Online risks, cybersafety campaigns and young people

A briefing paper for the Technology and Wellbeing Roundtable

Authors: Amanda Third and Sherene Idriss
with Philippa Collin, Rosalyn Black and Lucas Walsh

September 2013

Introduction

In recent years, the Australian government, corporations and youth-serving organisations have made substantial investments in mainstream traditional and social media campaigns targeting the online risks facing young people, with the result that there is a plethora of information available to young people about the risks and potentially harmful consequences of engaging online.

With online safety community awareness strategies and media campaigns reportedly reaching saturation point in Australia, it is crucial that the sector now evaluate the long-term impacts of this awarenesss-raising. To date, there is limited reliable data relating to the impact of about online safety, particularly as relates to their ability to produce long-term behaviour change.[1] 'Recent research clearly shows that teaching children about the risks of Internet use and/or 'key tips' for keeping safe has little impact on their behaviours (Mishna, et al, 2009; Campbell, 2009). Participation in educational Internet safety interventions is frequently shown to be associated with an increase in awareness

Some recent campaigns…

Cybersmart, the government initiative launched in 2008, is "designed to support and encourage participation in the digital economy by providing information and education which empowers children to be safe online" (Cybersmart website). Cybersmart have produced educational films such as 'Tagged', advertisements such as 'Cyberslap' where the tagline is – 'you don't need a black eye to be bullied', as well as educational resources freely available on their website.

To deal with the growing problem of cyberbullying, 'BackMeUp', an Australian Human Rights Commission initiative, was launched in August 2013 (Australian Human Rights Commission website) calling on local celebrities to educate students about cyberbullying and the ways that young people can make changes to stop these kinds of behaviours in their friendship circles.

[1] The Australian Communications and Media Authority (ACMA) regularly evaluates their online safety initiatives. One further exception is the work by Albury and Crawford (2012) who analyse the messages in the *Megan's Story* media campaign that highlights the negative consequences of sending sexual text messages.

and knowledge in children but not with reducing risky online behaviours (Mishna, et al, 2009).[2] Given this, online safety strategies targeting young people must reach beyond awareness raising and aim for **long-term behaviour change**.

To foster sector-wide conversation about these issues, this briefing paper summarises key research insights about the following:

1. The complex relationship between young people's online safety and their experiences of risk.
2. The principles underpinning effective traditional media and social media campaigns
3. The intergenerational gap between adults and young people's perceptions of online safety
4. What we know about how young people think about online safety

This briefing paper also identifies a series of key questions for the Roundtable to consider in its deliberations on this issue.

The complex relationship between risks, harm and online safety

The relationship between risks, harm and online safety is complex. Research from the AU Kids Online project suggests that taking calculated risks when interacting online is key to young people's capacity to develop digital literacy skills that enable them to maximise their online safety.[3]

Emerging evidence overwhelmingly suggests that **exposure to risks does not necessarily equate with harm**.[4] Young people's online practices are rooted in their everyday lives and peer relations, providing a lens through which they navigate potential risks. This sometimes means that young people do not conceptualise risks in the same ways that the adults in their lives do. We discuss this in more detail below.

Further, **not all young people are at equal risk online**. Young people who take risks offline are more likely to engage in risky online behavior, a fact that many online safety campaigns to date have not necessarily been well-equipped to address.

There are proven benefits to engaging online.[5] To **maximise the benefits of connectivity** it is important for young people to not only understand the risks of engaging online, but to also develop the necessary skills and strategies to deal with them effectively. Ideally, and in line with the principle of enhancing broad-based **digital resilience**, strategies should aim to nurture young people's digital literacy and emotional resources so that they can **seek assistance, solve problems, and recover from any adverse online experiences**.[6]

[2] Suzanne Barr, *SuperClubsPLUS: Its role in cybersafety education and learning in young students*, 2010.
[3] AU Kids Online
[4] Suzanne Barr, *SuperClubsPLUS: Its role in cybersafety education and learning in young students*, 2010.
[5] See for example, Philippa Collin, Kitty Rahilly, Ingrid Richardson and Amanda Third, *The Benefits of Social Networking Services: A Literature Review*, Report prepared for Inspire Foundation. December, 2010. ISBN: 978-0-9871179-1-5
[6] Resilience is the capacity of individuals and communities to adapt to and gain strength from adverse experiences across online and offline settings. Digital resilience develops over time and with exposure to a diversity of experiences online.

Strategies should also promote an attitude of 'continuous learning' that prepares young people to adapt new safety practices as new platforms and their attendant risks emerge.

Discussion point: Given the complex relationship between online risks and safety, and given the need to promote digital resilience, what sorts of behavior change should online safety campaigns aim to achieve?

Some research insights about what does and doesn't work in the online safety space

> *'Programs are more likely to have an impact if they are delivered developmentally, over long time frames (i.e. months, even years), and in authentic child focused ICT environments'.*
>
> - Suzanne Barr[7]

> *'To be most effective, cyber safety education needs to occur in spaces with which young people want to engage, and give them opportunities to explore and experiment with different strategies, make mistakes, get immediate feedback and self-correct.'*
>
> - Amanda Third, Pota Forrest-Lawrence, and Anne Collier

Participatory Design Guide

The Young and Well CRC has developed a participatory design guide to support researchers, policy-makers and the youth, health and community sectors to involve young people in the development of online services and activities designed to improve young people's mental health (Hagen, P., Collin, P., Metcalf, A., Nicholas, M., Rahilly, K., Swainston, N., 2012. *Participatory Design of Evidence-based Online Youth Mental Health Promotion, Intervention and Treatment.* Young and Well Cooperative Research Centre).

See: http://youngandwellcrc.org.au/knowledge-hub/publications

Young people generally view themselves as experts in the digital world. One consistent critique of existing online safety campaigns is that they do not always resonate with youg people's lived experiences. For example, Brown and Gregg have found that online safety campaigns tend to problematise, and soemtimes criminalise, a range of young people's common online practices rather than contextualizing those practices within young people's broader online and offline cultures.[8]

Recent research indicates that online safety programs, policies and products are most effective when they are built upon processes of **user engagement** and **participatory research and design**. User-centred approaches to online safety engage target audiences in:

- identifying, defining and prioritising online 'risks';
- generating the necessary evidence about users' interactions;
- developing programs, policies and products that embed users' insights and experiences.

[7] Suzanne Barr, *SuperClubsPLUS: Its role in cybersafety education and learning in young students*, 2010.
[8] Brown and Gregg, 2012

This ensures that cyber safety strategies connect into users' existing online and offline practices in a meaningful way, fostering **maximum uptake and impact**. Online safety initiatives should be **regularly evaluated** using the same processes.

Research shows that young Australians do not distinguish between the 'online' and the 'offline' and that their **decision-making frameworks translate across online and offline domains**. Some of the most troublesome online risks are strongly associated with offline risks and these two worlds do not exist independently.[9] To address online risks, it is crucial that offline behaviours are also considered. Wherever possible, cyber safety strategies should seek to leverage the relationship between online and offline to positive effect.

To date, Australian responses to the challenge of cyber safety have been characterised by interventions that are frequently focused on one or a few key issues (eg: privacy, bullying, etiquette), a key population (eg: children, seniors) and/or a setting (eg: schools). **Long-term online safety strategies** are urgently needed. Given the constantly evolving digital media landscape, short-term approaches struggle to adequately prepare users to deal with continuously shifting online safety challenges and proliferating forms of technology. Users need to be encouraged to take on a 'continuous learning' attitude, whereby cyber safety and digital literacy are configured as key pillars of a life-long learning approach to digital participation.

Evidence shows that the best way to promote cyber safety and digital citizenship is to create a **culture change** – across the levels of policy, industry, the community and the individual – that is supported by the ongoing development and provision of information, resources, programs and campaigns that are flexible enough to stay up to date with advances in the digital world. This involves moving from one-off interventions, resources and campaigns to looking at ways to join up learning and behaviour change opportunities. This may require **increased sector coordination and collaboration,** as well as initiatives that address **parents' and professionals' digital literacy.**

Currently, few education campaigns and programs alert young people to the potential **legal consequences** of some of their online interactions.[10]

Discussion point: How can we better embed these principles in the design, delivery and evaluation of online safety campaigns?

[9] Third et al, *Cyber Safety In Perspective*, 2013.

[10] One exception here is the 'Stronger Choices' cyber safety campaign featuring the Tiwi Island band B2M

Some principles of effective mainstream media campaigns

Despite the large number of online safety campaigns operating in the public domain, there is limited rigorous published research about their capacity to promote harm-minimisation and effect long-term behaviour change. This does not mean that campaigns are ineffective in meeting the challenge of online safety but instead points to the need for more research that allows vested organisations to generate conceptualisations of risk that resonate with young people's everyday online practices, and embed these in campaign messaging and harm minimisation strategies. To generate this research, we must engage both young people and the adults who support them in the definition of both risks and solutions. Methodological questions about how to define and measure engagement, outcomes and impacts of online safety campaigns must also be addressed.

The literature on campaigns relating to health and public safety issues provides some insights that might be usefully applied to the challenge of promoting online safety. The following summary excerpts the key insights of a recent comparative analysis of a range of health and public safety campaigns internationally.[11]

Wakefield, Loken and Hornik state that 'the great promise of mass media campaigns lies in their ability to disseminate **well defined behaviourally focused messages** to large audiences repeatedly, over time, in an incidental manner, and at a low cost per head.'[12] However, they also note that there 'campaign messages can fall short and even backfire'.[13]

To ensure the best possible impact and sustain outcomes, campaigns must

- Have clear messages and aims
- Be able to compete in an increasingly fractured and cluttered media environment alongside pervasive marketing for competing products and/or opposing messages
- Leverage the power of social norms
- Use appropriate and well researched formats (eg: avoid boring factual messages or age-inappropriate content)
- Respond to the needs of heterogeneous audiences (homogeneous messages might not be persuasive to heterogeneous audiences)
- Address behaviours that audiences have the resources to change[14]

Importantly, campaigns can use both direct and indirect pathways to achieve behavior change in a broad population.

[11] Melanie A Wakefield, Barbara Loken, Robert C Hornik, 'Use of mass media campaigns to change health behaviour', *The Lancet,* Vol 376, October 9, 2010.
[12] Melanie A Wakefield, Barbara Loken, Robert C Hornik, 'Use of mass media campaigns to change health behaviour', *The Lancet,* Vol 376, October 9, 2010, 1261.
[13] Melanie A Wakefield, Barbara Loken, Robert C Hornik, 'Use of mass media campaigns to change health behaviour', *The Lancet,* Vol 376, October 9, 2010, 1261.
[14] Melanie A Wakefield, Barbara Loken, Robert C Hornik, 'Use of mass media campaigns to change health behaviour', *The Lancet,* Vol 376, October 9, 2010, 1261.

a) **Direct**

Direct pathways aim to:

- invoke cognitive or emotional responses
- affect decision-making processes at the individual level

This can lead to:

- removal or lowering of obstacles to change
- helping people to adopt healthy or recognise unhealthy social norms
- associate valued emotions with achieving change

These changes can strengthen intentions to alter, and increase the likelihood of achieving, new behaviours.

b) **Indirect**

a. Mass media messages can set an agenda for and increase the frequency, depth, or both, of interpersonal discussion about a particular health issue within an individual's social network, which, in combination with individual exposure to messages, might reinforce (or undermine) specific changes in behaviour.

b. Since mass media messages reach large audiences, changes in behaviour that become norms within an individual's social network might influence that person's decisions without them having been directly exposed to or initially persuaded by the campaign.

c. Finally, mass media campaigns can prompt public discussion of health issues and lead to changes in public policy, resulting in constraints on individuals' behaviour and thereby change.

Wakefield, Loken and Hornik conclude that media campaigns can directly and indirectly produce positive changes or prevent negative changes in health-related behaviours across large populations. They make the following recommendations for national governments, practitioners and professional bodies:

- Media campaigns should be included as key components of comprehensive approaches to improving population health behaviours

- Campaign messages should be based on sound research of the target group. Careful planning and testing of campaign content and format with target audiences are crucial

- Sufficient funding must be secured to enable frequent and widespread exposure to campaign messages continuously over time, especially for ongoing behaviours

- Changes in health behaviour might be maximised by complementary policy decisions that support opportunities to change, provide disincentives for not changing, and challenge or restrict competing marketing

- The likelihood of success is substantially increased by the application of multiple interventions and when the target behaviour is one-off or episodic (eg, screening, vaccination, children's aspirin use) rather than habitual or ongoing (eg, food choices, sun exposure, physical activity).

- Concurrent availability of and access to key services and products are crucial to persuade individuals motivated by media messages to act on them.

- The creation of policies that support opportunities to change provides additional motivation for change, whereas policy enforcement can discourage unhealthy or unsafe behaviours.

- Public relations or media advocacy campaigns that shape the treatment of a public health issue by news and entertainment media also represent a promising complementary strategy to conventional media campaigns.

- Outcomes should undergo rigorous independent assessment and peer-reviewed publication should be sought

Discussion points:

How can we better embed the above principles in the design, delivery and evaluation of online safety campaigns?

What is the behaviour change we want to see as a result of campaign impact? Do we want young people to change or do we want to promote their positive behaviours?

How might we better mobilise indirect pathways to ensure the best possible online safety outcomes for young people? What would the social, cultural and developmental levers be for achieving this?

What sorts of access to support are necessary to support young people's safety in relation to specific risks?

How might we deepen our use of social marketing strategies to achieve online safety impacts?

Young and Well CRC

Safe and Well Online: Researching social communications in the promotion of young people's safety and wellbeing

Safe and Well Online will develop and test a program of online, youth-centred social communications to promote young people's safety and wellbeing online.

In partnership with young people, community, government, end-users, research organisations and the digital media industry, this project will develop and evaluate an online social marketing framework, executing at least four campaigns and will use longitudinal tracking and innovative digital data collection to measure reach, outcome and impact of campaign activity whilst determining the efficacy of attitudinal and behaviour change in young people.

Informed by in-depth research with young people, it will use commercial online advertising techniques and methodologies to engage with young people and deliver messages and educative tools to promote positive behavioural change.

AIMS

1. Determine the efficacy of the Safe and Well Online framework to deliver attitudinal and behaviour change to promote cybersafety and wellbeing.
2. Establish a framework of best practice in online delivery of messaging to support safe behaviours.

Produce valuable evidence in the form of a national dataset on young people's engagement with online cybersafety campaigns, to inform policy, practice and knowledge utilisation for improving mental health.

RESEARCH QUESTIONS

1. To what extent do the social media campaigns delivered impact on young people's (i) attitudes, and (ii) behaviours towards safe online practices? Is change sustainable through this framework?
2. To what extent are young people engaging with social marketing and branding campaigns for cyber-safety and mental health promotion? What roles do: platforms, devices, frequency, type and nature of content play in effective messaging?

METHODOLOGY

Using evidence of best practice and a youth participation approach as the basis for developing an innovative methodology, this project will devise, test and evaluate a new program of four developmentally sequential youth-centred campaigns with four waves of delivery each year. Campaign themes may include respectful relationships, digital citizenship and cybersafety, violence prevention, and help-seeking. However, each will be determined by youth engagement and will be relevant to the time and setting in which the study is being undertaken. Using a mixed methodology, this project will use both pre- and post-test experimental design, in-depth interviews and focus groups, as well as opt-in active and passive tracking.

DESIGN

This project design is premised on previously successful programs for behaviour change, where intensity and duration of delivery are critical to outcomes (Spears, et al.). The overall program design of four sequential youth-centred campaigns sits within a recognised developmental and constructivist spiral learning model where the learner continually builds upon what they have already learned (Hawker & Boulton, 2000). It will use a 5-year, multi-method strategy comprised of:

1. Youth participation**,** where young people actively contribute to the development and delivery of each campaign (Years 1 through 5).
2. Longitudinal, test-retest methodologies for evaluation of (a) *implementation* and *process* of delivery (e.g. intensity and duration) and (b) the *efficacy* of the intervention/campaign for effecting behaviour change (Years 2 through 5).

For more information please visit:
http://www.youngandwellcrc.org.au/safe-and-supportive/safe-and-well-online

The challenge of defining the risks to young people's online safety

There is, by now, a lot of evidence available about the prevalence of online safety risks among particular age groups, and this evidence has been vital to organisations' capacity to develop and deliver cybersafety messages. There is strong evidence to indicate that cybersafety messages are being understood by young people, with anecdotal reporting suggesting that young people have integrated mainstream online safety messages into the everyday language they use to talk about their digital practices. Current approaches to cybersafety now generally aim to minimize risks whilst promoting the positive opportunities available to young people online. Further, research shows that a majority of parents and carers are taking active steps to support their children to negotiate online risks.[15]

However, complex factors shape the ways young people relate mainstream cybersafety messaging to their everyday technology experiences. This is best illustrated via a brief example. The AU Kids Online study reports that: 'Just over one in eight (14%) of Australian parents say they don't know whether their child has seen sexual images online... Significantly, half (49%) the parents of Australian children who say they have seen sexual images on the internet say their child has not seen such images.' [16] At first glance, this looks like an alarming statistic that points to a significant gap between young people's reported online practices and their parents' awareness of them. However, this statistic is later qualified by the following statement: 'Most Australian children (72%) have not experienced seeing sexual images online and, of those who have, almost two in three (64%) say they were not bothered or upset by the experience.'[17] This scenario highlights that exposure to risk does not relate to harm in a straightforward manner. It also highlights the fact that an online practice that is commonly defined by adults as a 'risk' is not necessarily framed by young people in the same way.

To date, whilst online risks are widely debated in the literature, nontheless, definitions of online risk and safety have been largely generated by adult-centred institutions. Indeed, evidence shows that dealing with some practices that are currently configured as serious risks within mainstream debates about online safety – such as cyberbullying, hacking and lack of privacy – is generally perceived by young people as a normalised or routine aspect of their digital practice.[18] As such, young people generally conceptualize cybersafety as an issue about risk management rather than eliminating all forms of online risks.[19] Hope (2007), in his study of *intentional* internet misuse in school settings explains that if young people 'fail to label their actions as 'risky' then from their viewpoint they are not engaging in risk taking and a discussion of their rationale becomes meaningless… Indeed, of the 57 students [Hope] interviewed, only five identified chat rooms as potentially hazardous, two expressed concern about accidentally stumbling across online pornography, and three voiced anxieties about school internet security'.[20]

[15] AU Kids Online, 28.
[16] AU Kids Online, 28
[17] AU Kids Online, 28
[18] ACMA report, 2012.
[19] Livingstone and Helsper, 2007.
[20] Hope, 2007, 91.

In a large-scale study of online risks and safety for Australian children, the authors investigated online experiences by asking children about things that had 'bothered' them, emphasizing that risks do not necessarily result in harm. Green et al. explain that, 'by bothered we meant, "made you feel uncomfortable, upset, or feel that you shouldn't have seen it." The aim was to focus on the child's self-report of concern or distress, avoiding an adult framing (e.g. danger, risk, bad things).'[21] Indeed, one of the challenges for researching young people's perceptions of online safety is that of finding ways to go beyond describing 'what young people know' about online safety to examine their everyday practices in more detail.

Cybersafety means different things to different groups of young people. Exposure to sexual images, for instance, may bother or upset young children but not necessarily older teens; indeed teens may seek out these images as part of exploring their sexuality and identity, and and take pleasure in subverting prescribed social norms. To date, there is very little rigorous qualitative evidence that documents how young people conceptualise risk and how they negotiate this in their everyday online interactions. There is an urgent need to introduce the insights and experiences of young people into debates about defining the risks of online engagements. This is not to suggest that policy-makers and practitioners should hand over complete responsibility to young people. However, it is evident that, unless we can embed young people's experiences in the conceptualisation of online safety, we risk producing messaging that does not connect meaningfully with young people's lived experiences of technology. The challenge is to consider young people's views in light of existing definitions to come up with more inclusive ways of understanding and responding to challenges and opportunities.

Staksrud and Livingstone suggest that when it comes to children and young people and the internet, 'restricting [their] online opportunities (whether by limiting their access to the internet or controlling their activities) is unsatisfactory.'[22] They suggest that more emphasis should be placed on 'coping responses', which include self-regulation, to reduce the harm that can result from online risks. This argument resonates with the research conducted on drink driving and speeding campaigns targeting young male drivers in Australia.[23] Tay concludes that advertisements that suggest alternative 'coping strategies' to drink driving, such as organizing a sober driver when out with friends, have been more effective in changing the dangerous driving practices of young male drivers. By contrast, campaigns that focus on emotional dimensions of fear, such as those more commonly found in anti-speeding campaigns may affect young men's attitudes towards reckless driving but are less likely to actually change their driving behaviours.[24] If we apply this approach to cybersafety, it becomes clear why fear-based campaigns are less likely to resonate with young people. Evidence suggests that online safety campaigns need to be wary of constructing young people, along with their digital practices, as problematic as this potentially undermines the young people's identification with campaign messages. Indeed, some research has shown that older children find cybersafety messages to be stale and/or overly sensationalised. [25]

[21] Green et al., 2012, 27.
[22] Staksrud and Livingstone, 2009, 365.
[23] Tay, 2005.
[24] Tay, 2005.
[25] Staksrud and Livingstone, 2009, 365.

Finally, online safety campaigns need to be attendant to the ways diversity impacts the perception and impact of risk online. We currently know very little about the ways that diversity intersects with young people's conceptualisations of risks online. There are gender differences in the ways young people perceive risks. For example, Australian girls (37%) are significantly more likely than boys (22%) to say that something on the internet has bothered them. Parents mirror this gender difference, seeing the internet as more problematic for their daughters than their sons.[26] There are also developmental differences, meaning that online safety strategies need to be able to respond to the shifting and dynamic notions of risk that impact young people in online contexts across different ages. However, there is much further work to be done to understand the ways that vulnerable young people experience and respond to online risks.

With more knowledge of young people's understanding of what cybersafety is and how they manage online risks, we can make improve the kinds of messages about online safety as well as the ways in which those messages need to be delivered. Qualitative youth-centred research can assist the development of strategies for harm-minimisation/promotion of safety and wellbeing providing much-needed evidence and understanding of young people's experiences of risk.

What we know about how young people think about and respond to adult-defined online risks

This section summarises some common themes emerging from research about how young people think about and respond to the notions of risk that have dominated the cyber safety landscape to date. Where possible and/or relevant, we make comparisons with other society-wide health and safety campaigns.

1. Cyberbullying

Cyberbullying is a key concern for young people participating in online spaces, even though most children have not experienced bullying, online or offline. Green et al note that, in Australia, 'as elsewhere, face to face bullying is more common than online bullying. Even so, the incidence of online bullying in Australia (13%) is twice as high as the European average (6%), although the small sample numbers prompt caution in interpretation'.[27] Cyberbullying generally occurs in seven ways:

1. Text messaging – can include the sending of a threatening message which can intimidate
2. Picture/videos – can be sent to make the person being bullied feel threatened
3. Phone calls – including silent and abusive calls
4. Email – sending threatening messages
5. Chat rooms – can involve sending threatening messages in from of other users
6. Instant messages

[26] AU Kids Online, 28.
[27] Green et al., 2012, 33.

7. Websites – can include social networking sites where the person bullied may be targeted in front of others[28]

Ackers reports that Year 8 students, typically 12-13 year olds, are 'most vulnerable to being a victim of cyberbullying.'[29] At this age, young people transition from using technology primarily for entertainment to using it for more social purposes. It takes them time and experience online to develop the necessary digital literacy to participate safely. Older teenagers are more likely to be active rather than passive users of online spaces, reflecting their improved digital skills.[30] These developmental considerations need to be taken into account by campaigns.

Children distinguish between one-off incidents and ongoing bullying behaviour.[31] It is now standard practice across the sector to conceptualise cyberbullying as a reoccurring experience.[32] As such, like many online safety issues, addressing cyberbullying requires consistent strategies across long timelines. This has obvious resource implications for the sector.

Research consistently finds that motivations for cyberbullying are the same as face-to-face bullying.[33] Importantly, Livingstone et al. find that cyberbullying is more common in countries where bullying in general is more common rather than in countries where the internet is more established or where young people have better access to the internet.[34] This highlights the need for campaigns to address the broader social and cultural contexts in which young people's online practices are embedded. It also suggest the need for cybersafety campaigns to support a culture change by leveraging the relationship between 'the online' and 'the offline'.

What distinguishes cyberbullying from 'offline' forms of bullying is the 'ease and speed with which large audiences can be accessed, the availability of the victim 24 hours a day, and the ability of the bully to remain anonymous'.[35] Kofoed and Ringrose add that because of the ways that young people share each other's phones, access each other's Facebook accounts, and participate in social networking in a collective way, cyberbullying must be thought about as a social rather than an individual phenomenon.[36] In this respect, campaigns that promote a sense of community and shared responsibility for managing risks (such as recent campaigns to promote 'respectful relationships') are founded in appropriate assumptions.

2. Engaging in online sexual practices

Approximately 20% of young people engage in sexting.[37] As it is currently defined, sexting refers to young people 'writing sexually explicit messages, taking sexually explicit photos of

[28] Ackers, 2012, 142.
[29] Ackers, 2012, 143.
[30] Green et al. 2012.
[31] Ackers, 2012, 142.
[32] Hinduja and Patchin 2010, 208.
[33] Oliver and Candappa, 2003.
[34] Livingstone et al., 2011.
[35] Ackers 2012, 153.
[36] Kofoed and Ringrose, 2012, 7.
[37] Willard, 2010, 542.

themselves or others in their peer group, and transmitting those photos and/or messages to their peers'.[38] Beyond moral debates about the role of technology in adolescent sexual identity and development, sending and receiving sexual messages constitutes a major risk for young people because Australian legislation deems the exchange of sexual images of young people under the age of 18 as 'child pornography', a criminal offence.[39] The potential legal implications of this digital practice are generally not well understood by young people, pointing to the complexities involved in using media campaigns to address online safety issues which have potential legal consequences.

Sexting was the focus of the major ThinkUKnowAustralia public campaign in 2010. The campaign turned around a short video featuring a female high school student, Megan, who experiences having her semi-naked photo shared around her school by a boy she thought she could trust. As the phones beep in class, Megan is reduced to tears and is humiliated in front of her teacher. In their evaluation of this media campaign, Albury and Crawford argue that the campaign promoted a fear-based approach to cybersafety education that reproduced gender stereotypes by defining young women as inherently at risk of sexual violence, and did little 'to engage with the serious legal penalties facing young people who are charged for sexting.'[40] Further, they argue that, in as much as the campaign positioned young people 'as both criminals and vulnerable subjects'[41] this cybersafety campaign places young people in a double bind.

Even when legal penalties are clearly understood, this does not necessarily limit young people's sexting practices. Sexting, like other 'risky' behaviours, emerges at the intersections of young people's explorations and performances of sexuality, pleasure, friendship, community, creativity, autonomy and self-determination, and individual identity. Research on cybersafety has not yet comprehensively grappled with the question of how notions of *pleasure* and risk are interrelated. Indeed there is very little qualitative research that provides a deep contextual understanding of the everyday ways that young people think about and negotiate 'risky behaviours' that have online dimensions. Where research does exist, it points to the ways that young people's 'risky' online practices are both embedded in and facilitate peer networks and sociality. Brown and Gregg, for example, explain how a 'big night out' amongst friends is something anticipated on Facebook.[42] They say, 'alcohol consumption is linked to tales brimming with fun, adventure and friendship. So while vomiting and making a fool of oneself may be part of the experience, a 'bad' story becomes a 'good' anecdote when it can be recounted later among friends.'[43] These are the kinds of social norms with which online safety campaigns must grapple.

Evidence shows that campaigns targeting binge drinking among young women have had very limited success because they do not tap into 'the peer-to-peer networks that have developed in recent years that are central to the pleasures of online and offline consumption.'[44] Hope (2007) argues that, in some cases, participating in 'risky' online practices is about 'public performance'; that is, it is about cultivating a reputation online and

[38] Willard 2010.
[39] Albury, Funnel and Doonan, 2010.
[40] Albury and Crawford, 2012, 466
[41] Albury and Crawford, 2012, 466
[42] Brown and Gregg, 2012, 361.
[43] Brown and Gregg, 2012, 361.
[44] Brown and Gregg, 2012, 365.

engaging an audience. Future campaigns might develop strategies that mobilise these 'micro-celebrity' practices.

3. Giving out personal information online

Online privacy refers to both immediate privacy considerations, such as disseminating personal information, as well as issues relating to an individual's 'digital footprint', which refers to the legacy of information available online over time. Research shows that young people appear to be aware of immediate privacy concerns, but are less engaged with the idea of their digital footprint.[45] The long-term effects of one's digital footprint are under-researched, meaning that there are no conclusive evidence-based determinations about the risks to reputation and young people's future opportunities. Young people tend to manage or avoid online risks based on past personal experiences rather than the cybersafety messages they receive. This suggests that cybersafety campaigns might be more effective if they mobilised indirect pathways for behaviour change. That is, rather than focusing on didactic cybersafety messaging, campaigns might usefully intervene in and reshape the broader social and cultural practices that expose young people to online risks.

In terms of privacy and social networking, Green et al. report that 83% of young people in Australia are likely to have their profiles set to private or partially private.[46] In a major ThinkUKnow campaign in the UK, advertisements highlighted the risks associated with sharing personal information online. In one short film, a young girl is shown revealing personal information to a friend she met online, eventually agreeing to meet the person she thought was a young girl and her confidante in a public park. The person behind the screen is shown to be an older male and a sexual predator. This campaign works with the prevailing understanding that giving away personal information online can lead to strangers using that information to hurt the young person. However, research by Green et al. found that most Australian children and young people are online friends with people they already know offline. Of the small minority that made friends online first, only 5% of those have considered meeting up with that person offline.[47] As such, the 'stranger danger' cybersafety campaigns address an extreme and generally unlikely case rather than speaking to the majority of young people's everyday online experiences.

Livingstone and Helsper add to this discussion by explaining that most children and young people communicate online with their offline friends, adding that age rather than gender affects the 'communicative risks' that occur with disclosing personal information online.[48] They say that as children grow older they are more likely to engage in 'sensation seeking' practices and become more careless about revealing personal information online.[49] They encourage researchers and policymakers to consider the 'offline social-psychological factors in young people's vulnerability to online risks.'[50] These factors might include traits such as young person's shyness, confidence, and dissatisfaction with life, loneliness or mental illnesses.

[45] ACMA report, 2012.
[46] Green et al. 2012.
[47] Green et al. 2012.
[48] Livingstone and Helsper, 2007, 634.
[49] Livingstone and Helsper, 2007, 634.
[50] Livingstone and Helsper, 2007, 636.

Conclusion

It is crucial that stakeholders in online safety mobilise campaigns to foster a **balanced public debate** about the opportunities and risks of digital engagement that enables users to make informed decisions about how they engage with new technologies. In turn, cyber safety strategies should inform users about the potential risks of engaging online without overstating them; acknowledge the benefits of connectivity; and provide users with access to resources and tools to enhance their digital literacy. The research summarized in this briefing paper provides a useful platform from which to initiate further discussions about the best ways to support young people's online safety practices and foster a process of social and behavioural change in ways that mobilise both conventional and social media in the context of lived experience.

Some prompts to further guide our discussion about cybersafety campaigns for young people

1. How do young people conceptualise the risks of online engagement? To what extent do young people associate online activity and the online environment with risk, what forms does this association take and what is its emotional content?
2. What do young people do with cybersafety messages? How does their awareness of online risks translate into their practice of safety both online and offline?
3. What are the changes that cybersafety campaigners want to see occur in young people's behaviours?
4. How can we leverage young people's existing online and offline practices for digital safety?
5. How can we move away from a focus that constructs young people's online practices as problematic towards a more stregnths-based approach?
6. Is it possible to target multiple risks using one campaign? What allows or prevents this?
7. Who are these campaigns targeting? How can we best address developmental issues?
8. How might campaigns speak more directly to young people's everyday experiences with technology? How do we speak to the fine line between pleasure/risk and harm/creative expression? Is the online environment an opportunity for pleasurable risk-taking, including risk-taking that supports a more autonomous/independent sense of self? In this case, is risk-taking in online contexts seen by young people as being, in fact, in their own interests and for their own benefit?
9. Research shows that those most at risk offline are correspondingly more at risk online, with marginalised young people identified in the US and Australia as the group who are most vulnerable online. How can cybersafety campaigns better address diversity?
10. "Many drivers in Australia still believe that anti-speeding enforcement is implemented more for the purpose of raising revenue than increasing road safety" (Tay 2005:927). A question for this research might be whether young people/children perceive cybersafety campaigns to be about limiting their freedom or restricting the creative ways they use the internet or digital spaces rather than for their own benefit. Is there a way to capture this in the pilot study?