Australian Government

Office of the
eSafety Commissioner

FEBRUARY 26, 2019

NATIONAL INQUIRY INTO SEXUAL HARASSMENT IN AUSTRALIAN WORKPLACES

OFFICE OF THE ESAFETY COMMISSIONER SUBMISSION

Introduction

The internet and digital technologies have revolutionised the lives of Australians – and Australian workplaces.

The increasing connectivity of Australian workplaces presents enormous benefits and opportunities. It also presents risks and harms, including cyber abuse.

Sexual harassment, like cyber abuse, is a complex issue that defies single or simple solutions.

As Australia's leader in online safety, the Office of the eSafety Commissioner (Office) welcomes the opportunity to provide a submission to the *National Inquiry into Sexual Harassment in Australian Workplaces* (Inquiry).

Our submission begins by highlighting the complex nexus between social, cultural and behavioural factors and cyber abuse. Given the interconnection between cyber abuse and online sexual harassment, we then draw upon our experience regulating online safety issues to offer insights and recommendations that may serve as a useful frame of reference for the Inquiry.

Terms of reference

The Office acknowledges that it could approach the terms of reference both as an employer and as a regulator. We have focused our submission on our regulatory role in promoting online safety, particularly the terms of reference relating to social media and technology. However, we want to reiterate that the Office takes a no tolerance approach to sexual harassment in the workplace and has practices, policies and procedures in place to prevent, manage and address sexual harassment.

The eSafety Commissioner has a constructive and collaborative working relationship with the Sex Discrimination Commissioner. Given the terms of reference relating to social media and technology, the Office also wants to reiterate its willingness and interest in assisting in responses and recommendations related to these issues.

Throughout this submission, we have used the term 'victim' to describe people who have experienced abuse or harassment. We acknowledge that some people use the term 'survivor'. We respect individual choice and encourage individuals to use language and terminology consistent with their experiences and beliefs.

Regulatory approach and activities

The Office leads, coordinates and advises on online safety issues to ensure all Australians have safe, positive and empowering experiences online.

Since 2015, the Office has administered a complaints service for Australian children who experience serious cyberbullying. The scheme serves as a safety net for young people who haven't been able to resolve their online issue via the social network's reporting functions. We work closely with social media services to help remove harmful material and provide relief for a young person and their family.

Since the introduction of the scheme, we have received over 1,100 complaints about cyberbullying affecting Australian children.

In July 2017, the Office's remit was expanded to cover all Australians. As the cyberbullying legislative scheme was not expanded to cover adults, if a person is experiencing serious cyber abuse, but their circumstances do not fall within one of our complaints or reporting schemes, we focus on providing information, guidance and support. Depending on the nature, context and severity of the online abuse, we may be able to draw upon our cooperative arrangements with social media services to informally provide relief to the individual. This may involve getting cyber abuse material removed.

We informally helped 702 adults in 2018, with the number of reports in the second half of 2018 representing an approximate 40% increase from the first half of 2018.

In October 2017, the Office introduced an image-based abuse portal to provide tangible support for Australians of all ages who have had their intimate image or video shared without their consent. In September 2018, our powers in this area were expanded with the establishment of a civil penalties scheme.

As at 31 December 2018, the Office had received 614 reports of image-based abuse. Despite nearly all the websites reported to date being hosted overseas, the Office has been successful in having image-based abuse material removed in over 80% of cases where removal was requested.

The Office's complaints data does not record whether cyber abuse occurs within the workplace, as whether or not the abuse occurs within or in connection to the workplace is not a requirement under any of our complaints or reporting schemes. Further, in order to promote the privacy and agency of victims, we aim to collect the minimum amount of information necessary to both satisfy our regulatory requirements and enable us to take action to provide a victim relief and support.

However, operating a number of complaints and reporting schemes within one Investigative Division allows us to identify crucial similarities and differences between the forms of online abuse. For example, we know that both girls and women tend to be bullied more than boys and men (66% of our cyberbullying reports come from girls). In contrast, one of the fundamental differences between youth-based cyberbullying and adult cyber abuse is that cyberbullying tends to be peer to peer and an extension of conflict happening within the school yard, while adult cyber abuse is often perpetrated by strangers.

Relationship between cyber abuse and online sexual harassment

There is a complex and multilayered relationship between cyber abuse and online sexual harassment.

Cyberbullying under the *Enhancing Online Safety Act 2015* is online behaviour that an ordinary reasonable person would conclude is likely to have a seriously threatening, seriously intimidating, seriously harassing or seriously humiliating effect on an Australian child. The Office has adopted this definition for cyber abuse, which we use as an umbrella term to capture different types of online abuse and that we apply more broadly to include adults. We categorise image-based abuse as a form of cyber abuse.

Sexual harassment under the *Sexual Discrimination Act 1984* is any unwelcome sexual advance, request for sexual favours or conduct of a sexual nature in circumstances where a reasonable person would have anticipated the possibility that the person harassed would feel offended, humiliated or intimidated.

Certain forms of online sexual harassment may therefore be a subset of cyber abuse. However, in order to constitute cyber abuse, the online behaviour must be serious. If online sexual harassment does not meet the threshold of seriousness, it may not constitute cyber abuse.

Whether online sexual harassment constitutes cyber abuse will therefore depend on the nature, context and severity of the online sexual harassment.

We believe that cyber abuse, including the extent it encompasses online sexual harassment, is fundamentally a manifestation of social, cultural and behavioural issues.

We therefore adopt a case management approach to our complaints and a wide, proactive and whole of community preventive approach to online safety. This includes driving a balance of awareness raising, education, regulation and technological measures. It also includes focusing on preventing the behaviours, attitudes and beliefs that underpin cyber abuse.

We believe a similar multifaceted approach, drawing upon the insights of our regulatory experience, may be useful for understanding and addressing online sexual harassment.

Technology and society

The findings of the *Everyone's business: Fourth national survey on sexual harassment in Australian workplaces* (2018 Sexual Harassment Survey) show that almost one in three women and one in five men have been sexually harassed online or via some form of technology.

It found a range of common sexual harassment activities perpetuated through technology, including:

- sexually explicit comments made in emails, SMS or on social media
- indecent phone calls (including voicemail messages and answering machine messages)
- repeated or inappropriate advances on email, social networking websites or internet chat rooms
- threatening to share intimate images without consent, and
- 'any other unwelcome conduct of a sexual nature that occurred online or via some form of technology'.

It is important to stress two points about the relationship between technology and cyber abuse: one, technology is a mechanism for the expression of *existing* forms of abuse; two, technology can facilitate *new* forms of abuse.

Cyber abuse is a 21st century manifestation of both bullying behaviour and social issues that have existed throughout history. There is a strong nexus between the inequality, discrimination and disrespect underpinning abuse online and offline. In other words, social media can serve to surface the reality – and frankly, the underbelly – of the human condition, including sexism, racism and homophobia.

At the same time, by enabling new forms of communication and engagement, modern technologies can magnify, enable and perpetuate abuse on a greater scale.

Image-based abuse is a compelling example of this. While intimate images and videos could previously have been shared without consent, modern technologies have greatly increased the scale and impact of distribution.

Cyber abuse can also be more covert, more invasive and more pervasive than traditional bullying. Further, online interactions differ from offline interactions in key aspects that may facilitate abuse. For example, the online disinhibition effect refers to people engaging with less social inhibitions in online interactions in comparison to in-person communication. Algorithms can also prioritise content based on criteria that don’t readily recognise that material is abusive or harmful.

While many of today’s online and social media services were developed to promote a diverse set of voices, freedom of expression and the speaking of truth to power, we have seen an increasingly dark side of the internet that is reflective of societal norms.

Ultimately, to understand how sexual harassment is manifesting in a modern workplace context, we need to understand what has historically driven sexual harassment, as well as the new and developing characteristics of cyber abuse and contemporary online sexual harassment.

Women, cyber abuse and sexual harassment

The Office undertakes an extensive research program to ensure our programs and resources are evidence based. This equips us with the insights and knowledge we need to understand the nature of online safety issues and design, implement and evaluate best possible solutions.

The full suite of the Office’s research findings, as well as all the research referenced throughout this submission, is available at the Office’s Research Library at www.esafety.gov.au/about-the-office/research-library.

From our research and programs, we know that while women are targeted in different ways, women overall are disproportionate targets of cyber abuse.

Our 2017 *Image-based abuse: National survey - summary* report shows women are twice as likely to experience image-based abuse compared to men.

Not surprisingly, more than two-thirds of our complaints about cyber abuse and image-based abuse involve women.

Women are more likely to experience abuse that is personal, sexual and gender-based.

Rooted in misogyny and reflecting society's broader gender inequality, often the abuse targeted at women is *because they are women*.

These gendered double standards also mean women face more significant repercussions than their male counterparts for perceived online transgressions, especially when they are perceived to have violated gender stereotypes.

A study released by Amnesty International and Element AI in December 2018 measured violence and abuse against a group of 778 women on Twitter.[1] It found that 7.1% of tweets sent to the women in the study were 'problematic' or 'abusive'. This equates to 1.1 million tweets mentioning the 778 women across the year, or one every 30 seconds.

While women are a key target, online abuse is also intersectional. Regrettably, people - women, men and non-binary - also experience abuse on grounds including sexual orientation, race, religion, disability and age.

Our 2017 *Image-based abuse: National survey - summary* report indicates that 1 in 10 Australians aged 18 years and over have had their intimate image/s or video/s shared without their consent. This increases to 1 in 4 women between the ages of 18–24 and 1 in 5 for those identifying as LGBTIQ. 1 in 4 Aboriginal and Torres Strait Islander people have experienced image-based abuse.

The Amnesty International and Element AI study found that women of colour were 34% more likely to be mentioned in abusive or problematic tweets than white women.

Intersectionality is equally relevant in the context of workplace harassment. For example, it can be difficult for women to extricate themselves from workplaces without suffering ramifications, especially economic ramifications. This is compounded for women with a disability, where physical, attitudinal, communication and social barriers may not accommodate or enable them to access and leave environments. Women in rural and regional Australia may have limited alternative employment options.

A 2016 Women in Media study found that more than one in five journalists have been cyberbullied, with 41% being trolled.[2] 60% of respondents believed harassment was more likely to be directed at women. The experience for some respondents was so extreme that they left the industry. Others changed the way they interacted with their audiences on social media.

Attacking a woman personally is often a deliberate tactic to silence her voice.

[1] Amnesty International and Element AI, Troll Patrol, December 2018, accessed at: https://decoders.amnesty.org/projects/troll-patrol/findings#what_did_we_find_container

[2] Women in Media, Mates over Merit?, June 2016, accessed at: https://www.meaa.org/download/mates-over-merit-full-report/

One of the key roles of the Office is ensuring women's voices are protected and promoted - not silenced.

This reinforces the importance of ensuring our responses do not marginalise or disempower women, especially women who are disproportionately impacted by the complex intersection of risk factors that make some people more susceptible or vulnerable to online risks and online harms. Excluding women and the use of technology in the workforce would exacerbate existing gender inequalities. Further, it negates the benefits that social media and the internet can bring in amplifying the voices of women who are too often silenced in public debate: Aboriginal and Torres Strait Islander women, women from culturally and linguistically diverse (CALD) communities, women who identify as LGBTIQ and women with disabilities.

This reinforces why the Office takes an inclusive and strengths-based approach, in which an individual's diversity, strengths and resilience are understood as important factors that can protect them from online harms.

We must also remember that this is not a women's issue: it is a societal issue that requires a societal response. Indeed, it was to further this social imperative that the Australian Government formed the Office as a regulatory agency dedicated to safeguarding the online safety of its citizens.

Office's women's programs and initiatives

The Office's women's programs and initiatives are both broad and targeted to align with the breadth and nature of the abuse women receive online.

Our eSafetyWomen initiative is specifically focused on women who are vulnerable to technology-facilitated abuse, as it is nearly almost an adjunct to domestic and family violence. We know through research with workers who support women experiencing domestic or family violence that 98% of cases involve some form of online abuse, surveillance or stalking. eSafety Women aims to empower women to manage technology risks and abuse and take control of their online experiences. We know that access to technology is crucial for enabling women to stay connected to their family and friends, as well as information and support services.

Since its launch in 2016, more than 7,200 domestic and family violence frontline workers across Australia have participated in eSafetyWomen training.

Our newest women's initiative, Women Influencing Tech Spaces (WITS), was launched in May 2018 to help women who are also disproportionately targeted for online abuse – those in the public eye. WITS is an initiative to both protect and promote women's voices. It recognises that women in leadership positions and with public personas, ranging from politics, business, media, sports and academia, experience shockingly high levels of abuse.

It also recognises, however, that social media can be, and should be, a powerful tool for women to engage, connect, communicate, learn and grow. For women in the workplace, it is an increasingly powerful tool to promote their voices and work, develop their professional connections and stay engaged with emerging issues.

Our objective with WITS is to give women the psychological armour to counteract cyber abuse and interact online with impact, confidence and resilience.

Intersectionality factors can also lead to women being targeted with abuse and our ongoing research with CALD women will bolster our understanding and responses to this. Our most recent research in this area, released in February 2019 and referred to later in this submission, is qualitative research on CALD women who have experienced technology-facilitated abuse. This is the first time in Australia that research focusing specifically on technology-facilitated abuse experienced by CALD women has been conducted.

Just as the Office's women's programs and initiatives are aimed at helping women stay connected safely and positively, our responses to cyber abuse and online sexual harassment must be aimed at empowering women to use technology and take back control.

Increasingly connected workplaces

Workplaces are becoming increasingly connected. The boundary of the workplace has been extended with digital devices. This, in addition to the fact that the online world doesn't operate to standard business hours, is blurring the distinction between private and professional lives.

Many employers now require or encourage their staff to be online. Social media, instant messaging services and other online collaborative forums have increased the channels for communication. While these services allow for increased collaboration and engagement, they also increase opportunities for cyber abuse and harassment.

It can be difficult to establish nuance online. Whether liking a tweet or sending certain emojis could amount to cyber abuse or harassment will depend on a number of circumstantial and contextual factors.

Employers often do not have policies in place to address these communication channels. Employees may be deterred from raising issues due to a lack of awareness of redress options, out of concern about discrediting business process, out of fear of being disbelieved or because they worry they'll be disadvantaged in career opportunities. Sadly, they also fear losing their job. These factors can lead to significant underreporting.

We must remember there is an inherent power imbalance between an employee and employer.

However, increased digital connections also means increased digital footprints. Perpetrators may leave a trail of data evidencing their harassment. This helps rectify the fact that historically a lack of evidence has made sexual harassment difficult to establish.

Digital records, screenshots and emails can be used to identify and verify harassment. Developments in artificial intelligence, as well as word and phrase filtering, can also be used to block, record and report harassment.

For example, we provide women information on collecting evidence as part of eSafetyWomen. We outline how to take screen shots of abusive posts, texts and email, as well as how to save and copy voicemails. More broadly, we encourage women to keep a record of any technology abuse and suspicious incidents, as this can help establish context and demonstrate patterns of behaviour by the perpetrator.

This means that while technology can be used to perpetuate abuse, it can also be a tool to fight harassment and hold perpetrators to account. This underscores the importance of empowering staff in all workplaces with the knowledge and skills to collect evidence, which can then be raised with their employer as part of an early intervention approach to minimise harms.

Anonymity

The need to have the right processes in place to manage the benefits and risks of technological advancements can also be demonstrated through the issue of anonymity.

Anonymity can facilitate negative online behaviours, as it allows individuals to freely exhibit inappropriate behaviour and attitudes without the normal social repercussions.

If an anonymous or impersonator account is implicated in image-based abuse, we report the account to the relevant platform for suspension or deletion. With other online harassment, we give guidance on how to report the anonymous or impersonator account to the relevant platform.

From reports made to us, and from the feedback we receive from the domestic and family violence frontline workers we train through eSafetyWomen, we know that current and former partners frequently use fake or impersonator accounts to abuse a woman. This is often done to reinforce control or to seek to cause harm through reputational damage. The perpetrator may set up an account that falsely represents to be the woman herself, her children or one of her family members, friends or trusted colleagues.

It can be difficult to have these accounts removed, especially when the woman is in a state of acute distress and trying to address a range of abusive and threatening behaviours. Exacerbating this situation is the fact that online platforms often put the burden on the victim to prove that the imposter account is not, in fact, them.

If this information is brought to us as part of a report of technology-facilitated abuse in a domestic violence situation, we provide advice on how to report the impersonator account, as well as guidance on the availability of support services and other action that might be taken.

At the same time, anonymity can afford women some useful protections by allowing victims to regain a sense of control over their experience. For example, there are now anonymous reporting app options that greatly ease the reporting process for complainants. Anonymity can also be used to help shield and protect a woman’s identity, which can provide her physical safety or protect her from online abuse. In some instances, the fear of retribution means that without anonymity, women's voices would otherwise be silenced.

The Office also allows complaints about image-based abuse or cyber abuse to be made using a pseudonym. We require some means to contact the complainant, typically an email address, but this can be a non-identifying email account set up specifically for this purpose.

We are very conscious of respecting a victim's privacy in our complaints processes, especially since image-based abuse represents one of the most egregious forms of privacy invasion. For example, when our Image-Based Abuse Team is gathering information or collecting evidence about a particular matter, they may need the victim to send them screen shots or information that includes their intimate images. We always ask the victim if they feel comfortable sharing the information and invite them to edit or black out parts of the image (e.g. 'private parts') they'd prefer not to share. This helps restore a sense of agency and control to the victim.

The issue of identity and anonymity is therefore representative of the Office's objective of harnessing the benefits of digital technologies and advancement, while mitigating and managing the risks.

Underreporting of cyber abuse and sexual harassment

Both cyber abuse and sexual harassment are significantly underreported.

The findings from the 2018 Sexual Harassment Survey show that only 17% of people who experienced workplace sexual harassment in the last five years made a formal report or complaint.

These findings closely mirror the research we have relating to our work with children's cyberbullying and image-based abuse.

The results of our 2017 national youth survey, released in our *State of play – youth, kids and digital dangers* report, showed that only around 24% of young people who had a negative online experience sought help in a formal way through their school, a social media company or the police.

Our research has shown that barriers to young people reporting cyberbullying include feelings of shame and embarrassment, fear of retaliation and fear of not being believed. Young people also had fears about the complaints process, including that they would lose control over the complaints process and that the issue would escalate and become public, resulting in the loss of their anonymity.

From our 2017 *Image-based abuse: qualitative research summary* report with female victims of image-based abuse, we know that most women did not take formal action in seeking help and support from professional services, such as the police, support services or legal advice.

This is incredibly concerning given the negative consequences reported by victims of cyber abuse and sexual harassment, including severe impacts on their physical and mental health. Our 2017 *Image-based abuse: National survey - summary* report shows that the impact of image-based abuse amongst online adults was overwhelming negative. Women were considerably more likely to report negative personal impacts as a result of image-based abuse, including in terms of their emotional response, fear of discovery and impact on life.

Overall, two-thirds of online adults who experienced image-based abuse indicated they had felt annoyed (65%) or angry (64%) with the person who had perpetrated the abuse, while many also felt humiliated (55%) and depressed (40%). Thirty-two percent had felt afraid for their safety. Online adults most feared the discovery of the photos/videos by their friends (51%) and family (48%), although many also feared discovery by an employer (41%), intimate partner (40%) and children (39%).

The most common negative impacts of the most recent experience of image-based abuse related to self-esteem (42%) and mental health (41%). One-third said it had impacted their physical wellbeing (33%) and relationships with friends (33%), while just over one-quarter said it had impacted their intimate/sexual relationships (28%), relationships with family (27%) and performance at work or study (28%).

We must do better to both prevent these harms occurring in the first place and provide support when they do.

Key insights and priorities

As discussed above, the Office adopts a whole of community and multifaceted regulatory approach. This begins with community awareness and education, early intervention and content take down services and extends to regulation and technological interventions. It is ultimately how these levers work in conjunction, rather than in isolation, that we can create real and meaningful change.

We have drawn upon our experience formally operating cyberbullying and image-based abuse schemes, and informally managing adult cyber abuse reports, to identify the following insights and priorities, which we hope can serve as a useful frame of reference for the Inquiry.

Workplace practices, policies, procedures and training

Employers must take a zero-tolerance approach to both cyber abuse and online sexual harassment.

Concerningly, the findings from the 2018 Sexual Harassment Survey show that in almost half of the cases where a formal complaint was made, the victim reported that nothing changed at their organisation as a result of their complaint.

As part of their duty of care to employees, employers must have practices, policies and procedures to prevent, manage and address sexual harassment. It is imperative that these specifically address online safety.

It is important for employers to understand the nuanced and complicated ways cyber abuse and online sexual harassment occur and, just as importantly, the profound and layered consequences such abuse can have.

It is also critical for employers to understand the myriad ways cyber abuse can manifest. There are overt ways of perpetuating abuse and harassment online, such as sharing images, and covert ways, such as promoting shame or by exclusion. An employee may experience cyber abuse from a colleague, manager or customer, or from individuals in their personal life.

Therefore, employers should not rely on the policies of the social media or technological services they use. Rather, they should proactively develop company specific policies, which are tailored to the online work practices and procedures of their business.

Practices, policies and procedures must also account for the fluid overlap of online and offline exchanges and professional and private lives. As discussed above, we know through research with workers who support women experiencing domestic or family violence that 98% of cases involve some form of online abuse, surveillance or stalking. Equally, we know that there is a strong connection between cyberbullying and conflict within the school setting and that the nexus of conflict often sits within the school community.

Practices, policies and procedures focused only on online interactions, or only on interactions strictly within work hours, are not consistent with modern workplace practices. They also risk dealing with only a fraction of the issue. Existing practices, policies and procedures in place to prevent, manage and address sexual harassment must be extended to the online environment and take account of the complex factors outlined above.

Policies, practices and procedures must also be supported by training. This could include social media self-defence training, which addresses cyber abuse and online sexual harassment. It could also include unconscious bias training and how these biases may translate into online commentary. However, unconscious bias training needs to be carefully considered and designed in order to be useful both within and beyond the workplace walls. Unconscious bias training can reinforce stigma and stereotypes if it raises awareness of biases without seeking to challenge them. Equally concerning is training that doesn’t encourage people to critically examine their own behaviour or falsely convinces people to believe they have ‘done their bit’.

This reinforces how important it is that a cultural commitment, both leadership and peer to peer, underpins and drives workplace policies, practices and procedures. Cultural change will occur if leaders and managers live the values on a daily basis and commit to wholly inculcating them into the organisational fabric.

Leaders also need to demonstrate the value and importance they place on online safety. Colleagues need to be reminded to visibly demonstrate support for other’s online, just as they are expected to communicate with respect interpersonally. Together, this will help create a society not simply of bystanders, but upstanders.

We would also encourage employers to take a holistic approach to their policies and training. They should not simply focus on reducing harm, but also on capacity building, especially building resilience and online competence.

For example, with WITS, we've already held events with industry leaders and managers, government officials, athletes and female journalists. They were equipped with resilience tips and online safety information to not only empower them to take action and strengthen their voices online, but also spread the online safety message. The 'upstander' message is at the core of WITS, in that it reiterates that women can together express solidarity and build strength by supporting each other online. Tips for how people can build their psychological armour online, as well as strategies to respond to online abuse, are also available on the WITS website (www.esafety.gov.au/women-influencing-tech-spaces).

Lastly, we want to caution employers about the potential shortfalls of policies that may protect the reputation of the organisation, while failing to protect the wellbeing of their employees stemming from their online engagement. Too often policies are focused on protecting the reputational brand of the company, rather than protecting and promoting the wellbeing of employees online. In particularly egregious instances of sexual harassment, internal processes have protected the perpetrator and company and blamed the victim. We must avoid victim blaming responses.

It is therefore imperative that breaches of company policy are reported and published transparently, while accounting for issues of confidentiality and privacy. This is critical for engendering trust and faith in internal processes. For similar reasons, it is also important that any monitoring of employees' devices is reasonable, proportionate and clearly communicated to employees.

This links to the broader point that workplace practices, policies, procedures and training should be open, transparent and accountable.

Encouraging help seeking behaviours

As discussed above, both cyber abuse and sexual harassment are notoriously underreported. From our research with female victims of image-based abuse, the most common barriers that prevented victims from reporting the abuse or seeking support were the negative stigma associated with image-based abuse, being unclear about where to go for help and fear of exacerbating the situation. Other barriers included psychological and emotional barriers, not recognising that it was an offence and concerns about mandatory reporting.

An intersectional lens is again important in understanding help seeking patterns and behaviours. We know from our research that Aboriginal and Torres Strait Islander people are twice as likely to have experienced image-based abuse in comparison with Australians who are not Aboriginal or Torres Strait Islander. However, Aboriginal and Torres Strait Islander people are less likely to use traditional reporting services due to a complex mix of culturally-specific and historical factors.

Our 2019 research into CALD women who have experienced technology-facilitated abuse highlight a number of the key barriers for reporting technology-facilitated abuse. These include a lack of awareness that technology-facilitated abuse may constitute a criminal offence, low level of literacy and low understanding of the judicial system, cultural biases and misunderstandings from some support services, and cultural and gender specific shaming.

The fear of stigma, for people of all sexes and ages, is a common barrier that prevents people reporting cyber abuse and sexual harassment.

Reporting cyberbullying, image-based abuse and other forms of cyber abuse to the Office is one of our most important safety recommendations. We know from feedback we receive about our complaints services that reporting can both provide a sense of relief and be empowering for the individual, as it restores them a sense of control. Having harmful content taken down, whether it be verbal online abuse or image-based abuse, helps de-escalate the trauma and humiliation a victim may feel as long as that material is online for everyone to see.

Reporting also puts the platforms on notice about the nature, volume and trends of abuse on their platforms. Over time, this should help improve the challenges posed by online abuse at an institutional and platform level.

We need to do more to promote help seeking behaviour. This includes exploring strategies to help victims overcome their reluctance to report. For example, enabling people to report incidents anonymously reduces the emotional strain on victims and allows them to further preserve their agency. In situations where there is little or no evidence, including to verify the abuse and who is responsible, the focus could be on facilitating an informal investigative process that allows the allegations to be raised and considered, while ensuring a fair and transparent process.

It also includes encouraging an upstander culture where abuse is not tolerated and where victims are encouraged and supported to speak out, without negative repercussions.

Raising awareness about reporting and support services

We must also raise awareness of the reporting services and support pathways that are currently available. Australia is the only country in the world with a regulatory agency solely dedicated to protecting the online safety of its citizens, including services to report cyberbullying and image-based abuse for removal from online platforms.

We know from our 2017 *Image-based abuse: National survey - summary* research that general awareness of information, help or support for image-based abuse is low among online adults, with only one-fifth (22%) knowing where to seek information, help or support.

Our 2019 research with CALD women also shows the impact of low digital literacy and language barriers. Language barriers contribute to CALD women not knowing what services are available to them and create challenges for them explaining their personal experiences with technology-facilitated abuse.

However, we also know from our work getting cyberbullying and image-based material removed that government intervention is important. Ultimately, the Office serves as a safety net when reports fall through the cracks. We also serve as an important advocate on behalf of the user, as there is often an inherent power imbalance between the person being abused and the social media service. Not only have we built relationships with the online platforms to cooperatively encourage the rapid removal of online content, we also have significant civil regulatory powers to compel take down and fine the content hosts if they are not compliant.

We need to raise awareness about the unique services of the Office of the eSafety Commissioner and the Australian Human Rights Commission so that we can provide more people with support and assistance.

We also need to promote and support Australia’s exceptional mental health and counselling services. Many of these organisations can be found on our eSafety & Mental Health WellBeing Directory (https://www.esafety.gov.au/wellbeing-directory).

Modern and inclusive practices

We must also ensure our reporting and support services are tailored to modern practices and account for diversity, inclusion and equity.

For example, young Australians use online and mobile technologies as a way to reach out and seek assistance. For some groups, including those that have historically found it difficult to engage with traditional help-seeking models and supports, such as people with a disability, those living in remote locations, CALD communities and LGBTIQ people, the impact of having access to real-time, easy-to-access support services that they are comfortable using cannot be overstated. This is reflected in support services offering online chat and email-based counselling, in addition to traditional telephone-based services, specifically to cater to the needs of a growing youth market. It also points to the need to ensure the localisation of materials and counsellors in multiple languages.

We need to review our traditional complaints mechanisms to ensure they remain accessible, relevant and useful for the people they are intended to serve.

Quick relief for victims

The complaints process under the *Sex Discrimination Act 1984* is based on conciliation. Notwithstanding the benefits of conciliation processes, we understand that in some instances, this has proved time-consuming and emotionally exhausting for complainants. With any complaints process, we must be careful not to retraumatise victims.

At the Office, we get our cyberbullying and image-based abuse material removed rapidly, often within hours. This provides an immediate sense of relief, serving as a ‘circuit breaker’ while we determine longer term steps and strategies, such as referral to support services.

From our experience, the prompt removal of material provides victims immense relief and de-escalates traumatisation. In any case of online sexual harassment, the immediate priority must therefore be to get the material taken down. This will provide the complainant an immediate sense of relief, while the conciliation process is undertaken and longer-term steps and strategies are identified. It should be noted that criminal penalties and litigation, while important and necessary in some circumstances, can often be lengthy and costly, both financially and emotionally, for the victim.

Safety by Design

Educating and empowering people will always form the basis for addressing the social and behavioural issues that manifest online. However, it is imperative that we also consider the technological approaches, interventions and frameworks we can employ to reduce cyber abuse and online sexual harassment.

The Office is currently undertaking a consultation process on Safety by Design. By embedding user safety into the design and functionality of products and services, we ultimately want safety to become the new design imperative for platforms that stimulate communication and interaction. This will help ensure that safety abuses can be prevented at the outset, rather than addressed retrospectively and after the damage has been done.

The reality is that the same technology platforms that can be used to spread positivity and ideas can be used for more nefarious purposes, including harassment and hate speech. Companies providing these services need to improve their efforts in not only surfacing and detecting this kind of content, but in ensuring they have the required policies, processes and commensurate enforcement to rid their platforms of malfeasance before the abuse is perpetrated.

The Office has developed a draft set of high-level Safety by Design principles. They set out the parameters required by industry to preserve the rights and dignity of users online, whilst protecting them from abuse and exploitation. We hope they will act as a model template and benchmark, for industries of all sizes and stages of maturity, to incorporate and assess user safety considerations throughout the design, development and deployment lifecycle of their products or services.

This underscores that preventative steps can be taken to ensure that online environments are less likely to facilitate, enflame or encourage illegal and harmful behaviours. Ultimately, the Safety by Design principles seek to secure a more ethical, value-centred and human-centred approach to the development of technologies.

Nationally coordinated and consistent Curriculum

The findings of the 2018 Sexual Harassment Survey show that two in five (39%) people aged between 18 and 29 had experienced sexual harassment online or via some form of technology.

Young people between the ages of 18 and 29 were also the most likely to be sexually harassed at work. Further, 1 in 5 young people aged between 15 and 17 had been sexually harassed at work.

These findings correlate with the Office’s research. Our 2016 *Research Insights: Teens, Kids and digital dangers* report showed that 1 in 5 young Australians have experienced cyberbullying.

The students of today are the workforce of tomorrow. A child’s educational journey therefore presents a critical opportunity to address the root causes underpinning online harassment and abuse, while equipping students with skills and understanding in digital literacy, digital citizenship and digital ethics.

We need a comprehensive and nationally coordinated respectful relationships and online safety education embedded in the Australian Curriculum and consistently delivered throughout a child's educational journey. This should be based on the 'Four Rs of Online Safety' - respect, resilience, responsibility and reasoning.

The Office has a wealth of educational resources for schools, parents, carers and communities. We ensure a strong evidence base underpins our education outputs. As a result, we know that successful education interventions tend to include:

- multiple exposures to online safety, using varied platforms, such as videos, games, posters, class discussions and parent and carer engagement
- a focus on specific skills, along with opportunities to practice those skills
- early education prior to the onset of targeted behaviour, as guided by well-trained educators, and
- monitored implementation and improvement of programs through evaluation.

The Royal Commission into Institutional Responses to Child Sexual Abuse affirmed the important role the Office has in educating parents, carers, communities and students, as well as helping schools to manage online risks. In response to the Royal Commission recommendations, we are working closely with the Department of Education to develop an online safety plan that will include a suite of resources to support the online safety efforts of schools.

A child's educational journey, which should begin before they start school and be supported by their parents, carers and wider community, is therefore one of the best mechanisms for empowering children to interact online safely and respectfully.

Social media disclosures

Finally, we acknowledge that there has been a growing trend, especially among women, to use social media to raise sexual harassment allegations.

In many ways, social media has become a platform for disclosure because of the failure of existing systems and processes to protect and support women.

Too frequently perpetrators were protected and the impact of their actions minimised. Too frequently women who used traditional reporting and redress mechanisms were disbelieved, undermined or penalised.

It is important that people who have experienced cyber abuse or sexual harassment have agency over their story and recovery.

However, we also acknowledge the challenges of this approach. It is equally important that the principles of due process and natural justice are upheld for all parties.

We believe it is by improving the complaints processes for sexual harassment that we can restore faith in the institutional systems and processes of justice. This, coupled with driving the social and behavioural change that reinforces that cyber abuse and sexual harassment are never okay, will create the holistic social and legal framework that encourages and supports people to use institutional systems and processes.

Conclusion

The eSafety Commissioner and Office commend the work of the Sex Discrimination Commissioner and her team in driving this important body of work.

As the world’s first and only government agency dedicated solely to online safety, we know that online issues are only becoming more complex and pervasive. It is inevitable that they will arise in the workplace. Employers are therefore an integral component of a whole of community and multifaceted approach to countering online harms, including online sexual harassment.

We believe it is though improvements and reform to workplace policies, complaints processes, regulatory responses and education that we can create the social and behavioural change to address cyber abuse and online sexual harassment and therefore enable Australians to embrace the vast potential of social media and technology.