ONLINE SAFETY ON THE EDGE

CONFERENCE REPORT

'Online Safety on the Edge' is the first conference co-hosted by the Office of the eSafety Commissioner, Australia, and Netsafe, New Zealand. Held 1 - 3 November 2017 in Sydney, the conference brought together 81 speakers and over 380 delegates from around Australia and across the globe, sharing their experiences, learning from one another, and exploring the latest online safety trends and successful interventions.

Conference presentations and workshops identified common and salient online safety concerns, drawing out five key challenges and future directions which pave the way for improving online safety and digital resilience. These are outlined, below.
Building on the success of this inaugural conference, a second conference will be held in Auckland, New Zealand on 8 - 9 November 2018.

KEY ISSUES

1. Image-based abuse: from victim-blaming to a shared responsibility

Image-based abuse is a current and significant issue across the globe—a point made clear in a number of sessions throughout the conference.
The panel: Image-based abuse: Global efforts to prevent and protect highlighted that many people hold outdated attitudes that blame victims of image-based abuse. Sixty-seven percent of Australians who are online agree that 'people should know better than to take nude selfies in the first place, even if they never send them to anyone', while 57% agree that 'a person who sends a nude or sexual photo/video to someone else is at least partly responsible if it ends up online'.[1] These results show that although most people recognise the considerable harm caused by image-based abuse, social stigma persists.

Interestingly, during the panel Where is the love? International research on sexting, cross-country research from the UK, NZ and Australia showed both differences and similarities among teenagers around sexting. While 9 in 10 Australian teens aged 14 - 17 agreed that spreading nude images or videos of someone without their consent was illegal and people shouldn't do it, 28% agreed that it was someone's own fault if their images were shared without consent, rising to 38% for the younger cohort of 14 year olds.

Overall, these conference sessions observed that without proactive, pre-emptive intervention, image-based abuse becomes a problem for victims to manage and navigate. There is a need to move from a culture that condones victim blaming to a culture in which everyone—bystanders, victims, policy makers working within social media services, frontline workers in anti-bullying NGOs, legislators, police, social workers, educators or parents—is empowered to confront image-based abuse as a shared responsibility.

2. The fiction of anonymity

Anonymity continues to be a very real online safety challenge acknowledged by agencies across the globe. Anonymous apps and online environments are often seen as the fuel for online hate, cyberbullying and abuse, as they allow perpetrators to hide behind a cloak of anonymity. But an examination of this issue reveals a more complex picture—as discussed by Justin Patchin in the panel Being online—What's the harm?

During the session, Patchin noted that though apps including After School, Yik Yak and Brighten are marketed as anonymous, in reality, they are not. Regardless of whether a particular 'anonymous' app requires an authentication process to sign up, posts can still be traced by internet service providers using IP addresses. Within the broader context of anonymous apps, as Patchin made clear, 'anonymity is really confidentiality': it is tied to terms of service in which companies agree to keep their users' identities private. But when it comes down to it, the cloak of anonymity can easily be stripped away.

At the conference, Patchin also outlined some benefits to anonymity. Anonymous apps, for example, can foster exploration, enabling teenagers to try out new facets of their identity or political beliefs without risking damage to their reputation or self-esteem. So while anonymous online environments play a role in perpetuating online abuse, anonymity can also be used to boost digital resilience and self-esteem by creating environments in which teenagers feel free to express themselves.

3. Respect matters: reconfiguring relationships and consent online and offline

A third challenge highlighted at the conference—one which was discussed at length on several panels—is the effect of pornography on children and the need for respectful relationships education.
The increased exposure of children, teenagers and young adults to pornography, whether deliberate or accidental, can have a significant impact on them. Viewing pornography is now one of the main ways children and young adults learn about sex and relationships and it has been noted that exposure to pornography at a young age has implications for how teenagers and young adults conceive of respectful relationships, gender-based violence and consent.
Conference presenters and attendees observed that part of the solution lies in talking to kids about pornography, instead of just talking about kids engaging in practices. As Maree Crabbe put it during the Tuning into Teens panel 'We need to find ways to talk to kids about porn… as it is shaping their conceptions of pleasure, power and consent'. Crabbe, Co-Founder and Coordinator of Reality & Risk: Pornography, Young People and Sexuality, calls for parents and educators to be 'genuinely curious' and to find ways to start candid, non-judgemental conversations about pornography, so that we can 'inspire young people to realise that relationships and sex can be so much better than what they see in porn'. Helping children and young people navigate the difficult terrain of pornography can be confronting, but it is crucial in fostering online, and offline, respect and digital resilience.

4. Creating a less hostile environment for women online

The hostility that women face online was a prominent topic of discussion during the conference, particularly in sessions: eSafetyWomen – combatting gendered abuse online and Life in the online fishbowl. Online environments are disproportionately hostile towards women, and it is well documented that female journalists and public figures receive an excessive amount of hate speech and online trolling.

As Jane Caro, Social Commentator, Writer and Lecturer, made clear at the conference: 'With women—the abuse is always gendered and it's so often about their appearance'.[2] Journalist, Ginger Gorman, and disability advocate, Carly Findlay, painted vivid pictures of their own experiences as the targets of vicious online abuse which had spilled into their lives offline, and provided insights on dealing with online trolls.

The harassment, abuse, and intimidation that women and minority groups endure online has its roots in wider societal contexts of power and control, often connected to physical harassment and violence. Recent research by SmartSafe in Australia showed that 98% of frontline domestic violence caseworkers had clients who had experienced some kind of technology-facilitated abuse.[3]

Helen Campbell, Executive Officer of the NSW Women's Legal Service, noted that technology can add new dimensions to domestic violence because 'there is no escape as it isn't geographically based' and 'images can travel fast and have permanency'. One of the reasons why online abuse is so insidious is that our digital footprints often reveal a great deal of personal information, including bank details or home addresses, and perpetrators can manipulate and expose this information to exact real-life consequences for their targets. Cumulatively, analysis of the gendered nature of online abuse shows that the challenge clearly remains: to foster online environments in which a diversity of voices is heard and valued.

5. The limits of the law

While new legal and policy responses are being established in response to the issues posed by online environments, a challenge identified at the conference is the limitations of these.

In conference sessions, David Harvey, Director of the New Zealand Centre for ICT Law at the University of Auckland, discussed the scope of the Harmful Digital Communications Act in New Zealand while Will Gardner, CEO of Childnet International, surveyed the UK's response—which includes the introduction of age verification mechanisms along with a requirement on ISPs to make filters available to consumers. Both observed that the transnational nature of online content, along with the sheer volume of illegal or potentially harmful content, poses big challenges in shaping effective policy and legal responses.

Key points raised throughout the conference included that for targets of online abuse, the response from law enforcement, courts and social media services can be frustrating and disempowering. Often police can't investigate without a specifically worded threat, and many law enforcement officers lack the technical knowledge required to protect personal accounts or data. In addition, the complexity of existing law means police may not be aware of specific civil and criminal penalties that apply to online abuse.

Twitter, Facebook and other social media services do offer users the option to report, block or mute offenders, and in some cases users can be banned or suspended. However, responses from law enforcement and social media services almost always focus on the abuser, placing the burden to manage abuse, even while it is ongoing, firmly on the shoulders of the target. Automated tools for moderating hate speech have a role to play in lessening the burden on victims, but there is no technological panacea.

In the fight against child exploitation material, 'disruption is the name of the game and victim identification', argued Darren Kane, Chief Security Officer, NBN Co. Cross-border collaborations between law enforcement and the tech industry have seen the development of collaborative tools and databases that track and log child exploitation material, increasing the effectiveness of victim identification. However, the generational shift in the use of technology by younger children, with kids as young as three using smartphones, and the rise of live streaming, intensifies the growing problem of self-generated child sexual abuse material. As Detective Inspector Jon Rouse from Task Force Argos, Queensland Police asserted, 'I don't know if it can get any worse or the victims can get any younger'. [4]

FUTURE DIRECTIONS

Through broad discussion, collaboration and consideration, conference presenters and attendees identified five future directions in online safety which can help to improve online safety and digital resilience across the territories. These are:

1. The value of genuine consultation and partnership

Over the last decade, partnerships between industry, law enforcement, governments, NGOs, researchers, educators and young people have been at the heart of online safety initiatives. Antigone Davis, Head of Global Safety at Facebook, made clear that partnerships are needed to ensure online safety, 'We are experts in building sharing platforms, but we are not experts in online bullying and suicide prevention'.

Partnerships acknowledge that groups adversely affected by online abuse are often best placed to influence each other. As Tessy Ojo, Chief Executive of the Diana Award, observed, 'Young people are the best agents for change in their schools, communities and online, because they are best placed to understand the challenges and opportunities presented to them, to influence each other and their energy and enthusiasm can feed broad and deep participation'.

Further supporting this concept, Donna Cross, Professor at the Telethon Kids Institute, University of Western Australia, argued that 'Children are the agents of change, rather than being vehicles by which we achieve change... We need young people as co-designers and co-researchers, they need to be co-implementers.'

However, throughout the conference it was acknowledged that an element of tokenism has crept into some partnerships, and is cause for concern. Going forward, it is not enough to simply name-check key groups, offering them a near complete initiative or policy to green light. It's important to pay tribute to partnerships that understand and value the diverse strengths and insights that different people and organisations bring to the table, and are not afraid to continually seek criticism and feedback from the communities they are designed to serve. Initiatives such as Project Rockit, Australia's youth-driven network against (cyber)bullying, founded by Lucy and Rosie Thomas, were seen as a model of collaboration, with a 'brains trust' of teenagers and young adults empowered to shape and implement their online and face-to-face workshops.

2. The benefits and limits of artificial intelligence (AI)

AI was identified in sessions throughout the conference as an important future direction in online safety, and is currently used across industries, in a variety of ways.

There are many positives. Protective tools and technologies, such as automated moderation systems built into social media platforms, and algorithms designed to remove hate speech and pirated content from search results, have achieved a level of success in combating online abuse and illegal content. PhotoDNA, which has been used successfully in helping prevent sharing of child sexual abuse content, is also being introduced as tool in combatting image-based abuse.

However, creating a comprehensive technological solution to the problem of online abuse is extremely difficult—in part because of the complexity of understanding sentiment and context. As Mia Garlick, Facebook's Director of Policy Australia and New Zealand, made clear, 'Constant retraining and effort to understand context is essential'. Likewise, Sam Yorke, Policy Council, Public Policy and Government at Google, stated, 'We are good at technology, but we need help understanding the local context'.[5] Moderation systems that combine human moderators and machine learning or AI are more accurate, such as those employed by Facebook and Twitter,

yet no moderation system can be completely failsafe. Both automated systems and teams of human moderators need to understand local context. As eSafety Commissioner, Julie Inman Grant, argued, 'We need tools that are culturally palatable and locally appropriate'.

Garlick cited an example that illustrates the difficulties faced by hybrid human and machine moderation systems: a series of Facebook posts in which women were told they 'should go get on a bus', which were reported by users. This seemingly innocuous phrase was actually a veiled rape threat. It referenced the media coverage of the rape and fatal assault of a young women who was travelling on a private bus in South Delhi in late 2012. Without knowledge of the local context, there is a high potential that rape threats and other hate speech will go undetected.

Online moderators need to be representative of diverse groups—including people of different races, genders, sexualities, abilities and localities—and better educated to understand the complexities of different localised contexts.

3. Bridging the empathy gap: it's not about technology, it's about how to be social

Online safety education is often couched in technological terms, but conference attendees acknowledged that it is time to look forward—for it to be reconfigured as an intensely social issue.

As Kara Hinesley, Head of Public Policy and Government, Australia and New Zealand, Twitter, stated, 'These are symptoms of deeper behavioural problems we are seeing. Does it make sense to treat online behaviour differently to offline behaviour? These are, at root, behavioural problems we are trying to solve'.

During the conference it was frequently noted that it is easy to lose sight of the fact that online behaviour is a continuation of offline behaviour. Although young people often possess great technical skills, they cannot be expected to be experts in socially responsible behaviour without guidance. This perspective is neatly summed up by one of the 'brains trust' of young people guiding Project Rockit's anti-bully workshops: 'We are the tech experts, help us with the social stuff'. For Project Rockit, real social change occurs at the intersection of education and empathy.

Another highlighted aspect of the problem is that online safety education is often only included in technology-based subjects in schools, when it is included at all. Lesley Podesta, CEO of the Alannah and Madeline Foundation argued 'There is this misconception that online safety is technology teaching—it is not—it's social and critical thinking'. For many on the frontline, it is the development of social and critical thinking skills that can help to foster a safer online environment for all.

4. An intergenerational approach to online safety

Integrating the skillsets of different generations is key to building the community capacity needed to meet the challenges of online safety—now and in the long term.

eSafety Commissioner, Julie Inman Grant, explained that 'the 'sandwich generation' are key to unlocking the potential of online safety education: 'On the bottom, we have the younger generation who have excellent online skills but lack social and judgement skills, and on the top, we have older generations, who have better judgement but lack technological skills. The sandwich generation needs to look after both'.

Bridging generational gaps in online safety means rejecting labels and jargon and speaking to different groups in the language and terminology they use themselves. As Rosie Thomas, Co-founder/CEO of Project Rockit, pointed out, empathising with teenagers and young adults means 'speaking with them in their own language'. In

effect, this means avoiding terms like ‘sexting’ and ‘cyberbullying’ and talking about the behaviours that underlie these practices. Any message that is prescriptive or comes from ‘on high’—for example ‘never send intimate pictures of yourself’ or ‘don’t talk to strangers online’—may not connect with younger audiences. Instead, it is more constructive to foster critical judgement about online behaviour.

Conversely, using technological jargon or making assumptions about the technological competency of older audiences may alienate them, whether or not this underestimates or overestimates their technical capacity. Nan Bosler OAM, President of the Australian Seniors Computer Club Association said, ‘To older Australians, you have to add life to years, so be connected’.

5. It takes a village: fostering digital resilience

Few people would dispute the notion that online safety is a shared responsibility, but where do the roles of corporates, governments, NGOs, law enforcement, mental health professionals, educators and parents intersect? There is no easy answer to this, but the conference highlighted that all partners in online safety must continue to work together to define their respective roles and spheres of expertise.

The authors of a report from EU Kids Online How to cope and build online resilience, see resilience as the ability to deal with negative experiences both online and offline. Its authors argue that, ‘Resilient children are able to tackle adverse situations in a problem-focused way, and to transfer negative emotions into positive (or neutral) feelings’.[6] Amanda Third, Associate Professor, Institute for Culture and Society at Western Sydney University, argued that we need to become more comfortable with the idea of exposing children to online risks, as it is only through learning how to cope with adverse experiences that they will develop digital resilience: ‘We need to give parents a break. We have told parents for a decade that they should be scared of the digital. It is paralysing. While we are afraid, all we can do is throw our hands up in the air, or try to control and restrict what children do online’. Instead, it is better to promote a positive attitude to risk—one that breaks down the boundaries between harms and benefits, dangers and opportunities.

Executive Director at DQ Institute, Marsali Hancock, likens the challenges of online safety to those of the public health campaigns of the past: ‘We all know about germs and microbes and how to protect ourselves from them, but we don’t understand about how to be safe online’. Behavioural change is a slow process, but for online safety to be successful we need to break down issues into resolvable parts, and work across disciplines to come up with solutions. In practice, this means bringing parents and teachers into the circle of online safety education, by promoting internet access and the development of online skills, so they are better equipped to guide their children or students in online activities. Monitoring and talking with children about what they do online from a very young age, rather than restricting their access, is a better approach, as it allows them to make mistakes and learn from these experiences. Promoting a positive attitude to online safety is not a simple task. It takes a village to build digital resilience.

WORKING TOGETHER: WAY FORWARD

The challenge of growing safe and resilient online communities will never be a simple one. As is the case with all the complex community challenges, new issues will continue to emerge, and we must work diligently and cooperatively to propose, test and adapt solutions – while not being afraid to abandon those that are no longer fit-for-purpose.

The Office of the eSafety Commissioner proposes to:

- Lead by fostering a community of online safety practitioners in which parties deliver according to their expertise and their strengths.
- Grow a broader range of partnerships, reflecting our understanding that issues that occur online have their origin in a complex offline world, and nuanced solutions are required.
- Promote 'safety by design' across all sectors with a stake in online safety: from best practice technological solutions to robust, strengths based education and prevention programs that emphasise respect, resilience and responsibility.
- **B**uild stronger networks with those who are the target of our programs, ensuring we deliver on the challenge of 'nothing about them without them.'
- Develop specific, targeted resources to key audiences who are experiencing online hate, helping people to take back control.

The Office welcomes the opportunity to report on its learnings alongside Netsafe in November 2018.

[1] esafety.gov.au/image-based-abuse/about/research

[2]

[3] smartsafe.org.au/technology-facilitated-abuse-new-breed-domestic-violence

[4]

[5]

[6] 'How to cope and build online resilience? eprints.lse.ac.uk/48115/