (and paying for) a lawyer
- repeating her story to numerous individuals and service providers
- writing and swearing an affidavit and preparing relevant exhibits

- educating frontline providers about the nature and impact of digitised sexual abuse
- advocating for herself with Police decision-makers
- advocating for legislation change

She struggled to find the right support or expert advice.

> *Unfortunately, the helplines have little idea what to do if it's a bigger worry than online bullying or a privacy issue. They do not guide you down this path of the unknown. They don't tell you 'you need to do x, y, z'. If it gets complicated, they can't even do it for you. They tell you to go to the Police, but they don't sit there and hold your hand with you. They don't talk you through what the process is once you have been to the Police. They don't talk you through the process of court. They don't talk you through going to a lawyer. They don't talk you through what the legislation actually means, or what the interpretation of it is, and the gaps in interpretation and application of it.*

So, she had to find many of the answers herself.

> *I had to use an alternative search engine which is a bit more encrypted. I had to be a detective and find a VPN changer because he had hidden videos of me, and I needed access to find them to get them taken down.*

> *I had taken screen recordings of all the videos. It was very, very hard for me to do that, so I didn't want to watch myself, I screen-recorded all the videos because I thought, 'no, this isn't okay'.*

She went on to say that it feels like there is no support during or after experiencing online harm.

> *[There is] nothing, there is no support group at all, from Auckland to Invercargill. I have looked. I can't find anything. All these sexual assault websites have things [written about] sexual abuse from digital harm, but then you call them and they say 'I don't know anything about it'. So from there, it has been really, really hard.*

Her experience was shared by the rest of the participants, who also noted that the onus for 'getting safe' was often placed entirely on them, as victims. The effort, workload, and initiative required of them at the times when they were already vulnerable highlights the consequent discrepancy between what they needed to be safe, and what safety was made (in)accessible to them by others.

The experiences of these young women clearly highlight the need for prevention strategies that:

- Target perpetrators and people who use harm
- Improve the efficacy and reach of support services

- Remove the burden off victims of online harm

Lack of system knowledge about online harm

Our project also collected experiences of those who had navigated justice pathways. The onus for 'getting justice' also seemed to land on victims. Participants' stories show that discomfort and uncertainty about digital technology (especially the misuse of it by intimate partners) amongst those with judicial decision-making power negated their opportunities for safety and satisfactory resolution and also exacerbated their workload.

There appeared to be a lag between the digitised nature of the harm and the extent to which justice actors were procedurally equipped to acknowledge, cater for, and prove cases of digitally enacted harm. This gap between the nature of digital offending and procedural competence in responding to digital offending meant the onus to evidence, explain, and make sense of digital tactics fell disproportionately to victims.

> *I also found it really hard to find a lawyer who has knowledge of the Harmful Digital Communications Act... I contacted 7 lawyers, reputable law firms in [city] well known ones not just little tiny ones, nobody had dealt with Harmful Digital Communications Act. I even contacted a lawyer at a specialist IT law firm who deals with the digital communication, you know, like Ips, licencing those sorts of things, [but] they told me they had never dealt with [the] Harmful Digital Communications Act before, and they didn't know what it entails, or the legislation involved.*

> *I think that it is [because] digital communications and IT, it is a fluid thing it is changing. It could be someone has posted something online that I don't like, someone has slandered my name and so I just think there is no real push for people to familiarise themselves with the legislation. I found it really hard to engage them for advice.*

Another participant had collected screenshot evidence of her perpetrator's online harm. However, prosecuting the abuse was made difficult by the court's threshold for evidential sufficiency and the defence's challenging of the veracity of her screenshots, highlighting the ambiguity surrounding adequate authentication of digital forms of evidence.

> *He [perpetrator] had two phones and so the Police seized one but that was his burner phone. He had a person to go through all his files and present those to the court to say this is the [complete] history of everything [but] because Snapchat is a third party app, even if the Police go through all the files that are there, unless it is [data] that is inherently built into the system like a text message or a phone log or contacts that kind of stuff [they can't access the data].*

There is no way for people to prove the videos, images, or threats [are from the perpetrator]... because that is what my ex's lawyer tried to say, like, 'who is to say she hasn't faked the screenshot?'... Like you look at online bullying [for example], like someone can report it, but if you go in [as a defence lawyer] and say 'look the screenshot has been faked' then they have no way to prove it has or it hasn't, because they can't access the other person's information from the other end.

She went on to explain how an outdated legislative and policy setting (such as a lack of policy guiding the collection and admission of evidence held on third-party digital platforms and difficulty accessing legal teams at third-party digital platforms) can impede successful prosecution of online harm and, as a result, how much she had to do herself to overcome these gaps.

I reached out to Snapchat because I don't believe the Police understood where they needed to go with that. I just messaged Snapchat on Twitter.

There are people making [justice] decisions that don't know what a service provider is, or that there are many ways to transfer info between your browser and a website.

The whole process of trying to explain how him sending me things on Snapchat is harmful. Just trying to explain Snapchat to a 70-year-old judge. I just think people in the justice system need to be aware of how intricate technology is nowadays, and it is even getting worse and worse, like the amount of ways you can get away with stuff, with hiding who you are, and like with the ease with which people can get your personal information is just insane.

[The justice system] just needs to have people that are like unbiased tech experts, that can be like 'okay this is a really complicated way to explain it but here is me dumbing it down, so that you who still uses Internet Explorer can understand it'.

Perpetrators use the online space to access young people, to hide, maintain secrecy, conceal their identity and the extent of their reach, and to exercise control over them. Victims described how these environments allowed perpetrators to enter their lives without detection to initiate and escalate contact.

The experiences of these young women clearly highlight the need for prevention strategies that:

- Target perpetrators and people who use harm
- Upskill those with decision making power
- Improve the efficacy of justice pathways
- Impose regulations and duties on online service providers to protect children, young people, and other vulnerable users

Lack of systemic accountability

The following quote is testament to the sentiment threaded throughout many of our participants' stories: the people they disclosed to about their perpetrators' use of online harm tended to relegate these tactics to a presumptive category of lesser severity and significance.

> *They were like 'why don't you just block him' and I'm like I want him to get in trouble for what he has done to me, like I want to be able to prove to him there are consequences. That is what his lawyer said as 'well if you didn't want it to happen why don't you block him' and I'm like I don't get in trouble for not doing anything with my account. He is the one that cannot contact me, he can't contact me himself or get people to contact me on like his behalf or contact people like my friends for me, he is the one doing the wrong thing.*

The trivialisation of digital abuse present in victims' stories held them responsible for their own safety and justice, while the perpetrators faced little or no consequences for their abuse. This is a pattern seen across many forms of gender-based violence and reflects a gendered logic of responsibilisation.[xii]

The pattern of placing responsibility on women to 'keep themselves safe' contributes to a wider narrative of victim blaming – the 'problem' that responders and systems focus on becomes women's (in)action rather than men's violence. This in turn emboldens men's harmful behaviour through a lack of suitable accountability measures.

To even begin to address the issue of digital abuse and online harm there needs to be an explicit and reinforced effort to ensure that the responsibility for this harm lies with firstly, the perpetrator, and secondly, the service providers and systems that fail to prevent it.

Recommendations:

Adopt a gendered violence lens

- Ensure all strategies incorporate a gendered violence lens and centre on accountability and prevention

Acknowledge and address gender-based harm

- Recognise gender-based harm in online spaces and address this behaviour both online and offline to prevent further harm

Increase accountability for perpetrators

- Hold individuals who perpetrate abuse to account for their actions
- Make systems and platforms accountable for enabling or failing to prevent harm

Mandate reporting and regulation

- Introduce reporting schemes for online abuse

- Impose regulations and duties on online service providers to protect children, young people, and other vulnerable users

Focus on prevention and education

- Ensure solutions that educate young people about online safety also focus equally on preventing the behaviours that cause harm and target those most likely to cause harm

- Include community and family education as part of these solutions

Strengthen relationships and sexuality education

- Enhance education frameworks in schools to include healthy communication, digital literacy, and understanding of gendered harm, rather than focusing only on 'risky behaviour'

Upskill decision makers

- Provide digital literacy training to those with legislative and policy decision-making power to improve the quality of responses

- Remove the burdens on victims to prove their victimisation and the harm they experienced

Enforce existing laws

- Strengthen the impact of current laws by enforcing them consistently and effectively

Improve institutional responses through key ministries:

- Strengthen education and digital literacy

- Enforce existing laws

- Hold platforms accountable through regulation and international cooperation

- Protect children, women, and other people made vulnerable by the actions, behaviours, and offending of others.

[i] Stark, E. (2024). *Coercive control: How men entrap women in personal life 2ed*.; Reed, L. A., Tolman, R. M., & Ward, L. M. (2016). *Snooping and sexting: Digital media as a context for dating aggression and abuse among college students.*; Harris, B. A., & Woodlock, D. (2019). *Digital coercive control: Insights from two landmark domestic violence studies.*; Havard, T. E., & Lefevre, M. (2020). *Beyond the power and control wheel: How abusive men manipulate mobile phone technologies to facilitate coercive control.*; Henry, N., Flynn, A., & Powell, A. (2020). *Technology-facilitated domestic and sexual violence: A review.*; Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). *Technology-facilitated domestic and family violence: Women's experiences.*; Thompson, M. P., & Morrison, D. J. (2013). *Prospective predictors of technology-based sexual coercion by college males*.

[ii] Todd, C., Bryce, J., & Franqueira, V. N. (2021). *Technology, cyberstalking and domestic homicide: Informing prevention and response strategies.*; Marin, A. J., & Russo, N. F. (1999). *Feminist perspectives on male violence against women: Critiquing O'Neil and Harway's model.*; Smyth, A. (2002). *Feminist resistance to male violence against women. Which perspectives?*; Family Violence Death Review Committee. (2019). *Fifth Report Data: January 2009 to December 2015.*; Vine. (2025). *Frequently Asked Questions.*; World Health Organisation. (2021). *Violence Against Women.*; Fanslow, J. L., & Robinson, E. M. (2011). *Sticks, stones, or words?*

Counting the prevalence of different types of intimate partner violence reported by New Zealand women. Powell, A., Scott, A. J., & Henry, N. (2020). *Digital harassment and abuse: Experiences of sexuality and gender minority adults.*

[iii] Stark, E. *Coercive Control: How men entrap women in personal life 2ed.*; Harris, B. A., & Woodlock, D. (2019). *Digital coercive control: Insights from two landmark domestic violence studies.*

[iv] Dragiewicz, M., Harris, B., Woodlock, D., Salter, M., Easton, H., Lynch, A., ... & Milne, L. (2019). *Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime.*

[v] Harris, B. A., & Woodlock, D. (2019). *Digital coercive control: Insights from two landmark domestic violence studies.*; Dragiewicz, M., Harris, B., Woodlock, D., Salter, M., Easton, H., Lynch, A., ... & Milne, L. (2019). *Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime.*; Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., & Pracilio, A. (2020). Second national survey of technology abuse and domestic violence in Australia.; Harris, B. A., & Woodlock, D. (2019). *Digital coercive control: Insights from two landmark domestic violence studies.*; Todd, C., Bryce, J., & Franqueira, V. N. (2021). *Technology, cyberstalking and domestic homicide: Informing prevention and response strategies.*; Havard, T. E., & Lefevre, M. (2020). *Beyond the power and control wheel: How abusive men manipulate mobile phone technologies to facilitate coercive control.*

[vi] Tokunaga, R. S. (2010). *Following you home from school: A critical review and synthesis of research on cyberbullying victimization.*; Borrajo, E., Gámez-Guadix, M., & Calvete, E. (2015). *Cyber dating abuse: Prevalence, context, and relationship with offline dating aggression.*; Lucero, J. L., Weisz, A. N., Smith-Darden, J., & Lucero, S. M. (2014). *Exploring gender differences: Socially interactive technology use/abuse among dating teens.*

[vii] Henry, N., Flynn, A., & Powell, A. (2020). *Technology-facilitated domestic and sexual violence: A review.*; Harris, B. A., & Woodlock, D. (2019). *Digital coercive control: Insights from two landmark domestic violence studies.*; Henry, N., Vasil, S., Flynn, A., Kellard, K., & Mortreux, C. (2022). *Technology-facilitated domestic violence against immigrant and refugee women: A qualitative study.*; Havard, T. E., & Lefevre, M. (2020). *Beyond the power and control wheel: How abusive men manipulate mobile phone technologies to facilitate coercive control.*; Stonard, K. E., Bowen, E., Walker, K., & Price, S. A. (2017). *"They'll always find a way to get to you": Technology use in adolescent romantic relationships and its role in dating violence and abuse.*; Dragiewicz, M., Woodlock, D., Salter, M., & Harris, B. (2022). *"What's mum's password?": Australian mothers' perceptions of children's involvement in technology-facilitated coercive control.*; Dragiewicz, M., Harris, B., Woodlock, D., & Salter, M. (2021). *Digital media and domestic violence in Australia: essential contexts.*

[viii] Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., & Pracilio, A. (2020). *Second national survey of technology abuse and domestic violence in Australia.*; Henry, N., Flynn, A., & Powell, A. (2020). *Technology-facilitated domestic and sexual violence: A review.*; Dimond, J. P., Fiesler, C., & Bruckman, A. S. (2011). *Domestic violence and information communication technologies.*; Woodlock, D., McKenzie, M., Western, D., & Harris, B. (2020). *Technology as a weapon in domestic violence: Responding to digital coercive control.*; Harris, B. A., & Woodlock, D. (2019). *Digital coercive control: Insights from two landmark domestic violence studies.*; Havard, T. E., & Lefevre, M. (2020). *Beyond the power and control wheel: How abusive men manipulate mobile phone technologies to facilitate coercive control.*; Dragiewicz, M., Woodlock, D., Salter, M., & Harris, B. (2022). *"What's mum's password?": Australian mothers' perceptions of children's involvement in technology-facilitated coercive control.*; Dragiewicz, M., Harris, B., Woodlock, D., & Salter, M. (2021). *Digital media and domestic violence in Australia: essential contexts.*

[ix] Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). *Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms.*

[x] Internet NZ. (2017). *State of the Internet 2017: The State of the Internet in New Zealand.*

[xi] Zwimpfer, L., Crothers, C., Smith, P., Craig, B., Cotter, C., Alford, M., Nixon, C., & Yeung, S. (2017). *Digital New Zealanders: The Pulse of our Nation.*

[xii] Jordan, J. (2022). *Tackling Rape Culture: Ending Patriarchy.*